HOUSE OF COMMONS
CANADA

OPEN AND SHUT:

ENHANCING THE RIGHT TO KNOW AND THE RIGHT TO PRIVACY

REPORT OF THE STANDING COMMITTEE ON JUSTICE AND SOLICITOR GENERAL ON THE REVIEW OF THE ACCESS TO INFORMATION ACT AND THE PRIVACY ACT

BLAINE A. THACKER, M.P.
CHAIRMAN

OPEN AND SHUT:

ENHANCING THE RIGHT TO KNOW AND THE RIGHT TO PRIVACY

REPORT OF THE STANDING COMMITTEE ON JUSTICE AND SOLICITOR GENERAL ON THE REVIEW OF THE ACCESS TO INFORMATION ACT AND THE PRIVACY ACT

March 1987

Published under authority of the Speaker of the House of Commons by the Queen's Printer for Canada

Available from the Canadian Government Publishing Centre, Supply and Services Canada, Ottawa, Canada K1A 0S9

Issue No. 9
Chairman: Blaine A. Thacker

Minutes of Proceedings and Evidence of the Standing Committee on

Justice and Solicitor General

RESPECTING:

Review of the Access to Information and Privacy Acts

INCLUDING:

First Report to the House

Second Session of the
Thirty-third Parliament, 1986-87

STANDING COMMITTEE ON JUSTICE AND SOLICITOR GENERAL
(Second Session, Thirty-third Parliament)

Chairman: Blaine A. Thacker
Vice-Chairman: Rob Nicholson

MEMBERS

Robert Horner
Carole Jacques
Jim Jepson
Robert Kaplan
Alex Kindy
Allan Lawrence
John V. Nunziata
Svend J. Robinson
Ian Waddell—(11)

(Quorum 6)

Clerk of the Committee
Luke Morton

STANDING COMMITTEE ON JUSTICE AND SOLICITOR GENERAL

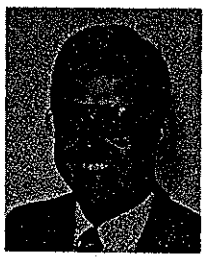
(Members and Alternates participating in the Access and Privacy Review)

Blaine A. Thacker, P.C.
Lethbridge-Foothills, (Alta.)
(CHAIRMAN)

Rob Nicholson, P.C.
Niagara Falls (Ont.)
(VICE-CHAIRMAN)

Warren Allmand, Lib.
Notre-Dame-de-Grâce—
Lachine East, (Que.)

Robert Horner, P.C.
Mississauga North (Ont.)



Jim Jepson, P.C.
London East (Ont.)

Alex Kindy, P.C.
Calgary East
(Alta.)

Allan Lawrence, P.C.
Durham-Northumberland
(Ont.)

Svend J. Robinson, N.D.P.
Burnaby, (B.C.)

COMMITTEE STAFF

Committees and Private Legislation Directorate
Luke Morton, Clerk of the Committee
Claudette St. Pierre, Secretary to the Clerk
Isabelle Des Chênes, Secretary
Fiona Bladon, Administrative Assistant
Lena L'Ecuyer, Proofreader
Carole Dancause, Proofreader

Consultants to the Committee
David H. Flaherty
T. Murray Rankin

Research Branch, Library of Parliament
Philip Rosen, Research Coordinator
Habib Massoud, Research Assistant

Translation Bureau
Andrée Larocque, translator

ORDER OF REFERENCE

Monday, November 19, 1984

ORDERED,– That the Standing Committee on Justice and Legal Affairs* shall have permanently referred to it all annual reports made to Parliament pursuant to section 72 of the Privacy Act and section 72 of the Access to Information Act; and

That it be an instruction to the Standing Committee on Justice and Legal Affairs to:

1. consider every report prepared under section 72 of the Access to Information Act and of the Privacy Act;

2. undertake, on a permanent basis, a review pursuant to subsection 75(1) of the Access to Information Act and of the Privacy Act, of the administration of those Acts; and

3. undertake, within three years of their coming into force, a comprehensive review of the provisions and operation of the Access to Information Act and of the Privacy Act pursuant to subsection 75(2) of each of the said Acts.

ATTEST

MICHAEL B. KIRBY
For the Clerk of the House of Commons

* On March 20, 1986 the Committee's name was officially changed from the Standing Committee on Justice and Legal Affairs to the Standing Committee on Justice and Solicitor General.

STATUTORY ORDERS OF REFERENCE

ACCESS TO INFORMATION ACT

S. 75.(1) The administration of this Act shall be reviewed on a permanent basis by such committee of the House of Commons, of the Senate or of both Houses of Parliament as may be designated or established by Parliament for that purpose.

(2) The committee designated or established by Parliament for the purpose of sub-section (1) shall, within three years after the coming into force of this Act, undertake a comprehensive review of the provisions and operation of this Act, and shall within a year after the review is undertaken or within such further time as the House of Commons may authorize, submit a report to Parliament thereon including a statement of any changes the committee would recommend.

PRIVACY ACT

S. 75.(1) The administration of this Act shall be reviewed on a permanent basis by such committee of the House of Commons, of the Senate or of both Houses of Parliament as may be designated or established by Parliament for that purpose.

(2) The committee designated or established by Parliament for the purpose of sub-section (1) shall, within three years after the coming into force of this Act, undertake a comprehensive review of the provisions and operation of this Act, and shall within a year after the review is undertaken or within such further time as the House of Commons may authorize, submit a report to Parliament thereon including a statement of any changes the committee would recommend.

THE STANDING COMMITTEE ON JUSTICE AND SOLICITOR GENERAL

has the honour to present its

FIRST REPORT

In accordance with its Order of Reference dated Monday, November, 19, 1984 concerning the review of the Access to Information Act and the Privacy Act, and pursuant to section 75 of each of the aforesaid Acts, the Standing Committee on Justice and Solicitor General has adopted the following report and urges the Government to consider the advisability of implementing the recommendations contained herein.

Pursuant to Standing Order 99(2), the Committee requests that the Government table a comprehensive response to the Report within one hundred and twenty (120) days.

A copy of the relevant Minutes of Proceedings and Evidence of the Standing Committee on Justice and Solicitor General (Issues Nos. 8, 10 to 18, 20, 22 to 29, and 30 of the First Session, Thirty-third Parliament and Issues Nos. 3, 8, and 9 which includes this Report, of the Second Session, Thirty-third Parliament) is tabled.

Respectfully submitted,

Blaine A. Thacker, M.P.
Chairman

TABLE OF CONTENTS

DETAILED TABLE OF CONTENTS

ACKNOWLEDGEMENTS

The comprehensive review of the provisions and operation of the *Access to Information Act* and the *Privacy Act* by the Committee could not have been completed without the labour of many people. All of those who responded to the Committee's invitation to make submissions by sharing their experience and insights played a central role in assisting us to formulate the conclusions and recommendations set out in this Report. The Information Commissioner, Inger Hansen, Q.C., and the Privacy Commissioner, John W. Grace, and their staffs, were unstinting in their support of the Committee in this comprehensive review and were generous in sharing their views on a formal and informal basis.

A task such as the one undertaken by this Committee could not be completed without the efforts of a highly competent, devoted staff. Such is the case here. Professors David H. Flaherty of the University of Western Ontario and T. Murray Rankin of the University of Victoria facilitated the Committee's task with their expertise, inspiration and good humour. Philip Rosen, of the Research Branch, Library of Parliament, lent his experience, patience and perseverance to accomplishing the numerous research tasks necessary to completing a Report of this nature. Habib Massoud, also of the Research Branch of the Library of Parliament, provided the Committee with valuable research assistance.

During the course of this comprehensive review, the Committee had the support of the logistical and administrative skills of three able Clerks: in chronological order, these were—Santosh Sirpaul, François Prégent and Luke Morton.

Finally, but not least of all, the Committee would like to thank the staff of the Committees and Private Legislation Directorate, the Translation Bureau of the Secretary of State and the other services of the House of Commons that have provided it with administrative and technical support.

EXECUTIVE SUMMARY

Section 75 of both the *Access to Information Act* and the *Privacy Act* required a Committee of Parliament to conduct a comprehensive review of the provisions and operation of both Acts. The legislation requires this comprehensive review to have commenced by July 1, 1986 and to be completed within one year. This Report by the Standing Committee on Justice and Solicitor General, which was designated by the House of Commons to carry out this task, is the outcome of that process.

During the winter of 1985-86, the Committee issued invitations to a number of government institutions, non-governmental organizations and individuals for briefs and submissions. In response, the Committee received in excess of eighty briefs. The Committee held public hearings during May and June 1986 when it heard testimony from thirty-one government institutions, groups and individuals.

The Committee's comprehensive review of the provisions and operation of the *Access to Information Act* and the *Privacy Act* is, in large measure, a pioneering experience. This Report is based upon an innovative legislative provision requiring parliamentary oversight and evaluation within a determinate time period. This unusual legislative provision has, since 1982, been included in a number of other Acts of Parliament. Hence, to a certain extent, the conduct of a comprehensive review by this Committee has blazed the trail for parliamentarians who may later be called upon to conduct similar future exercises in legislative oversight and evaluation. Consequently, the Committee has indicated in some detail in the Introduction to its Report how it conducted this comprehensive review of the *Access to Information Act* and the *Privacy Act*.

Section 24(2) of the *Access to Information Act* also required the Committee to review and report on the statutory prohibitions against disclosure contained in Schedule II of the Act. The Committee fulfilled this responsibility when, on June 19, 1986, it tabled its First Report in the House of Commons. It recommended that section 24 and Schedule II of the *Access to Information Act* be repealed but that the prohibitions already found in the *Income Tax Act*, the *Statistics Act* and the *Corporations and Labour Unions Returns Act* be added to the *Access to Information Act*.

The Committee's Report on the comprehensive review of the provisions and operation of the *Access to Information Act* and the *Privacy Act* is inspired by the principles enunciated in both Acts: that they are to enhance the right of access to government information and the protection of individual privacy enjoyed by all Canadians. This study has led the Committee to conclude that both Acts have shown major shortcomings and weaknesses. In some cases, the current legislative scheme is inadequate; in others, there are issues not addressed at all by the Acts.

The Committee's Report is structured as follows. Firstly, it addresses a number of 'threshold issues' which are common to the provisions and operation of both the *Access to Information Act* and the *Privacy Act*. Among these 'threshold issues' are the extension of the coverage of both Acts, the extension of access rights, and the status and role of Access/Privacy Coordinators. The Report then deals with exemptions and Cabinet confidences, as well as the roles of the Information Commissioner, the Privacy Commissioner and the Federal Court of Canada. Although these latter issues are common to both Acts, the Committee felt that they were sufficiently important to deserve separate treatment. The balance of the Report then deals with issues that are unique to each of the present Acts, as well as a number of issues which are beyond the reach of both pieces of legislation in their current form. In its concluding chapter, the Report addresses several resource issues and the need for future parliamentary oversight of the *Access to Information Act* and the *Privacy Act*.

The Committee deals with a number of 'threshold' issues in Chapter 2 of the Report. One of the major problems recognized by the Committee is how little the *Access to Information Act* and the *Privacy Act* are known both within government and among Canadians generally. Consequently, the

Committee recommends that both Acts be amended to ensure that there is provision for a public education mandate, and for the education and training of government employees.

At present, the Acts do not apply to all government institutions—hence there is confusion as to which are subject to this legislation. The Committee recommends that the *Access to Information Act* be extended to all government institutions and to offices directly responsible to Parliament, but not to judicial institutions. It also recommends that the *Privacy Act* be extended to all government institutions, to offices directly responsible to Parliament, and to judicial institutions. The Committee finally recommends that both Acts be extended to cover all Crown corporations and their wholly-owned subsidiaries, but that the *Access to Information Act* not apply to program material held by the Canadian Broadcasting Corporation.

At present, only Canadian citizens and permanent residents of this country have rights of access to information under both Acts. The Committee recommends that any person, natural or legal, should have access rights under the *Access to Information Act* and the *Privacy Act*.

Although the 'designated head' of each government institution named by regulation under the *Access to Information Act* and the *Privacy Act* is legally responsible for the administration of the legislation, in fact, the day-to-day work is carried out by Access/Privacy Coordinators who receive and process access requests. The Committee has concluded that Coordinators are the prime movers for the implementation of both Acts and that this status should be formally entrenched in the legislation. The Committee recommends that, because of the importance of their role, Coordinators should be officials of senior rank, wherever possible, and should have direct working and reporting relationships with senior management and program officials. The Committee has also concluded that Coordinators will do their jobs more effectively if they are provided with more training, backup, and coordination services by the Treasury Board Secretariat and the Department of Justice.

Chapter 3 of the Report deals with exemptions and the exclusion of Cabinet confidences in both the *Access to Information Act* and the *Privacy Act*. At present, both Acts are a confusing mixture of numerous exemptions: some are class- or harms-tested; some are discretionary or mandatory in nature. The Committee examined this confusing situation and has concluded that all exemptions in both Acts, with the exception of its proposed exemption dealing with Cabinet confidences, should be discretionary in nature and subject to a 'significant injury' test. This Chapter of the Report also contains a number of recommendations dealing with the narrowing of specific exemptions in both Acts.

Chapter 3 of the Report also deals with the exclusion of Cabinet confidences contained in both the *Access to Information Act* and the *Privacy Act*. Under the present legislation, Cabinet confidences are excluded from the ambit of both Acts: this means not only that there is no access to such documents, but also that a refusal of access to such documents is not reviewable by either the Commissioners or the Federal Court of Canada. The Committee received more submissions on the issue of Cabinet confidences than on any other question. The conclusion reached by the Committee is that Cabinet confidences should be subject to a class-tested, discretionary exemption. This Cabinet confidences exemption should only cover agendas, minutes of meetings and draft legislation or regulations which have been in existence for fewer than fifteen years. The Committee concluded that the remaining elements of the current provisions on Cabinet confidences would be adequately protected by other exemptions in both Acts. Because of the unique role of Cabinet in our parliamentary system of government, the Committee concluded that a refusal of access to Cabinet confidences should not be reviewable by the Commissioners but only by the Associate Chief Justice of the Federal Court.

The Committee deals with the Commissioners and the Federal Court in Chapter 4 of its Report. Under present legislative arrangements, the Information Commissioner and the Privacy Commissioner do not have the power to issue binding orders. They also share premises as well as some administrative and management staff. The Committee concludes that the office of the Information Commissioner and the Privacy Commissioner should be separated so that there should be no real or perceived conflict of

interest in the discharge of their respective duties. The Commissioners should continue generally to have powers of recommendation only, although the Information Commissioner should be empowered to issue binding orders in the areas of delays, fees, fee-waivers, and time extensions.

At present, the *Access to Information Act* and the *Privacy Act* provide two different standards under which the Federal Court of Canada can exercise judicial review under each Act. The Committee examined this issue and concluded that both Acts should be amended to allow the Federal Court to conduct *de novo* judicial review. In this way, the Federal Court of Canada could put itself in the place of the government institution and render the decision that, in its view, should have been made by the government institution.

In Chapter 5 of the Report, the Committee makes recommendations dealing with a number of particular issues under the *Privacy Act*. In the area of computer-matching, the Committee recommends that the *Privacy Act* be amended to ensure that this exercise in linking personal records is conducted only when demonstrably necessary and under the continued vigilant oversight of the Privacy Commissioner. The widespread collection of Social Insurance Numbers in all sectors of society has long been a source of controversy. The Committee examined this situation and has concluded that the *Privacy Act* should be amended to restrict the collection of Social Insurance Numbers by making it unlawful to collect them without lawful authorization. The Committee examined the provision of the *Privacy Act* (section 18) which permits the establishment of exempt banks containing personal information thereby deemed to be entirely beyond access. It was concluded that the arguments in favour of retaining exempt banks were unconvincing and that these banks should be deleted entirely from the *Privacy Act*.

In other issues dealt with in this part of the Report, the Committee recommends that there be civil remedies in damages and criminal penalties for breaches of the *Privacy Act*, that the Privacy Commissioner be consulted regularly by policy-makers and law-makers, that the *Privacy Act* be amended to cover the Canadian Police Information Centre and similar collection systems for sensitive data, that the provisions of the *Privacy Act* defining 'consistent use' and 'personal information' be clarified, and that a provision on security of personal information be added to the *Privacy Act*.

The Committee deals with a number of particular issues under the *Access to Information Act* in Chapter 6. At present, there are no detailed criteria under which government institutions may waive fees for access to information. The Committee recommends that the Act or the Regulations be amended to set out the criteria under which fee waivers would be granted; a proposed set of such criteria is set out in the recommendation. One of the major complaints heard by the Committee was about the length of time government institutions often take in fulfilling access requests. The Committee recommends that the initial response time available to a government institution should be 20 days, rather than 30 days as at present, subject to a further 40-day extension. Under the Committee's proposal, an extension beyond the additional 40 days may only be obtained through the issuance of a certificate by the Information Commissioner.

The Committee also looked at the issue of delays at the office of the Information Commissioner. To resolve these difficulties, the Committee recommends that after 60 days a complainant be allowed to obtain a certificate showing that a complaint investigation has not been completed—this would permit the complainant to seek review of the complaint by the Federal Court, if so desired. This recommendation would also apply to investigations by the Privacy Commissioner. The Committee concludes this Chapter by recommending that the *Access to Information Act* be amended to permit government institutions to release records without the need for an access request when the public interest so requires and a grave environmental, health or safety hazard makes it necessary to do so.

Chapter 7 of the Report deals with a series of emerging privacy issues. On electronic surveillance, the Committee recommends that the *Privacy Act* be amended to deal with it in explicit terms and that the Privacy Commissioner continue to monitor developments in this area. Similarly, the Committee makes these same recommendations in relation to drug tests and the use of the polygraph.

Unlike the situation in some countries, the federally-regulated private sector is not subject to the *Privacy Act*. Having considered this state of affairs, the Committee recommends that those portions of the *Privacy Act* dealing with fair information practises and complaints to the Privacy Commissioner be extended to the federally-regulated private sector. The emphasis would be on self-regulation by the federally-regulated private sector, with the Privacy Commissioner being empowered to review and approve implementation schemes. In practise, this means that the basic principles of the *Privacy Act* would be extended to banks, cable television operators, airlines, federally-regulated telephone companies and others.

The Committee concludes Chapter 7 by making a number of observations and recommendations in relation to the impact of information technology on individual rights, the oversight of the use of microcomputers and the regulation of transborder data flows.

The Committee briefly discusses a number of other access issues in Chapter 8 of its Report. Among these issues are the *Official Secrets Act*, the documents classification system, the oath of secrecy, 'whistle-blowing' and 'sunshine' legislation. In relation to Crown Privilege and the *Canada Evidence Act*, the Committee recommends that section 36.3 of that Act be deleted and that Cabinet confidences in that context be subject to judicial scrutiny along the lines proposed in relation to the *Access to Information Act* and the *Privacy Act*.

The final conclusions reached by the Committee in conducting its comprehensive review of the provisions and operation of the *Access to Information Act* and the *Privacy Act* are set out in Chapter 9. The resource, budgetary, and personnel implications of separating the Commissioners' offices and adding to the Privacy Commissioner's responsibilities are discussed in this Chapter. The Committee concludes that many of the Privacy Commissioner's new responsibilities can be fulfilled with modest resource increases, especially if these new duties are phased in over a reasonable period of time.

The Committee expresses its satisfaction with the comprehensive review process it has just completed. It recommends that the Commissioners and government institutions be heard more frequently and more regularly by Parliament in relation the both the *Access to Information Act* and the *Privacy Act*. Not only should government institutions continue to table their Annual Reports in Parliament, but the Committee also recommends that the Treasury Board Secretariat prepare Consolidated Annual Reports on both Acts to be tabled in Parliament. Finally, the Committee concludes that a further comprehensive review of the *Access to Information Act* and the *Privacy Act* be undertaken by a parliamentary committee within 4 years of the tabling of this Report in the House of Commons.

CHAPTER 1

INTRODUCTION

The entrenchment of fundamental rights and liberties in the *Canadian Charter of Rights and Freedoms* has been widely heralded and has had an important impact on government and the courts. Of similar significance was the enactment of the *Access to Information Act* and the *Privacy Act* by Parliament in 1982.[1] These laws have given Canadians potential instruments with which to strengthen Canadian democracy. The Charter and the two Acts represent significant limits on bureaucracy and have provided a firm anchor to individual rights.

A unique feature of the *Access to Information Act* and the *Privacy Act* is that they both provide for a parliamentary evaluation of their provisions and operation. That examination is the subject of this Report.

Committee's Mandate and Approach to the Task

Section 75 of both the *Access to Information Act* and the *Privacy Act* provide that a Committee of Parliament shall conduct a comprehensive review of the provisions and operation of these two pieces of legislation. Both Acts require that the comprehensive review commence within three years of their proclamation, that is by July 1, 1986, and that the task be completed within one year. By Order of Reference dated November 19, 1984, the House of Commons conferred the duty of effecting this comprehensive review upon the Standing Committee on Justice and Solicitor General.

Section 24(2) of the *Access to Information Act* required the Committee designated under section 75 of that Act to conduct the comprehensive review of its provisions and operation, that is this Committee, to review and report upon the statutory prohibitions against disclosure contained in Schedule II thereof. This review was to be completed by July 1, 1986. In its First Report, tabled in the House of Commons on June 19, 1986, the Committee recommended that section 24 and Schedule II of the *Access to Information Act* be repealed, but that the prohibitions already found in the *Income Tax Act*, the *Statistics Act* and the *Corporations and Labour Unions Returns Act* be added to the Act. (See Appendix B.)

During the Summer and Fall of 1985, the Committee formulated its approach to the comprehensive review. An exhaustive questionnaire setting out in detail the issues of concern to the Committee about each Act was developed by its staff. In early December 1985, the Committee issued a press release describing the manner in which it would be conducting the comprehensive review and the projected schedule it would be following. Nearly two hundred letters requesting written submissions as part of the review were sent out by the Committee to a large variety of government institutions, non-governmental organizations and individuals. These invitations were accompanied by questionnaires and a list of issues indicating what the Committee hoped would be addressed by submissions to it. In response to these invitations, we received in excess of eighty Briefs as well as other forms of submissions, all of which were carefully analyzed by the Committee. (See Appendix D for a list of submissions received.)

At the same time as the Committee was undertaking these early stages of its study, the Department of Justice and the Treasury Board Secretariat were also conducting an extensive examination of government institutions' experience with the *Access to Information Act* and the *Privacy Act* during the first three years of operation. Much of what was raised by the Committee in its questionnaires and list of issues was also addressed by this examination. The Committee closely monitored this internal review by government, but at an arm's-length distance. Much of the documentation generated by this internal government study of both Acts has been examined with a

critical eye by the Committee. Among the documents reviewed by the Committee were government institution submissions on exemptions, a media study, a report by a committee of government institution lawyers on legal issues, a report by officials who work with both Acts and a report on exempt banks.

The Committee held public hearings in Ottawa in May and June 1986, during which 31 government institutions, groups and individuals were heard. (See Appendix C for a list of witnesses.) The Minister of Justice, the President of the Treasury Board, the Privacy Commissioner and the Information Commissioner, considered by the Committee to be the main actors within government in relation to access and privacy, appeared before us to lead off our public hearings. The Committee then heard from carefully selected government institutions, non-governmental organizations with relevant experience, users of both Acts, academics and others. They brought to the Committee their unique experiences as users and administrators of both Acts, addressing both practical problems and fundamental philosophical issues. Those who appeared before the Committee were forthright in addressing the issues of interest to us in conducting our comprehensive review of the Acts. Once the Committee had completed its public hearings, it reviewed the submissions made to it and the evidence it had received.

The Committee's approach to the comprehensive review of the *Access to Information Act* and the *Privacy Act* has been to consult widely, both formally and informally, with those who are experienced and knowledgeable in this area both inside and outside of government. We were concerned not just with what the law and regulations say, but also with how they actually function. We have examined both how government institutions have administered the Acts and how Canadians have exercised their rights under these new laws. Where we have concluded that things can be improved upon, we have, in this Report, said how this can be done in clear, precise, concrete ways.

The general principle underlying the Committee's Report is the conviction shared by all parliamentarians that Canadian democracy is strengthened by making government, its bureaucracy and its agencies accountable to the electorate and by protecting the rights of individuals against possible abuse.

The principles upon which the two Acts are based were clearly enunciated by the Honourable John Crosbie, then Minister of Justice, when he told the Committee in May, 1986:

> "— That government information should be available to the public;
>
> — that necessary exceptions to the right of access should be limited and specific;
>
> — that decisions on disclosure of government information should be reviewed independently of government;
>
> — that the collection, retention and disposal of personal information, as well as its use and disclosure should be regulated in such a way so as to protect the privacy of individuals."[2]

A Brief History

Although both the *Access to Information Act* and the *Privacy Act* were adopted by Parliament at the same time, their historical background is not identical. In addition, although there are many similarities between both Acts, there are also some differences.

The *Access to Information Act* has its genesis in the late 1960's and the 1970's. During that period of time, Gerald Baldwin Q.C. and Barry Mather, former members of the House of Commons, introduced a number of private member's Bills which were the direct forerunners of the present *Access to Information Act*. At the same time, political scientist Donald C. Rowat of Carleton University published a number of influential articles advocating more open government and freedom of

information legislation. In June 1977, the Government tabled in Parliament a Green Paper on freedom of information which was referred for consideration to the Standing Joint Committee on Regulations and Other Statutory Instruments. The Joint Committee tabled its Report on the Green Paper in June 1978.

At about the same time, the Canadian Bar Association published a research study on freedom of information, entitled "Will the Doors Stay Shut?",[3] in August 1977, followed in March 1979, by a Model Freedom of Information Bill.[4]

Before the Liberal Government could act on the June 1978 Joint Committee Report, the May 1979 election intervened and a new Progressive Conservative Government came into power. The President of the Privy Council, the Honourable Walter Baker, introduced freedom of information legislation in the form of Bill C-15. It received second reading on December 5, 1979, but died on the Order Paper when the Government fell later that month. On July 17, 1980, the Honourable Francis Fox, Minister of Communications in the Liberal Government, introduced Bill C-43, containing both the present *Access to Information Act* and the *Privacy Act*. Parliament passed Bill C-43 in June 1982, and it was proclaimed in force on July 1, 1983.

The *Privacy Act* has its immediate origins in the mid-1970's. On July 21, 1975, Bill C-72, "An Act to Extend the Present Laws in Canada that Proscribe Discrimination and that Protect the Privacy of Individuals", received first reading, but it died on the Order Paper with the end of the parliamentary session. A revised version of this legislation, Bill C-25, received first reading on November 29, 1976. This Bill, the *Canadian Human Rights Act*, was passed by Parliament and proclaimed in force on March 1, 1978.

Part IV of the *Canadian Human Rights Act* contained measures for privacy protection, including a code of fair information practices and the creation of a Privacy Commissioner (as a member of the Canadian Human Rights Commission). The Progressive Conservative Government which came into power in 1979 drafted a Bill revising Part IV of the *Canadian Human Rights Act*, but the Government fell before it could bring this legislation before Parliament.

The draft Bill did see the light of day, however, when Bill C-535 (a private member's Bill) received first reading on May 2, 1980 under the sponsorship of the Honourable Perrin Beatty, M.P.

As mentioned earlier, the present *Privacy Act* was part of Bill C-43, which was passed by Parliament and proclaimed in force on July 1, 1983.

Description of the Acts

The Committee will not attempt to give an exhaustive description of how the Acts work. This is done more thoroughly and comprehensively elsewhere in other publications. We will simply sketch here the main elements of each Act. More detailed descriptions will be given later in this Report where it is necessary to locate our analysis and recommendations within the proper context.

Under the *Access to Information Act*, any Canadian citizen or permanent resident may, on application and payment of the appropriate fees, have access to records under the control of government institutions. The only government institutions currently subject to the Act are those set out in a Schedule to the Act. Government institutions may refuse access to records under their control if the records sought fall within the classes of records described in a number of broad exemptions in the Act. Any records classified as cabinet confidences are not accessible under the Act.

If an applicant believes that access to a record is being unfairly denied, a complaint may be filed with the Information Commissioner. The Information Commissioner, an independent officer directly accountable to Parliament, conducts an investigation and makes a non-binding recommendation to the

government institution and the complainant. If the government institution continues to withhold the requested records, the applicant may apply to the Federal Court for a binding order.

Since there are many similarities between the *Privacy Act* and the *Access to Information Act*, only the differences will be highlighted in this synopsis. In reality, the *Privacy Act* is data protection legislation. Sections 4 to 8 of the *Privacy Act* set out a code of fair information practices for government institutions. This code prescribes how personal information is to be collected and retained, when it is to be collected, and when it may be released to others or disposed of. Not only do Canadian citizens and permanent residents have access rights to their personal information under the *Privacy Act*, but they also have certain rights to seek correction of their personal information when they believe it is erroneous or incomplete.

In addition to the exemptions from access, as in the *Access to Information Act*, the *Privacy Act* currently provides that whole banks of personal information are exempt from access where all the files which they contain consist predominantly of information relating to international affairs, defence matters or police investigations. The Privacy Commissioner has powers and responsibilities similar to those of the Information Commissioner and is also empowered to audit compliance by government institutions with the provisions of the *Privacy Act*.

The Treasury Board Secretariat has general responsibility for co-ordination of the implementation of both Acts. The Department of Justice has general responsibility for the policy implications of the Acts. The designated head of each government institution is responsible for its compliance with both Acts. Each government institution is responsible for the designation of an Access to Information/Privacy Coordinator who has primary responsibility to receive and process access requests.

General Principles

It is provided in both Acts that their purpose is the extension of the laws of Canada — in the case of the *Access to Information Act*, to provide greater rights of access to records controlled by government institutions; in the case of the *Privacy Act*, to assure the protection of Canadians' privacy with respect to personal information about them which is held by government institutions.

Although access and privacy rights may, at first glance, appear to be contradictory, they do not often come into conflict. Access and privacy statutes are, in fact, complementary rather than contradictory. The development of access legislation is part of a widespread 'open government' movement in democratic societies. Democracies are strengthened by the ability of electorates to hold decision makers responsible for their policies and actions. Access legislation is one element of this general trend toward greater accountability.

Gerald Baldwin, Q.C., made this point when he told the House of Commons in 1977 that:

> "Open government by a workable freedom of information law will have very definite advantages for this parliament and for the public of Canada. Canadians are entitled to know what the government is doing to or for them, what it is costing them, and who will receive the benefits of the proposals which are made. This parliament will then be a better place."[5]

The Honourable Walter Baker, then President of the Privy Council, reinforced this point when he told the House of Commons on presenting Bill C-15 for Second Reading debate in November, 1979:

> "If this Parliament is to function, if groups in society are to function, if the people of the country are to judge in a knowledgeable way what their government is doing, then some of the tools of power must be shared with the people, and that is the purpose of freedom of information legislation."[6]

Privacy legislation, and more specifically data protection legislation, enables individuals to have some control over what is done with the personal information they provide to government in exchange

for benefits of some kind. This type of measure, with its attendant rights and safeguards, protects individuals by ensuring that they are not subjected to uncontrolled and unaccountable bureaucratic whim.

The 1980 Report of the Ontario Commission on Freedom of Information and Individual Privacy (the Williams Commission) made the following observation:

> "The essence of the informational privacy problem is the loss by individuals of control over the use and dissemination of information concerning their personal lives. The informational privacy value is depreciated when individuals are required to disclose information to another person or institution, and by a loss of control over subsequent uses made of that information. A privacy protection policy intended to preserve informational privacy would therefore attempt to restrict personal data-gathering activity to that which appears to be necessary to meet legitimate social objectives and would attempt to maximize the control that individuals are able to exert over subsequent use and dissemination of information surrendered to institutional record keepers."[7]

Turning the lofty goals of open government and privacy protection into a reality is not easy; it also costs money. The Treasury Board has estimated the annual cost of implementing the Acts to be over $8.4 million.[8] However, these figures must be placed in context. How much does the Government of Canada spend in communicating the information of its choice to the people of Canada? The Treasury Board has indicated to the Committee that in 1984-85 there were 1,330 professional information services officers on the government payroll whose primary function involved communications. The total salary cost was $49.6 million. Advertising, printing, publishing, and so forth involved an actual expenditure in 1984-85 of $289 million. These figures do not include communications expenditures by regional offices of the Government of Canada.[9]

Considering the importance attached by Canadians to open government and the protection of privacy,[10] the cost of implementing the *Access to Information Act* and the *Privacy Act* has not been excessive. This point is reinforced when the costs incurred in administering both Acts is compared with what the Government spends in communicating information of its choice. In addition, experience in other jurisdictions with freedom of information legislation has demonstrated that requests for information sometimes unearth inappropriate spending practices which, when changed, save the taxpayers millions of dollars. Both Acts have had a salutary effect on government record-keeping, leading to greater efficiency and consequent reductions in public expenditures.

The Honourable John Crosbie set out the Government's commitment to effective Access and Privacy legislation when he told the Committee that:

> "Access to Information and Privacy legislation is an area of compelling significance in a free and democratic society such as ours and the government is firmly committed to the basic principles that are the underpinnings of our laws."[11]

The Committee takes the spirit of both Acts—that they extend rights—as its point of departure. We have reviewed the provisions and operation of both Acts with a view to evaluating what has been achieved in the first three years of their operation. Our review has also enabled us to identify a number of emerging and parallel issues which are now beyond the scope of the Acts in their present form but which must be addressed. (See Appendix A for our recommendations.) Other issues concerning technical matters of lesser importance and apparent conflicts between the English and French versions of particular provisions of both Acts are not dealt with in this Report.

END NOTES

[1] S.C. 1980-83, c. 111, Schedules I and II.

[2] *Statement* by the Honourable John C. Crosbie, Minister of Justice and Attorney General of Canada, to the House of Commons Standing Committee on Justice and Solicitor General, May 8, 1986, p. 1.

[3] T.M. Rankin, *Freedom of Information in Canada: Will the Doors Stay Shut*? Canadian Bar Association, Ottawa, August 1977.

[4] Canadian Bar Association, *Freedom of Information in Canada: A Model Bill*, Canadian Bar Association, Ottawa, March 1979.

[5] Canada, House of Commons, *Debates*, December 16, 1977, p. 1954.

[6] Canada, House of Commons, *Debates*, November 29, 1979, p. 1858.

[7] Ontario, Commission on Freedom of Information and Individual Privacy, Report, *Public Government for Private People*, Queen's Printer of Ontario, Toronto, 1980, Vol. 3, p. 667.

[8] Treasury Board of Canada, *Report to the Standing Committee on Justice and Legal Affairs on the Access to Information Act and the Privacy Act*, March 1986, at pp.3 & 6.

[9] Letter to Blaine Thacker, M.P., Chairman of the Standing Committee on Justice and Solicitor General from Pierre Gravelle, Associate Secretary of the Treasury Board, August 26, 1986.

[10] Royal Bank of Canada, *Privacy Study*, Royal Bank of Canada, Public Affairs Department, Montreal, August 1984, Tables 1 and 3, pp.1-4; See also: Neil J. Vidmar, *Privacy and Two-Way Cable Television: A Study of Canadian Public Opinion*, Ontario Ministry of Transportation and Communications, Downsview, Ontario, May 1983, pp. 15-16, 27, 37, 43, and Table 4; and David H. Flaherty, *Protecting Privacy in Two-Way Electronic Services*, Knowledge Industry Publications Inc., White Plains, New York, 1985, pp. 6-7.

[11] *Statement* by the Honourable John C. Crosbie, *Op. Cit.* p.1.

CHAPTER 2

THRESHOLD CONCERNS

Creating a Public Education Mandate

Are Canadians aware of their rights under the *Access to Information Act* and the *Privacy Act*? The volume of requests under the *Access to Information Act* has been much lower than anticipated. There have been in the order of 2,500 requests for information per year under the Act. In her 1986 Special Report to the Committee, the Information Commissioner stated:

> Most people remain unaware of the Act. Many users, as well as those providing services under the Act, do not understand the purpose of the legislation, the need for access rights to be balanced with respect for privacy and the needs of third parties and the government....I have advocated and strongly urge Parliament to recognize the need for public education on access to information and to provide the resources to carry it out.[1]

The Committee has concluded that the people of Canada remain largely unaware of their rights under the *Access to Information Act*.

Government efforts to publicize the access and privacy legislation have been modest, especially when compared with expenditures on publicizing such initiatives as the *Canadian Charter of Rights and Freedoms*, the *Canadian Human Rights Act*, and the *Official Languages Act*. The Information Commissioner has expressed some uncertainty as to the authority of her office to advocate the use of the Act. The Committee notes that other Acts of Parliament, which provide various office holders with analogous functions, contain explicit powers in this regard. For example, the *Canadian Human Rights Act* specifically provides that the Canadian Human Rights Commission "shall develop and conduct information programs to foster public understanding of this Act and of the role and activities of the Commissioner thereunder and to foster public recognition of the principles described in section 2."[2]

The Committee heard evidence to the effect that the Canadian public is also not adequately informed of the rights afforded to it under the *Privacy Act*. Some of the specific investigations undertaken by the Privacy Commissioner further suggest that federal public servants are also not adequately aware of the rules in sections 4 to 8 of the *Privacy Act* concerning the collection and use of personal information. Members of the Committee again contrasted the lack of funds made available to publicize the *Privacy Act* with the large-scale public relations campaigns undertaken on behalf of certain other federal initiatives.

A related problem is the lack of a specific mandate for public education in the *Privacy Act*. The lack of a statutory mandate may explain why the Treasury Board has done relatively little to publicize the Access and Privacy legislation, after an initial flurry of activity at the time of implementation in July, 1983.

Recommendations:

2.1 The Committee recommends that, for purposes of clarification, the *Access to Information Act* and the *Privacy Act* mandate that the Treasury Board, the Information Commissioner, and the Privacy Commissioner foster public understanding of the *Access to Information Act* and the *Privacy Act* and of the principles described in section 2 of each Act. Such education should be directed towards both the general public and the personnel of government institutions. The appropriate provision in the statutes should follow the model of section 22 of the *Canadian Human Rights Act*.

2.2 The Committee further recommends that the Treasury Board undertake a public education campaign in conjunction with the proclamation of any amendments to the *Access to Information Act* and the *Privacy Act* and also consider printing notices about individual rights under both the *Access to Information Act* and the *Privacy Act* to be included in standard government mailings.

Coverage of Federal Government Institutions, Administrative Tribunals and Parliament

At present, the *Access to Information Act* and the *Privacy Act* apply only to those "government institutions" listed in a Schedule to the legislation. Departments and Ministries of State are listed, as are certain other government agencies. As a result, it is difficult for applicants without an up-to-date copy of the Schedules to know precisely what parts of the Government of Canada are subject to the legislation. This is a cumbersome drafting device causing continuing work and frustration for both the Treasury Board and the Department of Justice. The need to amend the Schedules on a regular basis to reflect changes in government organization is an unproductive and wasteful activity. The Committee prefers to design a system in which all government institutions are covered by the respective statutes.[3]

Neither Act contains a general definition of "government institution"; as a result, the two Acts do not apply automatically to newly-created institutions. Whenever a new agency is created, it must be added to the Acts by regulation. Sometimes an agency will be forgotten.

What government institutions are currently excluded from the ambit of the *Access to Information Act* and *Privacy Act*? The Ontario Commission on Freedom of Information and Individual Privacy (the Williams Commission) recommended in its 1980 Report that freedom of information legislation in that province should apply "to those public institutions normally perceived by the public to be part of the institutional machinery of the ... government." But in a modern state like Canada, what does the term "government" include? In addition to departments, agencies, commissions and Crown corporations, should the Acts also apply to agricultural marketing boards, the House of Commons, the Senate, the Library of Parliament, and the offices which are directly accountable to Parliament, such as the Chief Electoral Officer, the Official Languages Commissioner, the Auditor-General, the Information Commissioner, and the Privacy Commissioner?

The Committee agrees with the Ontario Commission on Freedom of Information and Individual Privacy that freedom of information and privacy legislation should apply to those public institutions normally perceived by the public to be part of the institutional machinery of government.[4] It has concluded that two alternative criteria should be employed to identify the institutions of the federal government which should be subject to the *Access to Information Act* and the *Privacy Act*. Firstly, if public institutions are exclusively financed out of the Consolidated Revenue Fund, they should be covered. Secondly, for agencies which are not financed exclusively in this way, but can raise funds through public borrowing, the major determinant should be the degree of government control. (Crown corporations are covered in a separate recommendation.)

The Committee recognizes that certain institutions that are perceived by the public to be part of the federal government are in fact joint ventures with provincial governments. Examples include the Canadian Egg Marketing Agency, the Canadian Dairy Marketing Agency, and the Canadian Broiler Chicken Marketing Agency. The Committee is aware that extending coverage of the *Access to Information Act* and the *Privacy Act* to such organizations may require consultation with the provinces but believes that the public interest will be best served by the successful conclusion of such negotiations in order to ensure coverage by the *Privacy Act*.

The Committee believes that the *Privacy Act* should extend to all federal courts and administrative tribunals, since officers and employees of such institutions should enjoy the same rights to protect their privacy as are enjoyed by other federal officers and employees. However, the

Committee agrees with the approach taken in most other jurisdictions and would not extend the *Access to Information Act* to cover the judicial branch of government. Accordingly, the Federal Court, the Supreme Court of Canada, and the Tax Court of Canada should continue to be excluded from the ambit of the *Access to Information Act*.

The coverage of the personal offices of Members of the House of Commons and Senators presents several special problems. Since the relationship between such elected and appointed officials and the electorate is sometimes described as akin to solicitor-client privilege, and parliamentary privilege is involved, the Committee suggests their continued exclusion from the scope of the *Access to Information Act*.

The *Privacy Act* presents a different issue, since it is arguable that employees of Members of the House of Commons and Senators should have the same rights of access to data collected about them as other government employees. On balance, the Committee concludes that it would be preferable to include these offices, for such specific purposes, within the coverage of the *Privacy Act*, just as they are already subject to the *Canadian Human Rights Act*.

Recommendations:

2.3 The Committee recommends that all federal government institutions be covered by the *Access to Information Act* and the *Privacy Act*, unless Parliament chooses to exclude an entity in explicit terms. Thus the Committee recommends the repeal of Schedule I to the *Access to Information Act* and the Schedule to the *Privacy Act*. The criteria for inclusion should be as follows: Firstly, if public institutions are exclusively financed out of the Consolidated Revenue Fund, they should be covered. Secondly, for agencies which are not financed exclusively in this way, but can raise funds through public borrowing, the major determinant should be the degree of government control.

2.4 The Committee recommends that the *Access to Information Act* cover all federal government institutions, including all administrative tribunals, the Senate, the House of Commons (but excluding the offices of Senators and Members of the House of Commons), the Library of Parliament, and such offices directly accountable to Parliament as the Auditor General, the Official Languages Commissioner, the Chief Electoral Officer and the Office of the Information and Privacy Commissioners. The criteria for inclusion should be as follows: Firstly, if public institutions are exclusively financed out of the Consolidated Revenue Fund, they should be covered. Secondly, for agencies which are not financed exclusively in this way, but can raise funds through public borrowing, the major determinant should be the degree of government control.

2.5 The Committee recommends that the *Privacy Act* cover all federal government institutions, the Supreme Court of Canada, the Federal Court of Canada, the Tax Court of Canada, all administrative tribunals, the Senate, the House of Commons (including the employees only of Senators and Members of the House of Commons), the Library of Parliament, and such offices directly accountable to Parliament as the Office of the Information and Privacy Commmissioners . The criteria for inclusion should be as follows: Firstly, if institutions are exclusively financed out of the Consolidated Revenue Fund, they should be covered. Secondly, for agencies which are not financed exclusively in this way, but can raise funds through public borrowing, the major determinant should be the degree of government control.

Coverage of Crown Corporations

Federal Crown corporations of a commercial nature are excluded from both Acts. Such corporations are owned or financially controlled by the Government of Canada. They are involved in

transportation, energy, communications and other fields. Often the Government's choice to establish a Crown corporation, as opposed to a more traditional government department or agency, represents purely a choice among different instruments of public policy. To subject most Crown corporations to the Acts, as the Committee recommends, would enhance their accountability to the Canadian public. Their legitimate secrets would be adequately protected under the various exemptions set out in the *Access to Information Act*, particularly sections 18 and 20, which deal with the matters affecting the economic interests of Canada and confidential business information.

Since its passage in 1969, Crown corporations have been subject to the *Official Languages Act*. When the *Financial Administration Act* was amended in 1984, it had the effect of bringing federally incorporated, wholly-owned subsidiaries of Crown corporations under that law.[5]

Following the format of the Treasury Board's Annual Report to Parliament on Crown corporations under the *Financial Administration Act*, the Committee recommends that the *Access to Information Act* and the *Privacy Act* cover all 53 parent crown corporations and their 127 wholly-owned subsidiaries; the majority of these are owned by CNR and Petro-Canada. As of July 31, 1986, they employed 187,000 people and had total assets of $55 billion.[6]

The Committee deems it impractical at this stage to extend the coverage of the *Access to Information Act* and the *Privacy Act* to certain other Crown corporations. Those not to be covered include 140 subsidiaries of Crown corporations which are not wholly-owned as well as 26 "joint and mixed enterprises" which have share capital owned jointly with other governments and/or other organizations (e.g. Telesat Canada). Finally, there are other entities without share capital for which the Government of Canada, either directly or through a Crown corporation, has a right to appoint one or more members of the Board of Directors or similar governing body (e.g., the various Harbour Commissions, Hockey Canada Inc., and the Vanier Institute of the Family).[7]

The Committee is of the general view that all wholly-owned Crown corporations and their wholly-owned subsidiaries should be covered by the *Access to Information Act* and the *Privacy Act*.[8] As the Privacy Commissioner stated to the Committee, "The first—and easy—step in extending the coverage of the *Privacy Act* should be to bring in these Crown corporations which had been allowed to claim exemption on the grounds of competitive disadvantage. Indeed, collective agreements in some Crown corporations not covered by the Privacy Act already give employees access to their own personal information. Such agreements or not, government institutions, because they are government, should set the highest standards of privacy protection.... Why should Canada Post be covered by the Privacy Act and not, say, the CNR? Why National Film Board and not the CBC?"[9] This view was supported in testimony before the Committee from the Canadian Bar Association, *La Ligue des droits et libertés*, the Social Science Federation of Canada, and the Canadian Rights and Liberties Federation.[10]

In March, 1986, the Government of Ontario expanded the scope of Bill 34, an Act to provide for Freedom of Information and Protection of Individual Privacy, to cover all Crown corporations, including the Liquor Control Board of Ontario, Ontario Hydro and the Ontario Lottery Corporation.[11] The Bill currently contemplates doing this by designating such organizations as "institutions" in the proposed regulations under the Act.[12]

A definition of Crown corporations should be developed for purposes of the *Access to Information Act* and *Privacy Act*. In principle, the Committee wants to include corporations in which the government has a *de facto* controlling interest and which provide goods or services to the public on a commercial or quasi-commercial basis.[13]

The Canadian Broadcasting Corporation argued in a Brief to the Committee that the application of the *Access to Information Act* and *Privacy Act* to the CBC would stifle the dissemination of information—which is its central mandate—for several reasons. It claimed that sources of information would dry up and applications would be made under the Acts in an effort to prevent the broadcasting of information. Several other similar claims were advanced. Although the Committee does not accept

the CBC's position entirely in this regard, it agrees that the wholesale application of the Acts to the CBC might impair its newsgathering function. It notes that the Australian *Freedom of Information Act* does not apply to the Australian Broadcasting Corporation in relation to program material. In other respects, however, this Crown corporation is subject to the Australian legislation. Such a compromise would appear appropriate in the Canadian setting as well.

Recommendations:

2.6 The Committee recommends that the *Access to Information Act* and the *Privacy Act* be extended to cover those Crown corporations and wholly-owned subsidiaries as are listed in the Treasury Board's *Annual Report to Parliament on Crown Corporations and Other Corporate Interests of Canada.* For this purpose, the Committee recommends that the *Access to Information Act* and the *Privacy Act* be amended to include such a definition of "Crown corporation".

2.7 The Committee further recommends that if the Government of Canada controls a public institution by means of a power of appointment over the majority of the members of the agency's governing body or committee, then both the *Access to Information Act* and the *Privacy Act* should apply to such an institution.

2.8 The Committee recommends that, with respect to the Canadian Broadcasting Corporation (CBC), the *Access to Information Act* not apply in relation to program material; otherwise, the Corporation should be fully subject to both the *Access to Information Act* and the *Privacy Act.*

The Status of Applicants

Who should be able to use the *Access to Information Act* and the *Privacy Act*? Presently the right of access under both Acts is available only to individuals who are either Canadian citizens or permanent residents within the meaning of the *Immigration Act, 1976*. Both Acts contemplate a possible extension by the Governor in Council to include other persons. No such extension has been granted to date under the *Access to Information Act*. In 1983, the right of access to personal information under the *Privacy Act* was extended to all inmates incarcerated in Canadian prisons.

It seems unnecessary and undesirable to limit the Access and Privacy legislation in this fashion. Organizations outside Canada can easily obtain the services of a qualified individual in Canada to apply on their behalf. The Committee notes than under the U.S. *Freedom of Information Act* the right of access to government records is available to any person without restriction. We are of the view that creating reciprocal rights of access in Canada would be appropriate at this time, particularly in light of the major bilateral initiatives currently underway between the Governments of Canada and the United States.

In addition, corporations, trade unions and other organizations are not allowed to use the *Access to Information Act* as it is presently drafted. As a result, individuals are now required to apply on behalf of these legal entities. It seems unnecessary for this rather technical limitation to continue. There appears to be no good reason, for example, why a corporation or trade union seeking government records should have to call upon an agent in order to invoke the statutory right of access under the Access legislation.

Most data protection laws do not restrict the right of access solely to citizens or residents of the country in question. Such legislation simply grants the right of access to "persons", "individuals", or "data subjects" without any further restriction. This is true for Quebec's 1982 Act, Ontario's Bill 34, the German *Federal Data Protection Act* of 1977, the United Kingdom's *Data Protection Act* of 1984, the French *Data Protection Law* of 1978, and the Swedish *Data Act* of 1982.[14]

At the first U.S. *Privacy Act* oversight hearings in 1983, both the Office of the United States Trade Representatives and the Department of State indicated that they favoured granting access rights to foreigners under both laws "in line with foreign data protection laws."[15] However, at present, foreigners do not have the right of access and the right to correct files.

The Privacy Commissioner has recommended to the Committee that "privacy rights should be extended to all persons in Canada, not limited to Canadian citizens and permanent residents."[16] His recommendation would apply to any person applying from within the boundaries of Canada. The Committee's view is that such access rights should be available to anyone about whom the federal government has collected personal information, since, as the Commissioner has argued, "persons with non-resident status are often affected profoundly by administrative decisions of federal government institutions."

Recommendations:

2.9 The Committee recommends that any natural or legal person be eligible to apply for access to records under the *Access to Information Act*. The location of the applicant should no longer be relevant. Corporations, non-profit associations, employee associations, and labour unions should also be able to avail themselves of this legislation.

2.10 The Committee further recommends that section 12(1) of the *Privacy Act* be amended so that access and correction rights for their own personal information are available to all individuals, regardless of citizenship or residence.

Access Tools

Under section 5 of the *Access to Information Act* and section 11 of the *Privacy Act*, the Treasury Board is responsible for producing guides for users entitled the *Access Register* and the *Personal Information Index*. They are updated by a *Bulletin*, published twice a year.

The Committee heard from many witnesses who testified that although the *Access Register* had been improved, it remains vague and difficult to understand. For example, the Consumers' Association of Canada termed the *Register* "useless" and indicated that "the description of records in the Register reveals little information."[17] The Department of Communications also noted in its Brief that "the Access Register is still a very broad description and not too helpful in locating the precise documents desired. It is our practice to phone [users] for further specifications."[18] In addition, the Index to the *Register* remains unclear in several places.

The President of the Treasury Board has indicated the production of the *Access Register* and the *Personal Information Index* involves a direct cost of $0.5 million annually for publication and distribution, and several times this cost in the staff time required within government institutions to inventory and describe their record holdings. He further testified that only a small proportion of access requests even made reference to the *Access Register*.

The Ministerial Task Force on Program Review (the Nielsen Task Force) suggested that consideration be given to an omnibus publication which would combine the *Access Register* with such other government publications as the *Organization of the Government of Canada* and the *Index of Programs and Services*.[19] There is much merit in this suggestion. An omnibus publication of this sort could provide potential users with more detail, so that access requests might identify the specific record sought more effectively.

Since the *Access Register* and the *Personal Information Index* are already produced from a computerized inventory of information, it should be possible to extract portions in the form of a customized directory, which would be of assistance to specific user groups. For example, applicants

concerned with Indian, Inuit, or Métis issues would benefit from the production of a concise directory which lists only those classes of records kept in the Department of Indian and Northern Affairs and perhaps in one or two other institutions, such as the Departments of National Health and Welfare and Regional Industrial Expansion. For this category of applicant, it may be unnecessary to produce the entire *Access Register* and *Personal Information Index*. Environmental associations, consumer groups, and veterans' organizations may have relatively limited requirements, which could be amply served by a more concise index to government record holdings. Similarly, inmates of correctional institutions ordinarily would not need to have the entire *Personal Information Index* in order to look up the information banks pertaining to them.

Since both the *Access Register* and the *Personal Information Index* are produced from an automated data base, it would be appropriate and helpful for the Treasury Board to allow users to have access to the data in them on an on-line basis and/or through their sale in digital form for use on computers.

Recommendations:

2.11 The Committee recommends that the *Access Register* be combined with such other government publications as the *Index of Programs and Services* and the *Organization of the Government of Canada.*

2.12 The Committee further recommends that this omnibus access tool and the *Personal Information Index* be made available by the Treasury Board and individual government institutions on an on-line basis and/or through their sale in digital form for use on computers.

2.13 The Committee further recommends that the Treasury Board and individual government institutions make available segments of these various user guides on a customized basis to suit the needs of particular user groups.

The Responsibilities of Access and Privacy Coordinators

The heads of government institutions are ultimately responsible for the implementation of the *Access to Information Act* and the *Privacy Act*. In practice, government institutions have Access and Privacy Coordinators on either a full- or part-time basis, whose primary responsibility tends to be the handling of requests for access to government records and personal information. On occasion, the Coordinators perceive a conflict between their responsibilities under this legislation and their career prospects in the government institution employing them. There is thus a problem of how best to protect their careers and to provide them with some measure of independence and effective training. The Committee believes that the offices of Coordinators must become the primary agents for promoting effective implementation of the *Access to Information Act* and the *Privacy Act* within each government institution.

The Privacy Commissioner has encapsulated the difficult roles of the Coordinators, whom he describes as the "privacy professionals":

> Theirs is a difficult role. They have divided loyalties, pulled on the one side to their own department where their careers are at stake, on the other to the Privacy Act and to fair information practices. Sometimes the two roles are difficult to reconcile, and that, of course, is inevitable.
>
> Not inevitable is the lack of support given to some privacy co-ordinators by their superiors. Some co-ordinators are even reluctant to press their concerns with departmental lawyers lest they be considered disloyal. Nor, as a group, do they seem influential as the privacy consciences of their departments. Many of them are not in the mainstream of their organization. The position of co-ordinator is not yet generally seen as desirable for career progress.[20]

His comments apply with equal force to Coordinators in the discharge of their responsibilities under the *Access to Information Act*.

An alternative model for more effective administration of the Acts within government institutions deserves consideration. In 1975, the U.S. Department of Defense set up a Defense Privacy Board, headed by the Deputy Assistant Secretary of Defense for Administration, and a Defense Privacy Office, comprised of three professional staff and a secretary. The director of the latter office is the Executive Secretary of the Defense Privacy Board. These persons and groups are responsible for the interpretation and implementation of the U.S. *Privacy Act* of 1974 in the Department of Defense. It is unfortunate that no Canadian federal institution has set up a comparable office designed to ensure the effective implementation of the *Access to Information Act* and the *Privacy Act*.

The current training of Access and Privacy Coordinators appears to be deficient in the sense that no regular government-wide program exists, except for the admirable *ad hoc*, cooperative efforts of the Administrative Policy Branch of Treasury Board and the Office of the Information and Privacy Commissioners. The latter involves six to eight courses a year for senior managers at a training centre during which actual cases are considered. The Treasury Board also carries out *ad hoc* training for government institutions which have a significant case load.

The Committee urges the Treasury Board to organize standard, formal training for new Access and Privacy Coordinators, perhaps using automated training modules, audiovisuals, and films. The U.S. Office of Management and Budget, which has statutory responsibilities comparable to the Treasury Board, places the burden for such training on the Office of Personnel Management (formerly the Civil Service Commission).[21] The Treasury Board might choose to enter into arrangements for such training tasks with the Public Service Commission of Canada. The Board could structure the training programs on the *Access to Information Act* and the *Privacy Act*, preferably as a standard part of departmental training in most instances, and then arrange for the Public Service Commission to offer the courses on a cost recovery basis.

Another relevant United States model exists in the area of training programs. In 1981-82 the U.S. Defense Department, through its Defense Privacy Office, and in cooperation with the Department of Health and Human Services, created its own training program on the *Privacy Act* for managers, who were taught initially by Privacy Office staff.[22] The goal should be to train local managers to offer training programs themselves.

Canadian government institutions should be encouraged to cooperate with each other for training purposes. The Royal Canadian Mounted Police and Revenue Canada, Taxation are candidates for leadership roles in this regard, since they are known to have created effective training programs for internal use. Revenue Canada, Taxation conducts training courses and refresher training sessions for its own staff concerning the *Access to Information Act* and the *Privacy Act*. These sessions employ case studies drawn from actual taxpayer files. Revenue Canada is currently planning to distribute a pamphlet in question and answer form on both Acts to all employees. In 1985, its Access to Information and Privacy Division conducted Executive Briefing Seminars in seven cities across Canada at the request of the Canadian Institute of Chartered Accountants.

The Committee applauds the initiative that Access and Privacy Coordinators themselves have taken in recent months in organizing a Federal Access and Privacy Association as a Canadian counterpart to the American Society of Access Professionals (ASAP), which offers training and education to U.S. federal government employees on both the *Privacy Act* and the *Freedom of Information Act*.

As a result of the Committee's hearings, the Treasury Board in 1986 conducted a survey of the roles and job satisfaction of Access and Privacy Coordinators in order to better understand their current problems. This involved a free-form discussion with fifteen Coordinators and staff advisors and the preparation of a Report by the Treasury Board.[23]

This Treasury Board Report confirmed a number of the Committee's concerns. All Coordinators "agreed that *the coordination role needed strong senior management support* through direct access to the deputy minister or a senior assistant deputy minister." This could be accomplished either by attaching the Access to Information and Privacy (ATIP) office to, or having it report through, that of the deputy minister or assistant deputy minister, or by designating a senior official with direct access to those officials as Coordinator. Coordinators felt a need for continuing senior management involvement and support to ensure that program managers effectively responded to ATIP demands. They also needed direct access to senior program officials to expedite requests and ensure sensitivity to ATIP legal and policy requirements. In addition, the accountability of senior program officials for direction on the handling of ATIP requests needed to be established.

The 1986 Treasury Board Report also noted the Coordinators' belief that the Treasury Board should update its requirement statement concerning the role of Coordinators, especially in such areas as information collection policy, information inventories, privacy protection, and security issues. The Coordinators were also concerned that senior management in government institutions did not fully appreciate the expanding scope of the ATIP Coordination role:

> In general, coordinators felt that there is a need for senior government officials to come to grips with the reality of Access and Privacy legislation, and to recognize that this represents a fundamental change in the conduct of public affairs affecting all stages in the treatment of government information, from creation to disposal, with implications well beyond the administrative processing of requests.[24]

The Treasury Board Report also addressed issues concerning the level, classification of staff, and training of administrative support staff in ATIP units. Finally, some Coordinators wanted the Treasury Board and the Department of Justice to become more active in central coordination and policy leadership on issues with government-wide implications.

The Committee makes the following recommendations to secure and enhance the critically-important roles of Access and Privacy Coordinators.

Recommendations:

2.14 The Committee recommends that the status and role of Access and Privacy Coordinators be given explicit recognition in section 73 of the *Access to Information Act* and section 73 of the *Privacy Act*, since they are the prime movers for implementation of the legislation within government institutions.

2.15 The Committee recommends, in light of the Treasury Board's 1986 consultation with Access and Privacy Coordinators, that the Treasury Board directly address the problem of ensuring that Coordinators, who should be senior level officials wherever possible, have direct reporting and working relationships with senior management and senior program officials of government institutions in order to ensure necessary support for, and understanding of, their complicated, demanding, and expanding tasks in information management. The Treasury Board should also update its requirement statement concerning the role of Coordinators, especially in such areas as information collection policy, information inventories, privacy protection, and security issues.

2.16 The Committee recommends that the Treasury Board organize standard, formal training for Access and Privacy Coordinators, perhaps using automated training modules, audiovisuals, and films.

2.17 The Committee further recommends that the Treasury Board and the Department of Justice become more active in central coordination and policy leadership on issues with government-wide implications for Access and Privacy legislation.

END NOTES

[1] Information Commissioner, *Special Report*, (Ottawa, 1985), p. 3.

[2] *Canadian Human Rights Act*, S.C. 1976-77, c. 33, s. 22(1)(a).

[3] Based on the current schedules, this would and should include administrators, administrations, advisory boards, agencies, archives, authorities, [federal] boards of trustees, bodies, bureaus, centres, commissions, councils, crown corporations, departments, directorates, institutes, libraries, ministries of state, mints, museums, offices, police, research centres, research councils, review boards, secretariats, services, statistical agencies, and tribunals, or such-like bodies.

[4] This was done in the *Public Sector Compensation Restraint Act*, S.C. 1980-83, c. 122.

[5] President of the Treasury Board, *Annual Report to Parliament on Crown Corporations and Other Corporate Interests of Canada; Public Accounts of Canada, 1986*, III (Ottawa, 1986), iii.

[6] *Ibid.*, III, iii. Statistics Canada reported that government-owned companies employed 208,134 persons in September 1986 (*The Globe and Mail*, Jan. 2, 1987).

[7] *Ibid.*, III, 370.

[8] Some examples of Crown corporations already covered in the Schedule to the *Privacy Act* (and the *Access to Information Act*) are the following: the Bank of Canada, Canada Deposit Insurance Corporation, Canada Mortgage and Housing Corporation, Canada Ports Corporation, Canada Post Corporation, Export Development Corporation, Farm Credit Corporation, Federal Business Commission, National Film Board, Northern Canada Power Commission, Royal Canadian Mint, the St. Lawrence Seaway Authority, and Uranium Canada Ltd.

The following Crown corporations are not currently covered by the *Privacy Act*: Air Canada, Atomic Energy of Canada Ltd., Canada Harbour Place Corporation, Canada Lands Company Ltd., Canada Museums Construction Corporation Inc., Canadian Broadcasting Corp., Canadian National Railway Company, Canadian National (West Indies) Steamships Ltd., Canadian Sports Pool Corporation, Cape Breton Development Corporation, Halifax Port Corporation, Harbourfront Corporation, Loto Canada Inc., Mingan Associates, Ltd., Montreal Port Corporation, Petro Canada, Port of Quebec Corporation, Prince Rupert Port Corporation, St. Anthony Fisheries Ltd., Societa a responsibilita limitate Immobiliare San Sebastiano, Vancouver Port Corporation, and VIA Rail Canada Inc. Thus the *Privacy Act* would be extended to 27 of the 57 Crown corporations on the Treasury Board list. (President of the Treasury Board, *Annual Report to Parliament on Crown Corporation and Other Corporate Interests of Canada*, III, vii-viii.)

[9] Privacy Commissioner, *Annual Report 1985-86* (Ottawa, 1986), pp. 10-11; *Minutes of Proceedings and Evidence of the Standing Committee on Justice and Solicitor General*, Issue No. 11 (May 13, 1986): 9, 31. (Hereafter cited as *Hearings*)

[10] *Hearings*, 13:35, 20:20, 22:18, 28:8.

[11] *The Globe and Mail*, March 26, 1986, p. 1.

[12] Ontario's Bill 34, An Act to provide for Freedom of Information and Protection of Individual Privacy, defines "institution" in section 2 as "any agency, board, commission, corporation or other body designated as an institution in the regulations."

[13] See: President of the Treasury Board, *Annual Report to Parliament on Crown Corporations and Other Corporate Interests of Canada*, III, 13.

[14] See: Quebec, *An Act respecting Access to documents held by public bodies and the Protection of personal information*, R.S.Q., c. A-2.1, article 83; Ontario, Bill 34, An Act to provide for Freedom of Information and Protection of Individual Privacy, 1986, section 43; West German *Act on Protection against the Misuse of Personal Data in Data Processing of January 27, 1977*, s. 4, French *Act 78-17 of January 6, 1978 on Informatics, Data Banks, and Freedoms*, c. 5; *Data Protection Act* 1984, c. 35, s. 21 (U.K.); Sweden, *Data Act*, 1982, ss. 22-23.

[15] *Oversight of the Privacy Act of 1974*, Hearings before a Subcommittee of the Committee on Government Operations, House of Representatives, 98th Congress, June 7 and 8, 1983 (Washington, D.C., 1983), p. 600.

[16] *Hearings*, Issue No. 11 (May 13, 1986): 9; Privacy Commissioner, *Annual Report 1985-86*, p. 24.

[17] *Brief* of the Consumers Association of Canada, pp. 5-6.

[18] *Brief* of the Department of Communications, p. 3.

[19] See Canada, *Organization of the Government of Canada 1980* (Ottawa, 1980), and Canada, *Index to Federal Programs and Services 1986*, (7th ed., Ottawa, 1986).

[20] Privacy Commissioner, *Annual Report 1985-86*, p. 25.

[21] Circular A-130, *Federal Register*, Vol. 50, No. 247 (Dec. 24, 1985), 52739.

[22] *Oversight of Computer Matching to Detect Fraud and Management in Government Programs*, Hearings before the Subcommittee on Oversight of Government Management of the Committee on Governmental Affairs, United States Senate, 97th Congress, 2nd Session, 15-16 December 1982 (Washington, DC: Government Printing Office, 1983), pp. 149-51.

[23] Treasury Board, *Review of Access to Information and Privacy Coordination in Government Institutions*, (1986), submitted to the Standing Committee on Justice and Solicitor General.

[24] *Ibid.*

CHAPTER 3

EXEMPTIONS AND CABINET CONFIDENCES: SAYING NO

Perhaps the most crucial part of any access to information or data protection statute is the series of exceptions to the rule of openness or privacy protection which it contains. A series of exemptions protects a variety of interests, both governmental and non-governmental. If either a record or personal information—or part thereof—comes within a specific exemption, then the government will be justified—or in some cases required—to refuse disclosure of all or part of the information sought. The government institution, however, must cite the statutory ground in the *Access to Information Act* or *Privacy Act* upon which the exemption is based or would be based if the record existed. At present, the department or agency is not required to confirm whether a particular record or specific personal information actually exists, since disclosure of its existence or non-existence may be the exact thing that needs to be withheld. Each government institution must "sever" exempted portions of records and provide access to the rest—solely, however, under the *Access to Information Act*.

Exemptions are very difficult to draft; however, the precise terms used in the statute are crucial in determining how open the government must be. The Department of Justice has clearly set out the drafting issue:

> The exemptions are based on either an "injury test" or "class test." Some exemptions are discretionary, while others are mandatory. Exemptions which incorporate an "injury test" take into consideration whether the disclosure of certain information could reasonably be expected to be injurious to a specified interest. Information relating to activities essential to the national interest, the security of persons or their commercial affairs are examples. "Class exemptions" refer to a situation in which a category of records is exemptable because it is deemed that an injury could reasonably be expected to arise if they were disclosed. An example of this is information obtained in confidence from the government of a province or an institution thereof.
>
> Discretionary exemptions allow the head of a government institution to decide whether the exemption needs to be invoked. Mandatory exemptions provide no discretion to the head of the government institution, and must be invoked.
>
> ... The confidences of the Queen's Privy Council for Canada [in practical terms, the Cabinet] that have been in existence less than twenty years are excluded from the provisions of the Act by virtue of section 69. Unlike the decision to apply an exemption, the decision to exclude records, pursuant to section 69 is not subject to review by the Information Commissioner or the Federal Court, and neither the Information Commissioner nor the Federal Court has the authority to examine such documents.[1]

The Information Commissioner has reported that some records are being withheld under mandatory exemptions where no harm would arise from their release.[2] In an important court decision,[3] Associate Chief Justice Jerome was called upon to consider the application of a discretionary exemption in the *Access to Information Act*. The court held that once it determined that a record came within the class of records referred to in this particular discretionary exemption [sec. 21(1)], the right of the applicant to disclosure is subject to the discretion of the government institution. Moreover, the court decided that in such circumstances, it will not review the exercise of discretion by the government institution, once it had determined that the record indeed falls within the exempt class of records. It was irrelevant that the Information Commissioner in that case had reviewed the record and was arguing for its disclosure—presumably trying to persuade the government institution that no injury would result from its release.

The Committee is very concerned about a situation in which harmless records are being withheld under statutes designed to promote disclosure. It is likewise concerned about the existence of mandatory exemptions in the two Acts, under which government officials "shall" maintain secrecy—even though no discernible injury might result from the disclosure of particular records. Accordingly,

major revisions in the drafting of the exemptions are considered vital to the credibility of this legislation. All exemptions should be discretionary in nature. They should also generally contain an "injury test", so that the government institution is required to demonstrate in each case the kind of harm that could reasonably be expected to occur as a result of disclosure.

Finally, as a general rule, each exemption should stipulate that the degree of injury resulting from disclosure must be "significant": accordingly, each exemption should be drafted so that the head of a government institution "may" withhold records or personal information "the disclosure of which could reasonably be expected to be *significantly* injurious" to a stated interest. When balancing competing interests, therefore, the Commissioners and the Federal Court should lean in favour of disclosure unless they are convinced that significant injury would result.

Recommendation:

3.1 The Committee recommends that subject to the following specific proposals, each exemption contained in the *Access to Information Act* and *Privacy Act* be redrafted so as to contain an injury test and to be discretionary in nature. Only the exemption in respect of Cabinet records (which is proposed later in this Report) should be relieved of the statutory onus of demonstrating that significant injury to a stated interest would result from disclosure. Otherwise, the government institution may withhold records or personal information only "if disclosure could reasonably by expected to be significantly injurious" to a stated interest.

A. Specific Exemptions

Information Obtained in Confidence From Other Governments

Section 13 of the *Access to Information Act* and section 19 of the *Privacy Act* at present contain a mandatory class exemption for records and personal information that were "obtained in confidence" from other governments. The need for this exemption is indisputable. It should not be possible to apply to the federal government for and obtain access to personal information and records in its possession which were provided in confidence by other governments. The applicant should, in principle, seek records and personal information from these other jurisdictions by applying to them directly. Thus, records provided to the federal government by the Government of New Brunswick, for example, should be sought from New Brunswick under its *Right to Information Act*. Not all provinces, however, have access to information legislation.

Section 19(1)(c) of the *Privacy Act* bars individuals from obtaining access to personal information obtained in confidence from "the government of a province or an institution thereof." Testimony before the Committee indicates that this subsection has created problems, since certain provinces have asked the federal government to treat all information it receives from them as confidential. As the Privacy Commissioner stated to this Committee:

> What is not defensible are the blanket claims of confidentiality which have been claimed by some provinces for all information they pass on to the federal government. In a federal state, a vast amount of personal information is exchanged from one level of government to another. When a province unilaterally imposes confidentiality upon all information it shares with the federal government, as some have done, significant amounts of personal information are automatically exempted from access. As the Privacy Act is now written, the federal government institution receiving personal information from a province which has insisted upon a blanket of confidentiality has no discretionary power. The instruction of section 19 is absolute:
> 'The head of a government institution *shall* refuse to disclose'[4]

The Committee agrees with the Privacy Commissioner that it is "profoundly damaging to the credibility of the Privacy Act if confidentiality claims are not made for good and sufficient reasons".[5]

Since only the Province of Quebec currently has legislation comparable to the *Privacy Act*, residents of the other nine provinces cannot be assured of access to their personal information contained in provincial files. This situation, of course, will change to the extent that other provinces adopt data protection legislation, such as Bill 34 which is pending before the Ontario Legislature. The Committee strongly favours the adoption of such data protection legislation by each of the provinces.

Nevertheless, the Committee recognizes that under current practice the control of personal data originating in a province generally remains a provincial responsibility. However, the present situation is unsatisfactory. As the Privacy Commissioner, among others, has pointed out: "Section 19 remains a major source of frustration to applicants for personal information and to the administration of the *Privacy Act*."[6] He found that departments' use of this section is "the single greatest blockage to release of personal information." Moreover, the Commissioner "found no procedures on the part of government institutions to determine whether or not information received from the provinces was obtained or received in confidence beyond the invoking of the blanket agreements with the provinces. These are the agreements which so often now frustrate the release of any information the federal government receives from the provinces."[7]

The Committee applauds the progress made by the Privacy Commissioner and the Solicitor General in achieving cooperation with the provinces of Quebec, Prince Edward Island and British Columbia in the reciprocal application of section 19(1)(c) of the *Privacy Act* concerning law enforcement information. In a laudable agreement, these provinces have accepted that personal information received from them will be treated as federally-generated personal information and that the provisions of the *Privacy Act* will apply.[8] Such law enforcement information evidently constitutes a substantial proportion of the information exchanged between the two levels of government.

The Committee believes that section 13 of the *Access to Information Act* and section 19 of the *Privacy Act* should be redrafted to allow for a discretionary, injury-tested exemption. It is recognized, however, that the records and personal information provided by other governments to a government institution are as important to them as the commercial information provided to a government institution by third parties is to these companies and individuals. The Committee therefore has concluded that other governments should have rights of notification and review similar to those accorded to third parties by sections 28, 29 and 44 of the *Access to Information Act*.

At present, some confusion has arisen as to whether U.S. state governments are included in section 13(1)(a) of the *Access to Information Act* and section 19(1)(a) of the *Privacy Act*. Both the *Access to Information Act* and the *Privacy Act* should be amended to clarify that the agencies or governments at the state or provincial level in other countries should be explicitly covered by this exemption. Similarly, the exemptions should clarify that institutions of native self-government, such as the Sechelt Indian Government District in British Columbia, should be accorded the same treatment as other governments under the two Acts.

Recommendations:

3.2 The Committee recommends that the exemption contained in section 13 of the *Access to Information Act* and section 19 of the *Privacy Act* be redrafted to be discretionary in nature and to contain an injury test. In addition, the exemption should permit other governments to be notified of an application for the disclosure of records or personal information that they have submitted in confidence and also permit them to dispute recommendations for the release of such information before the Information Commissioner or Privacy Commissioner and the Federal Court. The burden of proof in such cases should be placed upon the other governments. Where foreign governments are concerned, a time period of three months should be allowed for response and the Secretary of State for External Affairs should be served with the notice of application.

3.3 The Committee further recommends that section 13 of the *Access to Information Act* and section 19 of the *Privacy Act* be redrafted to clarify that institutions or governments of component elements of foreign states (such as State governments in the United States and their agencies) are included for purposes of this exemption.

3.4 The Committee further recommends that section 13 of the *Access to Information Act* and section 19 of the *Privacy Act* be amended so that institutions of native self-government are accorded the same protection as other governments for purposes of this exemption.

3.5 The Committee recommends that the Privacy Commissioner be requested to continue monitoring the exchange of personal information between the provinces and the federal government in order to promote the uniform reciprocal application of fair information practices.

Federal-Provincial Affairs

The Committee notes that Bill C-15, the 1979 Progressive Conservative Government's freedom of information Bill, formulated this exemption in a somewhat narrower fashion. Instead of the term "affairs", Bill C-15 employed the term "negotiations." The Committee believes that the term "federal-provincial affairs" is liable to be too expansive in a federation like Canada; accordingly, the narrower formulation is preferred. Only if the record or personal information would reasonably be expected to be significantly injurious to the 'negotiations' engaged in by the Government of Canada, could disclosure be denied under this exemption.

Recommendation:

3.6 The Committee recommends that the term "affairs" in section 14 of the *Access to Information Act* and section 20 of the *Privacy Act* be deleted and be replaced by the term "negotiations".

International Affairs and National Defence

Three major state interests are protected by this exemption, found in section 15 of the *Access to Information Act* and section 21 of the *Privacy Act*: international affairs, national defence and national security. Although the exemption is discretionary and contains an injury test, the Committee notes the Department of Justice's observation that no instances are known in which sensitive national security information has been released.[9]

One drafting difficulty appears to have emerged in this exemption. After a broadly worded injury test, nine classes of information which may be withheld are listed. Arguably, "any information" found in the broad classes listed, whether or not it would be injurious if released, must be withheld. The Information Commissioner has interpreted this section as requiring the department or agency to establish that the records withheld are not only of the kind or similar in kind to those enumerated in the subsequent paragraphs, but also that the Department must provide some evidence as to the kind of injury that could reasonably be expected if the record in question were released. On the other hand, the Department of Justice has asserted that one of the specific heads listed in the paragraphs need not be applied to information before the exemption can be claimed, as long as the specific injury test is met.

The Committee is of the view that the over-riding issue which arises in the interpretation of this exemption is whether an identifiable injury would result from disclosure. Nevertheless, this injury must be analogous to the illustrations within the nine classes listed in the exemption. Otherwise, there would be no purpose served by listing these classes of records.

Recommendation:

3.7 The Committee recommends that the Acts be amended to clarify that the classes of information listed in section 15 of the *Access to Information Act* and incorporated by reference in section 21 of the *Privacy Act* are merely illustrations of possible injuries; the overriding issue should remain whether there is an injury to an identified state interest which is analogous to those sorts of state interest listed in the exemption.

Personal Information

Although section 19 of the *Access to Information Act* appears to be mandatory in nature, in reality it refers to the definition of "personal information" contained in section 3 of the *Privacy Act*. A lengthy list of what is or is not personal information for purposes of both statutes is contained in section 3. This drafting approach is unfortunate, as one needs to examine both statutes in order to determine one's rights. The Committee has been assisted considerably by the Report of the Working Group of Federal Access to Information and Privacy Officials in this context.[10] Disclosure is permitted under the *Privacy Act* in a number of situations set forth in section 8, one of which contemplates weighing the public interest in disclosure against the invasion of privacy that might result.

The *Privacy Act* generally safeguards privacy interests except when records contain information in three basic categories:

1. Certain information concerning the terms of employment of public servants and their opinions expressed in the course of their employment;

2. Similar information concerning individuals performing services for a government institution under contract; and

3. Information "relating to any discretionary benefit of a financial nature, including the granting of a licence or permit."[11]

The Committee concurs in the general approach taken by those who drafted the legislation; however, it believes that certain clarifications are necessary in order to respond to specific problems that have developed. The Information Commissioner has suggested that it would be preferable to address this balancing judgment, not within the *Privacy Act* but explicitly within the body of the *Access to Information Act*.[12] In this way, the *Access to Information Act* would become a comprehensive code of disclosure for federal government information.

We understand that section 19 has been interpreted in some quarters as, in effect, constituting an absolute bar to the disclosure of personal information. Despite the balancing test found in section 19(2), the Committee understands that sometimes the mere fact that a record contains personal information is sufficient to bar access. This difficulty could be avoided if section 19(2) were amended to provide as follows:

"Notwithstanding subsection (1), the head of a government institution shall disclose any record....."

The Committee agrees with the Briefs submitted by the Department of External Affairs and the Report of the Working Group of Federal Access to Information and Privacy Officials to the effect that there needs to be a clarification of the definition of "personal information" as it applies to public servants.[13] Specifically, the Committee has been interested in the availability of records which would reveal the salaries of public servants. The definition of "personal information" contained in section 3 of the *Privacy Act* does not include information about public servants respecting "the classification, salary range and responsibilities of the position held by the individual".

As a matter of public policy, there should be no restrictions upon the disclosure of the exact salaries payable to officials appointed by order in council. The precise salaries of the chief executive officers and senior management of Crown corporations and regulatory agencies should generally be available under the *Access to Information Act*. As for other public servants, the Committee recognizes that access to the exact salaries of particular individuals during consecutive years would reveal to fellow employees and others whether or not certain merit increases were awarded and other sensitive information. Accordingly, the Committee concurs in the present arrangements by which only the salary ranges of regular public servants are available under the *Access to Information Act*.

Recommendations:

3.8 The Committee recommends that minor amendments to the definition of "personal information" be considered in order to address certain technical issues which have arisen in submissions to this Committee and to the Department of Justice.

3.9 The Committee recommends that the substance of sections 3 and 8 of the *Privacy Act* be incorporated in the body of the *Access to Information Act*.

3.10 The Committee recommends that section 19(2) of the *Access to Information Act* be amended to provide as follows: "Notwithstanding subsection (1) the head of a government institution shall disclose...."

3.11 The Committee recommends that the definition of "personal information" under the *Privacy Act* be amended so that the exact salaries of order in council appointments be available pursuant to a request under the *Access to Information Act*, and that only the salary range of other public servants be excluded from this definition.

Disclosure of Personal Information "In the Public Interest"

Section 8(2) of the *Privacy Act* establishes a number of circumstances under which "personal information under the control of a government institution may be disclosed." In turn, the *Access to Information Act* contemplates the disclosure of personal information in three circumstances: (1) if the individual to whom it relates consents to this disclosure; (2) the information is publicly available, or (3) the disclosure is in accordance with section 8 of the *Privacy Act*.[14]

One of the circumstances in which the head of the government institution may disclose personal information is of great concern to the Committee. Where the head of the institution is of the opinion that "the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure,"[15] the information may be released. Determining what is in the "public interest" obviously may have serious consequences for an individual's privacy. The Committee is concerned that the decision in this case is left essentially to the discretion of the government institution; the individual concerned is not involved, nor is he or she usually notified of the decision.

A record of disclosures under section 8(2) of the *Privacy Act* is kept for review by the Privacy Commissioner. He is to be notified in writing of any disclosure beforehand "where reasonably practicable" or "forthwith" after the disclosure in other circumstances. The Privacy Commissioner may notify the individual affected if he deems it appropriate to do so. Generally such notification is the exception rather than the rule.

This tension between individual privacy and disclosure "in the public interest" is a feature in most access legislation. For example, the U.S. *Freedom of Information Act* bars disclosure of the following: "Personnel and medical files and similar files, the disclosure of which constitute a clearly unwarranted invasion of personal privacy".[16] The proposed Ontario Freedom of Information and Individual Privacy Act (Bill C-34) stipulates "that a record shall not be withheld from disclosure where there is a

compelling public interest in disclosure that outweighs the interest in non-disclosure or in confidentiality."

The records of disclosure under section 8(2) of the *Privacy Act* have been submitted to the Committee by the Privacy Commissioner. They indicate that this special condition for disclosure is being used in ways that may not be totally appropriate in light of the strong privacy values endemic to our political culture. The Privacy Commissioner is persuaded that "government departments have used this section cautiously and consulted the Commissioner's office frequently before taking any action, particularly when examining whether the public interest or merely public curiosity was at stake."[17] He has also expressed his concern that he is normally not given advance notice of proposed releases and has written in protest to various federal institutions on occasion. The Commissioner reviews the notices of releases that he receives under the *Privacy Act* and considers each situation on its own merits. His staff frequently consults institutions which are proposing to release personal information under section 8(2)(m) of the Act. This consultation may lead to the information not being released. In the 1985-86 fiscal year, the Privacy Commissioner received some 24 notifications from a total of 13 government institutions.[18]

Two examples of public interest releases under the Act will illustrate the issue. In one instance, Transport Canada informed the Privacy Commissioner that it intended to release the names and addresses of federally licensed Canadian pilots as requested by the publisher of an aviation magazine. A few pilots had previously complained that this practice constituted a violation of their privacy. Transport Canada decided not to release the list to the magazine after the Privacy Commissioner was notified and observed that he could not realistically be expected to notify all the individuals concerned. He indicated that he would investigate any subsequent complaints.[19] In another case, the Department of Veterans' Affairs released personal data to the Royal Canadian Legion for a survey on housing for single veterans. There is no available evidence to indicate that the individuals concerned were notified in advance or agreed with such disclosures.

Those people who have given personal information to a government institution should have complete assurance that their personal information is not going to be released to any outside body without a right to comment or to challenge this disclosure. However, the major bureaucratic burden that would result from a statutory duty to locate and notify large numbers of people in some instances, would raise enormous practical difficulties. An example of this difficulty would be the need to notify the thousands of people holding Canada Savings Bonds that a government agency held money in their names.

Under the *Access to Information Act*, businesses are notified of the pending release of information about them and offered an opportunity to contest such disclosure. The *Privacy Act* creates a different standard for the release of personal information: normally a person is neither notified in advance nor given the opportunity to contest a decision of the government institution to disclose personal information. At present, the only protection is offered by the Information Commissioner, who may recommend that since personal information is involved, a record should not be released under the *Access to Information Act* or by the Privacy Commissioner, who often learns about the release after the fact.

The Committee has concluded that individuals should generally be notified of impending disclosures of personal information about them. If a considerable number of people are affected by a decision to disclose records that could invade their privacy, the Privacy Commissioner should have the authority to determine whether an impending disclosure of personal information would violate individuals' privacy to an extent which is not warranted in the "public interest", and, if so, to order the government institution to take all reasonable efforts to notify the individuals concerned. The Act should provide sufficient opportunity for any concerned individuals to contest the disclosure of their information before the Federal Court.

Recommendations:

3.12 The Committee recommends that section 8(5) of the *Privacy Act* be amended to require that individuals generally be notified of the impending disclosure of personal information about them and be entitled to contest this disclosure before the Privacy Commissioner and Federal Court. When considerable numbers of people are affected, the Privacy Commissioner should have the authority to determine whether the disclosure of personal information under section 8(2)(m) constitutes an unwarranted invasion of personal privacy. If the Commissioner so determines, he shall order the government institution to make reasonable attempts to notify the individuals concerned, who should have such time as the Commissioner stipulates to contest the disclosure before the Federal Court.

3.13 The Committee further recommends that the head of the government institution be permitted to appeal the Privacy Commissioner's determination that a particular disclosure of personal information under section 8(2)(m) of the *Privacy Act* constitutes an unwarranted invasion of personal privacy to the Federal Court in the event of a disagreement.

Confidential Business Information and Related Procedures

Section 20 of the *Access to Information Act* protects certain kinds of information furnished to a government institution by a third party. A third party may be any person, group of persons or organization that is not a "government institution" under the Act. Generally, section 20 protects confidential business information of the following kind: "trade secrets"; confidential, financial, commercial, scientific or technical information; information which, if disclosed, would likely have an adverse impact upon the business in question or interfere with its contractual or other negotiations. There is considerable overlap among the classes of records listed in section 20. Although its scope may be uncertain, its purpose is clear: to limit the public disclosure of a third party's confidence which may be found in government records.

One type of information that is protected is so-called "trade secrets". This key term, however, is not defined in the Act. The Committee agrees with the Canadian Bar Association that a narrow definition of this key term is appropriate,[20] given that other subsections provide a broader protection for the confidential business information contained in government files.

Recommendation:

3.14 The Committee recommends that the following definition of "trade secrets" should be contained in the *Access to Information Act*:

> **A secret, commercially valuable plan, formula, process or device, that is used for the making, preparing, compounding or processing of trade commodities and that can be said to be the end product of either innovation or substantial effort.**

Product or Environmental Testing (section 20(2) and section 18 of the Access to Information Act)

At present, there is no provision which addresses the disclosure of the results of product or environmental testing carried out by the Government of Canada for federal government institutions. Section 18, which protects the economic interests of Canada, closely parallels section 20, which protects third-party information—except that there is no equivalent clause pertaining to the results of product or environmental testing. As a result, government institutions may not have to disclose their own product or environmental testing results, although such testing results carried out by or on behalf of such institutions on private sector products or activities are subject to disclosure. The Committee

agrees with submissions by such groups as the Public Interest Research Centre that this position is both illogical and unfair; it puts the Government in the position of having a more pervasive right of non-disclosure for testing of government activities than for its testing of private sector activities.

Recommendation:

3.15 The Committee recommends that section 18 of the *Access to Information Act* require disclosure of the results of product or environmental testing, along the lines of section 20(2).

Public Interest Override

Section 20(6) of the *Access to Information Act* authorizes the disclosure of information relating to public health, public safety or protection of the environment if the public interest in disclosure "clearly outweighs" specified commercial injury to the third party. At present, this provision may not override "trade secrets".

It appears that this public interest override has been used very sparingly to date. The Department of Justice reported that only two of the government institutions it surveyed had used this provision, in one case concerning allegations of poisoning and in the other the release of information relating to the drug Thalidomide.

Recommendation:

3.16 The Committee recommends that the public interest override contained in section 20(6) of the *Access to Information Act* extend to all types of third-party information set out in section 20.

Third-Party Intervention Under Section 28 of the Access to Information Act

Where a government institution intends to release a record that contains information that may affect a third party, the head of the government institution must advise the third party and give it twenty days to make representations as to why the record should not be disclosed. If the government institution still considers that the disclosure is permitted under the Act, it must advise the third party and give it a further twenty days to file an application with the Federal Court in an attempt to prevent its disclosure. The third party has no right to complain to the Information Commissioner about the release of a record. However, if the government institution accepts the third party's representations and decides against the release, the applicant for the record may complain to the Information Commissioner.

Several difficulties have arisen with third-party procedures. Notification of third parties within the thirty-day time limit has often been difficult, particularly where many third parties must be notified or when such parties are located outside of Canada. A second issue relates to the definition of "third party" contained in section 3 of the *Access to Information Act*. It should be clear, for example, that a band council established pursuant to the *Indian Act* has third-party status. A third issue which has arisen is which party must bear the burden of proof when third parties apply to review decisions to disclose records which may contain confidential business information. The issue of which party is to bear the burden of proof is addressed with respect to general refusals to disclose records: the government institution bears the burden. The Act should be amended to clarify that the burden of proof should be placed upon the third party to establish that disclosure would harm one of the listed interests protected under section 20 of the Act.

Recommendations:

3.17 The Committee recommends that, where many third parties are involved or such parties reside outside of Canada, the *Access to Information Act* be amended to provide for substitutional service of notification by means of notice in the Canada Gazette and advertisement in any relevant trade journal, periodical or newspaper.

3.18 The Committee further recommends that the *Access to Information Act* be amended to clarify that third parties bear the onus of proof before the Federal Court when they challenge decisions to disclose records that may contain confidential business information.

Government Operations

Perhaps of all exemptions, section 21 of the *Access to Information Act* (pertaining to policy advice and recommendations as well as other governmental interests) has the greatest potential for routine misuse. The *Privacy Act* does not contain an equivalent provision. Section 21 currently contains four categories of information relating to the internal decision making and policy-development process. These categories of information presently covered in section 21 are as follows:

1. Advice or recommendations developed by or for a government institution or a Minister;
2. An account of consultations involving government officials, a Minister or his or her staff;
3. Positions or plans for negotiations carried on by the Government of Canada and related considerations; and
4. Administrative or personnel management plans that have not yet been put into operation.

The exemption can only be invoked if the record in question came into existence less than twenty years prior to the request under the *Access to Information Act*. Records of the type set out above which have been in existence for more than twenty years may, nevertheless, be withheld under the other exemptions set out in the Act. The exemption set out in section 21 does not apply to records containing reasons for an administrative decision affecting the rights of a person, nor to reports prepared by outside consultants or advisors.

The Committee agrees with the many briefs it received to the effect that section 21 of the *Access to Information Act* is cast in language that is far too broad. The Consumers' Association of Canada, the Canadian Daily Newspaper Publishers Association, the Centre for Investigative Journalism, and the Canadian Bar Association were among the groups which took this position. This exemption should be limited to policy advice and minutes at the political level of decision-making; factual information used in the decision-making process should generally not be covered by this exemption, although, of course, certain factual information may be withheld under other exemptions. The intent of the section should be clear: only records dealing with matters prior to a decision having been taken, which are clearly of an advisory or policy nature, may be withheld under section 21.

This exemption currently bars access to records for twenty years after their creation. The Committee recognizes that the precise scope of any limitation period is arbitrary in nature; nevertheless, it has concluded that a twenty-year period is far too long. There should be little reason in most circumstances for records containing policy advice to be safeguarded for two entire decades. Particularly sensitive information might still be withheld under other exemptions for a longer period in certain instances. The Committee believes that resort to this exemption should only be possible for a period of ten years—the maximum duration of two Parliaments.

Recommendation:

3.19 The Committee recommends that section 21 of the *Access to Information Act* be amended not only to contain an injury test but also to clarify that it applies solely to policy advice and minutes at the political level of decision making, not factual information used in the routine decision-making process of government. The exemption should be available only to records that came into existence less than ten years prior to a request.

Solicitor-Client Privilege

The exemption contained in section 23 of the *Access to Information Act* and section 27 of the *Privacy Act* applies when legal advice of any kind is sought from a government lawyer who provides this advice in such capacity. It attaches to the communications which relate to the seeking of such advice. The exemption should not be used to thwart the spirit of the Acts simply because the Department of Justice has had occasion to provide information as part of routine government decision making. Only if the record sought would genuinely impair the confidential relationship existing between the lawyer and his or her governmental client should this exemption be available. The Committee notes that a narrower formulation of this exemption has been used in other legislation.[21] It agrees with the Public Interest Research Centre that this exemption generally should be limited to cases in which there is pending litigation.[22]

Recommendation:

3.20 The Committee recommends that section 23 of the *Access to Information Act* and section 27 of the *Privacy Act* be amended to clarify that the solicitor-client exemption is to apply only where litigation or negotiations are underway or are reasonably foreseeable.

The Existence of a Record

Neither the *Access to Information Act* nor the *Privacy Act* requires a government institution to confirm whether a particular record actually exists. Sometimes disclosure of a record's existence may be the essential information requiring protection. If a government institution avails itself of this provision, it must state the provision on which a refusal could reasonably be expected to be based, if the record existed.

Only in rare circumstances can such a denial be justified. The Committee notes that the provision is used infrequently, and when it is invoked, most frequently the exemptions pertaining to international affairs and national defence, and law enforcement are involved. In the proposed Ontario legislation on access to information and individual privacy (Bill 34), only when law enforcement information is at stake may the government refuse to confirm or deny the existence of a record.

Recommendation:

3.21 The Committee recommends that section 10(2) of the *Access to Information Act* and section 16(2) of the *Privacy Act* be amended to permit the government institution to refuse to confirm or deny the existence of a record only when disclosure of the record's existence would reveal information otherwise exempt under sections 13, 15, 16 or 17 of the *Access to Information Act* or sections 19, 21, 22 or 25 of the *Privacy Act* (information from other governments, international affairs and national defence, law enforcement and investigations, and safety of individuals).

B. Cabinet Confidences

Cabinet confidences that have been in existence less than twenty years are excluded entirely from the ambit of the *Access to Information Act* and the *Privacy Act*. There is no exemption for such

Cabinet records: the Acts simply do not apply to them. Consequently, there can be no review by the Commissioners or the Federal Court of decisions to deny requests for records or personal information when this exclusion is invoked. No examination of such documents can be undertaken either by the Commissioners or by the Federal Court. The Information Commissioner, however, has used the authority of section 36.3(1) of the *Canada Evidence Act* to obtain a Ministerial Certificate to the effect that a record or a portion of a record constitutes a confidence of the Queen's Privy Council for Canada. Such Certificates are issued when a complaint involves excluded information and the Information Commissioner seeks confirmation that the document is in fact a Cabinet confidence.

What does the exclusion of Cabinet confidences contained in the two Acts entail? For ease of reference, section 69 of the *Access to Information Act* will be considered; section 70 of the *Privacy Act* is virtually identical. The provision begins with a blanket exclusion for "confidences of the Queen's Privy Council for Canada". The Council is defined as including the Cabinet and Committees of Cabinet (section 69(2)). Without restricting the generality of the term "confidences" of the Cabinet—and nowhere defining this amorphous concept—the provision goes on to list several specific categories of documents which are to be excluded from the ambit of the legislation. These categories are as follows:

(a) "memoranda" designed to present recommendations to Cabinet;

(b) "discussion papers" designed to explain or analyze policy choices to be made by Cabinet;

(c) Cabinet "agenda" or records recording deliberations or decisions of Cabinet;

(d) records used for interministerial communications leading up to government policy determinations or records reflecting these communications or discussions;

(e) records created to brief Ministers concerning matters on which Cabinet decisions are to be taken;

(f) draft legislation;

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

None of the key terms used in the provision excluding Cabinet records—"memoranda", "discussion papers", and so forth—is defined in the Act. The only refinement contained in the legislation concerns discussion papers. Under section 69(3) of the *Access to Information Act*, those discussion papers relating to decisions which have been made public or which relate to decisions that are more than four years old are not covered by the exclusion. Nevertheless, this category of discussion papers may still be withheld if they contain records which may otherwise be withheld under the exemptions in the *Access to Information Act*.

The Committee recognizes several important justifications for withholding records coming within many of the categories listed in the provision concerning Cabinet confidences. Firstly, the important convention of collective ministerial responsibility requires that each Cabinet member be held personally responsible for government policy. Therefore, all members of a Government in a parliamentary system can be held publicly accountable and, accordingly, frank exchanges among Ministers are to be expected and encouraged. Section 69(1)(d), which protects interministerial communications, can be explained on this basis.

A second justification for some degree of Cabinet confidentiality is the desire for Ministers of the Crown to receive candid advice from their officials. The Committee agrees that it is clearly in the public interest for candid and confidential advice to be offered to Ministers by senior public servants. Section 69(1)(e) is designed to protect this interest. However, this clause appears to be largely redundant in light of the policy advice exemption contained in section 21 of the *Access to Information*

Act. In particular, section 21(1)(a) and (b) permits a government institution to withhold any record that contains "advice or recommendations developed by or for ... a Minister of the Crown" and "an account of deliberations involving officials or employees of a government institution, a Minister of the Crown or the staff of a Minister of the Crown." Memoranda developed by a Minister for presentation to Cabinet are adequately protected by section 21; section 69(1)(a) is not necessary. Therefore, section 21 fully accords with the second important justification for Cabinet confidentiality in Canada's parliamentary form of government.

A third justification for some measure of Cabinet secrecy is that government ought not to be required routinely to divulge Cabinet agenda or the nature of the issues that have been or will be considered by Cabinet. The timing for the release of particular matters may often be dictated by external events and routine disclosure of Cabinet agenda, decisions or, in particular, draft legislation would not be consistently in the public interest. To the extent that briefing books and similar materials would indicate the nature of matters currently before Cabinet, this information should likewise be generally exempt from disclosure. Accordingly, the Committee accepts the need for the legislation to provide some degree of protection for matters in paragraphs (c) and (f) listed above.

Nevertheless, the Committee does not believe that the background materials containing factual information submitted to Cabinet should enjoy blanket exclusion from the ambit of the Acts. It is vital that subjective policy advice be severed from factual material found in Cabinet memoranda, discussion papers, and other records. Factual material should generally be available under the Acts—unless, of course, it might otherwise be withheld under an exemption in the legislation. For example, if the disclosure of certain factual information considered by Cabinet might reasonably be expected to reveal sensitive law-enforcement information, it could be withheld under the exemption contained in section 16 of the *Access to Information Act*. However, as the *Access to Information Act* is presently drafted, the ability to "sever" exemptable material from non-exempt records set out in section 25 of the Act does not apply to Cabinet confidences. In addition, the Committee has heard testimony to the effect that discussion papers sometimes contain policy recommendations, the effect of which is to preclude access to such discussion papers, which often offer a rich source of information to those applying under the *Access to Information Act*.

The Committee is strongly of the view that the absolute exclusion of Cabinet confidences from the ambit of the *Access to Information Act* and the *Privacy Act* cannot be justified. The Committee heard more testimony on the need to reform this provision than on any other issue. The exclusion of Cabinet records has undermined the credibility of the *Access to Information Act* and the *Privacy Act*. The then Minister of Justice, the Honourable John Crosbie testified before the Committee as follows:

> I think that in the past too much information was said to be covered by the principle of Cabinet-confidence.... A lot of the information previously classified as Cabinet confidence can and should be made available.[23]

The Committee agrees. Ken Rubin, an Ottawa researcher and experienced user of both statutes, has published a comprehensive study which examines the issue of Cabinet confidences in considerable depth.[24] Mr. Rubin's study contains numerous examples of overly broad claims of Cabinet confidence which, on examination, often appeared to be without merit.

The Committee recognizes that there must be an exemption protecting certain Cabinet records; to a substantial degree, our parliamentary system of government is predicated upon the free and frank discussion of matters of state behind closed doors. Nevertheless, the Committee believes that a suitably worded exemption—*not an exclusion*—would provide ample protection for Cabinet secrecy. In recognition of the special role that the Cabinet plays in our parliamentary system, no injury test should apply to information of this category. As such a recommendation is contrary to our general recommendation that exemptions should contain injury tests, the Committee hopes to emphasize its recognition of the special nature of Cabinet government. Furthermore, the Committee recognizes that it may seem inappropriate for even an office-holder directly accountable to Parliament, such as the

Information Commissioner or the Privacy Commissioner, to be in a position to "second guess" a Cabinet decision concerning the release of one of its records. Only a very senior judge of the Federal Court of Canada should be empowered to review Cabinet records—yet not to assess the merits of a claim concerning the potential injury arising out of their disclosure.

By transforming the Cabinet exclusion into an exemption, the severability provisions of the *Access to Information Act* would apply to this category of record. Therefore, under our recommendation, exemptable Cabinet records might be withheld, with the balance of the record being disclosed under the *Access to Information Act* or the *Privacy Act*.

The drafting of an appropriate exemption for Cabinet records is problematic. A delicate balance must be struck. The Committee is attracted to the suggestion made by Dean John McCamus in his testimony on behalf of the Social Science Federation of Canada.[25] He proposed that subsections (a) and (b) of section 69(1) of the *Access to Information Act* (section 70(1)(a) and (b) of the *Privacy Act*) be deleted. As an alternative, he suggested that records coming within section 69(1)(a) or (b) should be exempt only if the disclosure of such records would reveal current discussions of the Cabinet or its agenda. The Canadian Daily Newspaper Publishers' Association preferred the definition of Cabinet confidences contained in the Model Bill proposed by the Canadian Bar Association in 1979.[26]

The Committee recommends that an exemption for Cabinet records be drafted roughly along the following lines:

> (1) The head of a government institution may refuse to disclose a record requested under this Act where the disclosure would reveal the substance of deliberations of the Queen's Privy Council for Canada, contained within the following classes of records:
>
> (a) agenda of Council or records recording deliberations or decisions of Council;
>
> (b) a record used for or reflecting consultation among Ministers of the Crown on matters relating to the making of government decisions or the formulation of government policy;
>
> (c) draft legislation or regulations;
>
> (d) records that contain information about the contents of any records within a class of records referred to in paragraph (a) to (c).
>
> (2) For the purposes of subsection (1) "Council" means the Queen's Privy Council for Canada, committees thereof, Cabinet and committees of Cabinet.

As indicated above, the interest protected currently by "memoranda", "discussion papers" and briefing notes for Ministers [section 69(1)(a), (b) and (e)] should be protected in appropriate cases by the "policy advice" exemption contained in section 21 of the *Access to Information Act*.

Recommendations:

3.22 The Committee recommends that the exclusion of Cabinet records found in section 69 of the *Access to Information Act* and section 70 of the *Privacy Act* be deleted. In its place, an ordinary exemption for Cabinet records should be added to the *Access to Information Act* and the *Privacy Act*. No injury test should be included in this exemption.

3.23 The Committee recommends that section 69(1)(a) [Cabinet memoranda], section 69(1)(b) [discussion papers] and section 69(1)(e) [Ministerial briefing notes], as well as section 69(3)(b) of the *Access to Information Act* [section 70(1)(a), (b) and (e) and section 70(3)(b) of the *Privacy Act*] be deleted. The amended exemption for Cabinet confidences should be drafted in the following terms:

(1) The head of a government institution may refuse to disclose a record requested under this Act where the disclosure would reveal the substance of deliberations of the Queen's Privy Council for Canada, contained within the following classes of records:

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

(b) a record used for or reflecting consultation among Ministers of the Crown on matters relating to the making of government decisions or the formulation of government policy;

(c) draft legislation or regulations;

(d) records that contain information about the contents of any records within a class of records referred to in paragraph (a) to (c).

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

Currently, Cabinet confidences which are more than twenty years old are not excluded from the ambit of the legislation by the Cabinet confidences provision [section 69(3)(a) of the *Access to Information Act* and s. 70(3)(a) of the *Privacy Act*]. For how many years should Cabinet records be presumptively exempt from disclosure? The Committee recognizes that any choice of limitation period will be arbitrary. It considers twenty years to be too lengthy a period. Instead, the Committee is of the view that a fifteen-year period—being the maximum duration of three Parliaments—would provide adequate protection. It must be emphasized that Cabinet records or portions of Cabinet records may nevertheless be withheld for a period greater than fifteen years if they continue to be protected under one of the other exemptions in the legislation.

Recommendation:

3.24 The Committee recommends that the twenty-year exemption status for Cabinet confidences be reduced to fifteen years.

Who should be in a position to examine Cabinet records and, if the test contained in the pertinent exemption is found not to have been satisfied, to order their release? In light of the special status of the Cabinet in Canada's parliamentary form of government, the Committee believes that a special framework is required for this delicate task. Despite the extreme care that has been exercised by the Information Commissioner and the Privacy Commissioner in discharging their functions, the Committee is of the view that only a senior Federal Court judge should be able to examine Cabinet records and order their release in appropriate circumstances. As at present, the Commissioners might still, nevertheless, seek a certificate under section 36.3 of the *Canada Evidence Act* and be permitted to take a case to the Federal Court on behalf of an applicant should they elect to do so—albeit without the benefit of a review of the record at issue. Once the exemption for Cabinet confidences is invoked by a government institution, the Office of the Commissioner should be by-passed. As Gerald Baldwin, Q.C. observed in a Brief to the Committee, under the *Canadian Charter of Rights and Freedoms*, our courts are playing an increasingly pivotal role in public affairs.[27] Therefore, as Mr. Baldwin indicated, it does not seem at all inconsistent to permit the Federal Court to play a more central role in this area of Canadian public affairs as well.

Recommendation:

3.25 The Committee recommends that the *Access to Information Act* and the *Privacy Act* be amended to contain a specific framework for the review of Cabinet records. Appeals of decisions under the Cabinet records exemption should be heard solely by the Associate Chief Justice of the Federal Court, with procedures similar to those contemplated in section 52 of the *Access to Information Act* and section 51 of the *Privacy Act*.

END NOTES

[1] Department of Justice, *The Access to Information Act: A Background Study* (April 1986) at pp. 3, 39.

[2] Information Commissioner, *Main Brief to the House of Commons Standing Committee on Justice and Legal Affairs*, part 15, at F.5.

[3] *Information Commissioner* v. *Chairman of the Canadian Radio-Television Telecommunications Commission* (Federal Court No. T-707-85, February 28, 1986).

[4] Privacy Commissioner, *Annual Report 1985-86*, pp. 13-14.

[5] *Ibid*, p. 14.

[6] Privacy Commissioner, *Annual Report 1985-86*, p. 14.

[7] These statements were made in response to written questions from the Committee.

[8] Submission by Privacy Commissioner to Committee: Sept. 2, 1986

[9] Department of Justice, *The Access to Information Act: A Background Study* (April 1986) at p. 23.

[10] *Personal Information: Whose Business Is It?, Report of the Working Group of Federal Access to Information and Privacy Officials* (March, 1986).

[11] Section 3(j) to (l) of the definition of "personal information" found in the *Privacy Act*. See, generally, J.D. McCamus "The Delicate Balance: Reconciling Privacy Protection with the Freedom of Information Principle" (1986) *3 Gov't. Information Q'ly 49*.

[12] Information Commissioner, *Main Brief to the House of Commons Standing Committee on Justice and Legal Affairs*, part 15, at F.16.

[13] *Submission* of the Department of External Affairs at page 6; *Report of the Working Group of Federal Access to Information and Privacy Officials* (March, 1986) at pp. 21-27.

[14] *Access to Information Act*, section 19(2)

[15] *Privacy Act*, section 8(2)(m).

[16] U.S. *Freedom of Information Act*, 5 U.S.C. s.552(b)(6).

[17] This statement was made in response to a written question from the Committee.

[18] Privacy Commissioner, *Annual Report 1985-86*, pages 47-48.

[19] *Ibid.*, page 46.

[20] This definition, recommended by the Canadian Bar Association in its Brief to the Committee, is taken from the experience under the U.S. *Freedom of Information Act* and is set out in *Public Citizen Health Research Group* v. *Food and Drug Administration*, 704 F.2d, 1280 at 1288 (D.C. Cir. 1983).

[21] See, e.g., section 54(g) of the *Canadian Human Rights Act*, S.C. 1976-77, c.33. It provides that records may be withheld if knowledge of the existence of the record or information "might disclose legal opinions or advice provided to a government institution or privileged communications between lawyer and client in a matter of government business."

[22] Testimony of E. May, Public Interest Research Centre, Proceedings of Standing Committee on Justice and Solicitor General (May 29, 1986) at 18:6.

[23] Testimony of the Honourable John Crosbie, Proceedings of the Standing Committee on Justice and Solicitor General (May 8, 1986) at 10:22.

[24] Ken Rubin, *Access to Cabinet Confidences: Some Experiences and Proposals to Restrict Cabinet Confidentiality Claims* (September 1986).

[25] Minutes of Proceedings and Evidence of the Standing Committee on Justice and Solicitor General, 22:15-17. (June 4, 1986).

[26] *Brief* of the Canadian Daily Newspaper Publishers' Association at page 4. The scope of the Cabinet records exemption in the Model Bill of the Canadian Bar Association (March 1979) is as follows:

> (a) a record of the deliberations or decisions of the cabinet or of a committee of cabinet;
>
> (b) a record of a briefing to the cabinet or a committee of cabinet;
>
> (c) a record containing a policy or proposal which has been prepared by a Minister for presentation to the cabinet or to a committee of the Cabinet, or which has been reviewed and approved by a Minister for presentation to the cabinet or to a committee of the cabinet.;
>
> (d) a record which has been prepared in connection with cabinet business by officers attached to the cabinet office; or
>
> (e) a record of consultation between ministers on a matter relating to government policy.

[27] See, in particular, *Operation Dismantle Inc. et al* v. *The Queen et al* (1985) 18 D.L.R.(4th) 481, in which a panel of the Supreme Court of Canada unanimously expressed itself willing in principle to review Cabinet decision making in order to ensure that the rights and freedoms guaranteed by the Charter were upheld.

CHAPTER 4

THE COMMISSIONERS AND THE COURT

A. The Commissioners

One of the main departures in Canada's *Access to Information Act* and *Privacy Act* has been the creation of an Office of the Information Commissioner and Privacy Commissioner. Rather than requiring a complainant to resort immediately and exclusively to the courts, as in the United States, both Acts have wisely provided for Commissioners to be appointed. Their appointment by the Governor in Council as office-holders directly accountable to Parliament must be preceded by a resolution of the Senate and House of Commons. To further enhance their independence, the Commissioners are provided with security of tenure for a seven-year term. Complaints may be made to the Information Commissioner about denials of access to records under the *Access to Information Act*, but also about delays, fees, extensions of time to provide access, language of the record provided, or about any other matter related to requesting or obtaining access under the Act. Similarly, complaints may be made to the Privacy Commissioner by individuals about allegedly improper disclosure of personal information about themselves to others, denials of their request to correct information on their file or of their right to annotate it, delays, and problems with the *Personal Information Index*.

The Commissioners must investigate in private and provide all parties with a reasonable opportunity to make representations. Extensive powers to compel evidence are conferred. It must be emphasized that neither Commissioner has the power to order the disclosure of records or personal information. In this sense, the Acts contemplated that the Commissioners would play a role similar to that of an Ombudsman: the Commissioners are only empowered to make recommendations. He or she may harness all the prestige of the office to encourage compliance with the Acts. In Annual Reports to Parliament, the Commissioners may take recalcitrant government institutions to task. Special Reports on important matters are also possible under the Acts. The coercive powers possessed by a court, however, are deliberately withheld from the Commissioners.

Several witnesses appearing before the Committee recommended that the Information Commissioner be equipped with the power to order disclosure of records. The Committee has rejected this suggestion. Experience to date suggests that there are considerable advantages to the advisory, more informal, role played by the Commissioners under the present legislation. However, the Committee is of the view that for certain subsidiary issues (e.g., concerning fees, fee waivers, delays and so forth) the Information Commissioner should be empowered to make binding orders.

In addition, a broad audit power concerning the implementation of the *Access to Information Act* should be provided, just as the Privacy Commissioner enjoys broad investigatory powers of this nature under section 37 of the *Privacy Act*.

Submissions from the Privacy Commissioner and the Information Commissioner have both emphasized the vital need in the legislation to retain two independent Commissioners. The responsibilities of the two offices are separate and distinct; they must remain so. Under current arrangements, the Offices of the Information and Privacy Commissioners together constitute a department for the purposes of the *Financial Administration Act*. Each Commissioner has the status of a deputy head under the *Public Service Employment Act*. As a result, there is a considerable administrative burden imposed upon the Office. At present, the corporate management function of both Commissioners, comprising 14 person-years, is shared so that financial, personnel and communications officers are responsible to both Commissioners. Presumably, financial considerations dictated a common support service.

Are the current office arrangements satisfactory? There can be no doubt that the functions of the two Commissioners are incompatible. Each has a unique mandate. One is supposed to promote open

government; the other to protect personal privacy. At times, the *Privacy Act* is invoked in order to prevent the release of personal information which has been sought under the *Access to Information Act*. Each Commissioner must conduct impartial investigations and make impartial findings. Each may be called upon to support their respective positions on the same case before the courts or before Parliament. In this circumstance, real or perceived bias must be avoided. Although the Commissioners do not make binding decisions, each Commissioner is required by statute to investigate complaints, receive the representations from the complainant and the government institution involved, and determine if complaints are "well founded". Accordingly, the divergent duties imposed on each Commissioner demand that there be no real or perceived conflict of interest.

The Committee has concluded that the present structure of the Offices of the two Commissioners may lead to real or perceived bias. In practice, the two Offices make every effort to avoid consultation on individual cases. Nevertheless, the same corporate management staff receive and open correspondence, retain contractors and legal counsel, and handle individual case files—subject, of course, to appropriate security measures. Some members of the public and even some senior government officials perceive that the two Commissioners and their staff work together. The common management structure may undermine the Commissioners' ability to conduct investigations in private, as required by their respective statutes. This structure contributes to the appearance, if not the reality, of bias. Therefore, the Committee is of the view that the two Offices must be separated, with separate parliamentary votes for each office and a separate corporate management structure.

Recommendations:

4.1 The Committee recommends that the central mandate of the Information Commissioner and Privacy Commissioner to make recommendations on disclosure be confirmed, but that the power allowing the Information Commissioner to make binding orders for certain subsidiary issues (relating specifically to delays, fees, fee waivers, and extensions of time) be provided in amendments to the *Access to Information Act*.

4.2 The Committee recommends that the Information Commissioner be statutorily authorized to conduct audits of government institutions, *inter alia*, to assess the degree to which the policy of open government contained in the *Access to Information Act* has been implemented. The resources necessary to undertake this additional responsibility should be provided.

4.3 The Committee recommends that the Office of the Information Commissioner and Privacy Commissioner be separated in order to avoid any real or perceived conflict of interest in the discharge of the Commissioners' two mandates. A separate parliamentary vote for each Office should likewise be required.

B. Judicial Review

The precise scope of the Federal Court's authority to review refusals by government institutions to disclose records or personal information under the legislation is most unclear. The *Access to Information Act* does not confer upon the Court any explicit powers to review some matters about which individuals may complain to the Information Commissioner; matters such as fees, unreasonable extension of time to give access, and the language of records are not subject to judicial review under the Act. Similarly, the *Privacy Act* contemplates judicial review solely for issues involving access to records containing personal information. However, the failure to give access within the required time may be deemed a refusal under both Acts. The Court is empowered to order or to forbid the release of a record or personal information or to make such other orders as it considers appropriate. The Court may award costs to an unsuccessful applicant if it finds that important new principles have been raised.

Both Acts contain a two-tiered standard for judicial review which provides less scope for the Federal Court in respect of certain listed exemptions than for others. For more sensitive records or

personal information, the Court may order the head of the government institution to make disclosures only if it finds that the head of the government institution did not have reasonable grounds upon which to base a refusal. For other kinds of records or personal information, the Court is empowered to order disclosure if it concludes that the government institution "is not authorized to refuse" disclosure.

In other words, there are two separate provisions in each Act setting out the ambit of the Federal Court's authority. Both provisions are ambiguous. Both require substantially less than full judicial review. In interpreting section 49 of the *Access to Information Act*, Associate Chief Justice Jerome has held that once a record has been determined to fall within a class of records referred to in an exemption, the applicant's right to disclosure is subject to the discretion of the government institution to make disclosure.[1] The Federal Court has held that in such circumstances, it will not review the exercise of discretion by the government institution once it is determined that the record indeed falls within the class of records exempted from disclosure. Accordingly, the Federal Court is by no means at liberty to substitute its own view for that of the government institution as to whether or not a particular document may or may not be disclosed under the legislation. In the second provision for judicial review contained in both Acts, the Federal Court must determine whether the institution has "reasonable grounds" on which to refuse to disclose a record or personal information. The ambit of this provision is equally unclear. Some commentators have indicated that a narrower power to review is required by this provision; others seem to take the opposite view.[2]

In Bill C-15, the Progressive Conservative forerunner of the *Access to Information Act*, a simple *de novo* appellate jurisdiction was conferred upon the Federal Court. Under this Bill, the Court would have been able to substitute its own view for that of the head of the government institution: a full right of appeal was envisaged. The Committee considers this approach preferable, since there is considerable uncertainty surrounding the current standard. Also, the Committee believes that both Acts should be clarified to confirm that where discretion contained in an exemption is reviewed, the Federal Court should be entitled to substitute its judgment for that of the government institution, as is the case of freedom of information and privacy statutes in other jurisdictions.

Recommendations:

4.4 The Committee recommends that sections 49 and 50 of the *Access to Information Act* and sections 48 and 49 of the *Privacy Act* be amended so as to provide a single *de novo* standard of judicial review.

4.5 The Committee further recommends that the Acts clarify the Federal Court's general jurisdiction to substitute its judgment for that of the government institution in interpreting the scope of all exemptions.

END NOTES

[1] See: *Information Commissioner* v. *Chairman of the Canadian Radio-Television and Telecommunications Commission* (Federal Court, No. T-707-85).

[2] It would appear that the intent of section 50 of the *Access to Information Act* (Section 49 of the *Privacy Act*) was to provide government institutions with a broader authority to withhold particularly sensitive classes of information referred to therein. See the comments of Strayer, J. in *Re Ternette and Solicitor General of Canada* (1985), 9 *Admin.L.R.* 24.

CHAPTER 5

PARTICULAR ISSUES UNDER THE PRIVACY ACT

Assessing the General Effectiveness of the Privacy Act

The main goal of the *Privacy Act*, as enshrined in section 2, is to "protect the privacy of individuals with respect to personal information about themselves held by a government institution ...." The major provisions of the *Privacy Act* designed to achieve this central objective seem to be functioning effectively; nevertheless, some important improvements are needed in a variety of areas.

The *Privacy Act* differs from the *Access to Information Act* in that it has already been revised once on the basis of experience.[1] Some problems persist; they need to be addressed more successfully as the recommendations below suggest. Certain of the statutory changes proposed in this Report are fundamental and add to the scope of the legislation; others are either of less consequence, or require changes in administrative policies and practices, rather than in the *Privacy Act* itself.

Promoting More Active Implementation of the Privacy Act

Sections 4 to 9 are the heart of the *Privacy Act*; they incorporate the standard code of "fair information practices" that is at the core of all effective data protection legislation. Under section 4 of the *Privacy Act*, for example, the heads of government institutions are required to have procedures in place to ensure that personal information which is collected "relates directly to an operating program or activity of the institution." Government institutions are required to collect personal data directly from the individuals concerned, wherever possible, and to inform them of the purposes of data collection. Such information must be kept as accurate, up-to-date, and complete as possible. Subject to various conditions, information may only be used for the purpose for which it was collected, or for a consistent use. Likewise, it may only be disclosed, without the consent of the individual, in conformity with stated rules. It should be noted, however, that section 8(2) describes thirteen purposes for which such personal information may be disclosed to third parties.

The *Privacy Act* features a system of shared responsibility for the implementation of sections 4 to 9. As described in the Introduction to this Report, the prime actors are the heads of government institutions, the Department of Justice, the President of the Treasury Board, and the Privacy Commissioner. Investigators from the Office of the Privacy Commissioner have "found no evidence that either the Treasury Board or the Department of Justice provided any specific education programs to help government staff interpret these sections."[2] Moreover, the Office of the Privacy Commissioner "has found no evidence of procedures in place to ensure systematically that institutions need the personal information they collect" or that they advise individuals in a systematic way of the purpose for collecting data about them.[3]

Section 71 of the *Privacy Act* spells out the duties and functions of the Treasury Board. The President of the Treasury Board is required to keep "under review the manner in which personal information banks are maintained and managed to ensure compliance with the provisions" of the *Privacy Act*. Among other responsibilities, the Treasury Board is also required to prepare (and distribute to government institutions) directives and guidelines concerning the operation of the *Privacy Act*. Statistics Canada and the Public Archives of Canada assist the Treasury Board in the implementation of such records management policies.

There has been some criticism of how well the Treasury Board carries out these relatively explicit responsibilities. The Committee encourages the President of the Treasury Board to implement the duties imposed under section 71 with vigour, since these oversight responsibilities are crucial to the effective implementation of the legislation by government institutions.

In 1983 the Treasury Board published the *Interim Policy Guide: Access to Information Act and the Privacy Act*. It instructs all government institutions to employ the *Guide* in implementing the legislation and in dealing with relevant activities under the laws. The volume has the particular benefit of breathing life into the sometimes narrow words of the legislation. Unfortunately, the *Interim Policy Guide* has not been updated and issued as a full-fledged *Policy Guide* with all the attributes of a Treasury Board order, nor has it been incorporated in the *Administrative Policy Manual*. If these instructions were binding on all employees, and deviations permitted only on advice from the Department of Justice, considerable confusion in implementation of both Acts would be eliminated.

The Committee welcomes the new Treasury Board policy on government information collection, which now requires an independent review and registration process under the auspices of Statistics Canada, and the Committee plans to monitor the Board's implementation of sections 4 and 5 of the *Privacy Act* during future annual reviews of the legislation.

The Committee also looks forward to the results of a review by the Treasury Board and Public Archives of Canada of the administrative arrangements necessary to ensure that section 6 of the *Privacy Act* on retention and disposal of personal information is applied in practice.

The Committee supports the Privacy Commissioner's emphasis on his role as auditor of the federal government's personal information-handling practices. Specifically, it is pleased that he has audited exempt banks and the disclosure of information for law-enforcement purposes under section 8(2)(e). The production of a *Privacy Act Audit Guide* by his office, and his efforts to strengthen the auditing talents of his staff, are equally welcome.[4]

Recommendations:

5.1 The Committee recommends that the Treasury Board update the *Interim Policy Guide* and issue it in permanent form as a full-fledged *Policy Guide* in the *Administrative Policy Manual* within twelve months of the tabling of this Report in Parliament.

5.2 The Committee recommends that the Treasury Board prepare a written submission to the Standing Committee on Justice and Solicitor General on the detailed operational activities of Statistics Canada and the Public Archives of Canada in implementation of records management policies under the *Privacy Act*.

5.3 The Committee further recommends that the Treasury Board continue to publish its *Implementation Reports* and that the Department of Justice continue to publish its *Communiqué*, because of their importance in assisting government institutions with the implementation of the *Access to Information Act* and *Privacy Act*.

5.4 The Committee recommends that the Privacy Commissioner undertake continuing audits to ensure compliance with sections 4 to 8 of the *Privacy Act*. To make this responsibility explicit, the Committee recommends that section 37(1) be clarified by adding the italicized words to the existing section: "The Privacy Commissioner may, ... carry out *audits and* investigations in respect of personal information under the control of government institutions to ensure compliance with sections 4 to 8."

5.5 The Committee further recommends that the "may" in section 37(1) of the *Privacy Act* be changed to "shall" in order to emphasize the central place of this auditing and investigative responsibility for successful implementation of the Act (without depriving the Privacy Commissioner of any discretion in his initiation of specific compliance audits and investigations).

Oversight of Computer-Matching Programs

"Computer matching" involves a particular type of record linkage or matching of personal data. It has been defined as "the comparison of different lists or files to determine whether identical, similar, or conflicting information appears in them. Comparisons can be made by matching names, social security numbers, addresses, or other personal identifiers."[5]

As noted in a June 1986 Report from the U.S. Office of Information Technology, computer matching can be used to detect unreported income, unreported assets, duplicate benefits, incorrect personal identification numbers, overpayments, ineligible recipients, incongruous entitlements to benefits, present addresses of individuals, and service providers billing twice for the same activity. The same report distinguishes *computer matching*, which involves comparing records after an individual is already receiving government benefits or services, and *front-end verification*, which "is used to certify the accuracy and completeness of personal information at the time an individual applies for government benefits, employment, or services."[6]

The Privacy Commissioner has drawn particular attention to the risks of computer matching, because the existence of computers and automated data banks makes widespread matching truly feasible. In the vivid language of the Privacy Commissioner, "Computer matching turns the traditional presumption of innocence into a presumption of guilt: in matching, even when there is no indication of wrong-doing, individuals are subject to high technology search and seizure. Once the principle of matching is accepted, a social force of unyielding and pervasive magnitude is put in place."[7]

The process of government would indeed be more efficient if we were all watched and monitored; the problem is to establish acceptable and tolerable limits to computer matching. There is an especially strong resistance to far-flung matching operations that involve access to a broad array of personal data from various government institutions. The current mechanisms to regulate such practices are inadequate. In particular, a balance must be achieved between the privacy interests of individuals and other societal values, such as the reduction of fraud and waste.

The Privacy Commissioner concluded in his Brief to the Committee that although a recent Supreme Court of Canada decision "reinforces the protection against cross-matching now implicit in the Privacy Act, growing pressure to use the technique in pursuit of some undoubtedly admirable causes may make it prudent to make the prohibition specific and explicit."[8]

Although the Department of Justice has stated that computer matching by federal institutions is currently covered by the *Privacy Act*, the Committee believes that certain aspects of this practice require stronger protections and controls in the legislation itself.[9]

At present, the *Privacy Act* does not deal with computer matching or record linkages in such explicit terms as would be desirable, although it does establish in section 7 the basic principle that personal information should only be used for the purpose for which it was collected. Yet as the Privacy Commissioner has pointed out, "Section 7(a) proscribes the use of personal information except 'for the purpose for which the information was obtained ... or for a use consistent with that purpose'. Since computer matching involves the comparison of personal information collected for different purposes, the practice contravenes this provision of the Act. Only an unacceptably broad interpretation of the words 'consistent use' could be used in an attempt to justify computer matching as now understood."[10] The Commissioner is concerned that, just as in the U.S. experience, where the concept of "routine uses" has facilitated the transfer of data for computer matching, the analogous Canadian standard of "consistent uses" may likewise promote unacceptable computer matching in this country.

The U.S. Senate has recently considered a Bill on computer matching introduced by Senator William Cohen of Maine on August 14, 1986.[11] It is expected that the Bill will be considered in the House of Representatives in 1987. It would have the effect of revising the U.S. *Privacy Act* to regulate computer matching.[12] Its main control mechanisms are the preparation and publication in the *Federal*

Register of a detailed, written matching agreement and the creation of Data Integrity Boards in each federal agency to oversee and coordinate the agency's implementation of matching agreements.

For various reasons, some clarification of the *Privacy Act* is desirable to control the use of computer matching. A special survey by the Treasury Board Secretariat in 1984-5 revealed that government institutions are indeed carrying on a considerable amount of data matching.[13] However, many government institutions have failed to account adequately for their computer matching activities, as required by the *Privacy Act*. The President of the Treasury Board informed the Committee that sections 7 and 8 of the Act "do not deal adequately with the use of the new technology for data matching."[14] A legitimate matching procedure should be a matter of public record or be made subject to guidelines. Computer matching should be explicitly prohibited if it involves using information collected for one purpose for another inconsistent purpose.

Recommendations:

5.6 The Committee recommends that the President of the Treasury Board issue guidelines requiring government institutions to follow the requirements listed below and also recommends that a specific section incorporating these requirements, and a definition of computer matching, be added to the *Privacy Act*:

Government institutions should be required:

a) to give sixty days advance public notice (a comment period) of intended matches in the Canada Gazette and to describe all current matching activities and the type of information resulting from the match in the annual *Personal Information Index*;

b) to report in sufficient detail in the announcement of proposed matches to identify clearly the authority under the *Privacy Act* permitting the match; and

c) to register any new bank resulting from data-matching.

5.7 The Committee further recommends that the *Privacy Act* prohibit all but the most carefully circumscribed data matching, especially with respect to those matches involving the use of personal data from another government institution.

5.8 The Committee recommends that the Privacy Commissioner be especially vigilant in his oversight of computer matching and make a particular point of drawing perceived abuses to the attention of Parliament, both in his Annual Report and in his appearances before the Standing Committee on Justice and Solicitor General.

Controlling Uses of the Social Insurance Number

The Social Insurance Number (SIN) is the most common unique personal identifier in use in Canada. The basic reason for the development of SINs in the early 1960s was the need for numerical identification of individuals to use mainframe computers efficiently; this technological imperative largely continues to the present day. SINs were introduced for purposes of federal unemployment insurance and pension plans in 1964, but no controls were placed on additional uses of this new numbering system, despite some promises that this proliferation would not occur. In fact, the impetus to multiple uses of SINs as a numbering scheme began as early as the initiation of the system in 1964-5. Between 1965 and 1977, the House of Commons paid little systematic attention to the burgeoning uses of SINs.[15]

In 1981 the first Privacy Commissioner, Inger Hansen, Q.C., prepared a Report on the Social Insurance Number in which she recommended the creation of a new criminal offence "against the privacy of another" in order to regulate its use.[16] The Government took no action on this Report.

The number of ways the Social Insurance Number is used today worries many Canadians. This identifying number is so important, so special, and so much a symbol of the need for data protection that it demands certain controls over its use. In 1985-86 the Office of the Privacy Commissioner heard from more than 100 individuals who "either wanted to complain about an organization's use of social insurance numbers or sought clarification about the requirement to provide a SIN."[17]

The simple problem is that Canadians are constantly being asked for their SIN. It is used as a unique personal identifier in a wide variety of settings in all sectors of society.[18] It is alleged that certain police departments require a SIN from persons calling their emergency numbers. Some funeral homes require the number of the deceased to obtain a burial permit from municipal authorities. Persons seeking access to some federal office buildings are asked to produce their SIN. It is thought that credit bureaus use the SIN as a primary means of linking pieces of information about a specific person. Insurance companies regularly ask policy holders to supply their SINs in making policy claims. In the private sector, persons who refuse to divulge their SIN risk the denial of services.

Although it is a very important tool in the operation of our increasingly automated society, the Committee's view is that the Social Insurance Number should not be employed in ways never intended or authorized by Parliament. Individualized numbering systems should be devised to meet the needs of specific systems. The fundamental problem at present is that "the elected representatives of the Canadian people have failed to ensure the existence of adequate policies for controlling the development and uses of social insurance numbers."[19] The 1964 legislation creating the SIN failed to provide any safeguards on its use for other purposes. Thus, the uses of the number as a unique personal identifier have proliferated. The general public seeks controls over the unauthorized uses of the SIN - by the private sector, in municipal and provincial governments, and at the federal level.

Federal employers should take the lead in the judicious use of the SIN. Specifically, as the current Privacy Commissioner has noted, Social Insurance Numbers "should be protected from indiscriminate and trivializing uses."[20] At present, there are 11 Acts or regulations giving federal agencies the authority to collect the SIN, primarily for purposes of unemployment insurance, income tax, and social security.[21] Federal government institutions must question why they are collecting the SIN and whether they truly need it.

The Privacy Commissioner poses the dilemma quite clearly by noting that "if a [Social Insurance] number is requested for any other purpose, an individual is simply not obliged to provide it. Of course, by not providing it, he or she may not receive the goods or services which are desired. That is a decision for each person to make." The Privacy Commissioner further noted that "Uncontrolled and general use of the SIN establishes a *de facto* national identifier with all its ominous and de-humanizing implications."[22] This theme has also been recently emphasized in the U.S. Congressional Office of Technology Assessment's study of *Electronic Record Systems and Individual Privacy*.[23]

In the 1970s, the Progressive Conservatives made the use of SINs a major political issue. The Progressive Conservative Government prepared legislation for controlling the uses of the Social Insurance Number, but it was not introduced before the Government fell at the end of 1979. The Bill was part of the Progressive Conservatives' initiatives on access to government information and improvement of privacy protection. The Honourable Perrin Beatty, M.P., and Senator Jacques Flynn subsequently introduced Bill C-535 in the House and Senate in May 1980.

The 1980 Progressive Conservative Bill C-535, which was essentially a revision of the original privacy legislation, (Part IV of the *Canadian Human Rights Act* of 1977), also proposed a new section of the Act, which would have limited government's use of the Social Insurance Number to the administration of an Act of Parliament or a number of basic programs: pensions, student loans, family allowances, old age security, income tax, and unemployment insurance. Otherwise, "no right, benefit or privilege shall be withheld from and no penalty shall be imposed on any individual by reason of a refusal by the individual to disclose to a government institution the Social Insurance Number assigned to the individual ...." Except for the authorized uses, individuals could require the deletion of their SIN

from any file about them. Whenever government institutions requested a SIN, they would be required to explain the consequences, if any, of failure to provide it.[24] Section 35(1)(f) of Bill C-535 explicitly authorized the Privacy Commissioner to review complaints about Social Insurance Numbers.

Since 1980, three Members of the House of Commons from the Progressive Conservative party, Messrs. Hnatyshyn, Gamble, and Stackhouse, have introduced identical Bills "respecting the use of Social Insurance Numbers."[25] The preamble to these private members' bills is as follows:

> Whereas it is desirable to prevent Social Insurance Numbers from becoming an employee identification number, a student identification number, a patient identification number, a customer identification number, and generally a national single identification number;
>
> And Whereas it is desirable to ensure that any further disclosure or use of Social Insurance Numbers is specifically authorized by prior Act of Parliament after full consideration and public consultation.

The Committee shares the continuing concerns expressed in these private members' Bills.

The Committee notes that at its 1986 Annual Meeting, the Canadian Bar Association passed a resolution on the Social Insurance Number expressing "its deep concern over the philosophy of using a compulsory identification number as a means of tracing or locating persons for purposes other than income tax, social assistance and pensions, as initially instituted."[26] Furthermore, the Committee also takes note of the fact that, after the unauthorized removal of tax records containing the Social Insurance Numbers of 16 million Canadians from an office of Revenue Canada, Taxation in November 1986, *La Ligue des Droits et Libertés* announced the organization of a coalition of Quebec organizations to demand controls on the use of such numbers.[27]

Recommendations:

5.9 The Committee recommends that a new section of the *Privacy Act* limit the collection and use of Social Insurance Numbers to those activities explicitly authorized by federal Act or regulations. Otherwise, there should be a statutory prohibition against the federal government, the provinces, or the private sector denying services or goods to an individual, because of a refusal to provide a Social Insurance Number. The Committee also urges the creation of a statutory cause of action under the *Privacy Act* for individuals faced with such refusals.

5.10 The Committee recommends that the *Privacy Act* be amended as follows:

> **It shall be unlawful for any federal, provincial or local government institution or the private sector to ask any person for his or her Social Insurance Number, unless such a request is authorized by law.**
>
> **It shall be unlawful for any federal, provincial or local government institution or the private sector to deny to any individual any right, benefit, or privilege provided by law, because of such individual's refusal to disclose his or her Social Insurance Number, unless such disclosure is required by federal statute.**
>
> **Any federal government institution which requests an individual to disclose his or her Social Insurance Number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.[28]**

Exempt Banks

Section 18 of the *Privacy Act* authorizes the Governor in Council to establish personal data banks to which individuals cannot obtain access under any circumstances. This section stipulates that the

information banks in question "contain files all of which consist predominantly of personal information" concerning international affairs, national defence, and law enforcement and investigation, as described in sections 21 and 22 of the *Privacy Act*.[29] Individuals who apply for access to an exempt bank are neither given denial nor confirmation of the existence of information about them. The Privacy Commissioner has an oversight function with respect to these exempt banks and may examine them in detail, except when issues of Cabinet confidence arise.[30]

Until 1986, there were about 20 such "exempt banks" for the entire federal government out of a total of more than 2200 personal information banks. The Treasury Board has informed the Committee that there will now be only 5 exempt banks, as soon as the orders in council revoking the exempt status of 15 exempt banks have been prepared.[31]

The remaining 5 exempt banks will be as follows:

NATIONAL DEFENCE:

Military Police Investigation Case Files
DND/P-PE-835
P.C. 1985-798, March 14, 1985

Communications Security Establishment, Security and Intelligence Investigation Files
DND/P-PU-040
P.C. 1984-4088, December 20, 1984

PRIVY COUNCIL OFFICE:

Security and Intelligence Information Files
PCO/P-PU-005
P.C. 1983-1230, April 21, 1983

REVENUE CANADA:

Tax Evasion Cases
RCT/P-PU-030
P.C. 1985-800, March 14, 1985

ROYAL CANADIAN MOUNTED POLICE:

Criminal Intelligence Operational Records
CMP/P-PU-015
P.C. 1985-864, March 14, 1985

In November 1986, the Committee received from the Department of Justice a *Report on Exempt Banks*, based on a review of such banks undertaken by that Department in conjunction with the Treasury Board Secretariat. It is of some interest that those who produced this forty-page Report were themselves denied access to 4 of the then 20 exempt banks. For 4 of the 5 exempt banks, described in the previous paragraph, which are supposed to remain, the Report's findings were almost completely excised from the copy of that document given to the Committee, on the basis of sections 15(1)(f) (international affairs and defence) and 23 (solicitor-client privilege) of the *Access to Information Act*. This was a graphic example for the Committee of the broad range of exemptions from disclosure available to government institutions under the *Access to Information Act*.

Revenue Canada's exempt bank on "Tax Evasion Cases," is the fifth of the exempt banks noted in the preceding paragraph. The findings of those who reviewed this bank merit repetition: "We were denied access to this bank. However, as about 45% of its files admittedly pertain to corporations (i.e., non-personal information), it is doubtful whether it meets the test of section 18 [of the Privacy Act]."

The Committee is impressed by the fact that, after the reduction in the number of exempt banks announced by the Treasury Board in 1986, the following institutions no longer have exempt banks:

Canada Employment and Immigration Commission, Canada Post Corporation, the Correctional Service of Canada, Canadian Security Intelligence Service, and the Department of the Solicitor General.

The status of exempt banks had already been at issue, because of the *Ternette* decision in 1984.[32] When Mr. Ternette's application for personal information from the RCMP's exempt bank of Security Service records reached the Federal Court of Canada, his lawyer asked the Department of Justice to confirm that all the files in the bank had been examined before it was closed, in order to confirm that the bank met the criteria for exemption. Since the response was negative, the Department of Justice subsequently indicated that this bank could no longer be treated as exempt. The Federal Court also asserted its right to review such files to determine whether or not a file was properly included in an exempt bank. A notice of appeal originally filed by the Solicitor General was discontinued in November 1984.

As a result of the decision in the *Ternette* case and subsequent developments, the concept of exempt banks has lost much of its rationale and validity. Mr. Justice Strayer of the Federal Court concluded that an order in council creating an exempt bank under section 18(1) of the *Privacy Act* can only be made "where *each* of the files in the bank consists 'predominantly of personal information described in section 21 or 22.' This follows from the fact that exemptable banks must contain files '*all* of which' consist of such material."[33] The Privacy Commissioner has conducted a systematic examination of all exempt banks and is treating them as open, if there is evidence that they were improperly constituted.

It would be preferable, in the view of the Committee, to treat all personal data in information banks in the same fashion, thus applying the numerous standard exemptions available under the *Privacy Act* to all requests by individuals for access to their personal data. As the Privacy Commissioner explained: "Each application will require the institution to examine the file, not to reject the request automatically because of the privileged position of an information bank. Government institutions may regret the loss of an easy denial of access. But applicants for personal information will be assured of receiving individual treatment."[34] The Committee believes that there should be no body of personal information which is entirely exempt from any kind of review and record-by-record examination.[35]

Administrative convenience is the only major argument in favour of exempt banks. It is much simpler for an institution to claim full exemption for an information bank, and it may be less expensive to do so, in terms of workload, than to review every data bank containing information on international affairs, national defence, and law enforcement and investigation. However, the *Ternette* decision requires a procedure to ensure that the files in question "consist predominantly of personal information," as required by section 18(1) of the *Privacy Act*. Thus individual files must now be reviewed for such purposes as a consequence of this judgment. Moreover, sections 4 to 9 of the Act, concerning the collection, retention and disposal of personal information, imply that government departments must have a review mechanism in place to ensure compliance with fair information practices.

In a similar vein, sensitive information of the type intended for exempt banks raises fears in some quarters about what personal data the government is actually collecting. The public should have the assurance that such data is reviewed in detail in order to ensure their conformity with the *Privacy Act*.

The Privacy Commissioner and the Canadian Bar Association have supported the concept of deleting the provision for exempt banks from the *Privacy Act*. As the Commissioner stated: "Given my choice, I would not have exempt banks. I think it gives the Privacy Act a bad name .... Obviously, some information should be exempted, but I think information ideally should be exempted on a case-by-case basis."[36]

Recommendation:

5.11 The Committee recommends that the concept of exempt banks be removed from the *Privacy Act* by repealing sections 18 and 36, since there is no compelling need to retain such a concept in light of the other strong exemptions on disclosure that exist in the legislation.

Criminal Penalties

As illustrated below, most privacy and data protection statutes include criminal sanctions for breaches of the legislation. The Canadian *Privacy Act* is an exception to standard practice elsewhere in this regard.[37]

The U.S. *Privacy Act* has included criminal penalties since its inception, and these have been applied on occasion.[38] The section prohibits officers or employees of an agency from knowingly and willfully disclosing individually identifiable information to any person or agency not entitled to receive it, or from willfully maintaining a system of records without meeting the notice requirements of the Act. An additional subsection further prohibits any person from knowingly and willfully requesting any record concerning an individual from an agency under false pretenses. The penalty under each section is a fine of up to $5000.[39]

On December 12, 1985, the U.S. Office of Management and Budget issued a circular on the management of federal information resources. It requires each head of an agency to "review annually the actions of agency personnel that have resulted either in the agency being found civilly liable under section (g) of the [Privacy] Act, or an employee being found criminally liable under the provisions of section (i) of the Act, in order to determine the extent of the problem and to find the most effective way to prevent recurrences of the problem."[40]

The Quebec *Act Respecting Access to Documents held by Public Bodies and the Protection of Personal Information* contains a substantial section on sanctions in chapter VII.[41] Penal provisions in section 158 to 161 cover the following activities: knowingly denying or impeding access to information which should be made available; knowingly giving access to information which is not to be disclosed; and impeding the progress of an inquiry or examination of a request or application by the Commission by knowingly providing it with false or inaccurate information or by knowingly omitting to provide it with information it requires. The sanction in each of these instances includes costs and fines of amounts under $1000. Fines for each subsequent offence within two years rise as high as $2500.

Chapter VII of the Quebec data protection law imposes various types of criminal sanctions for breaches of the statute. For example, the Act declares as follows: "Every person who contravenes this Act, the regulations of the government, or an order of the Commission is guilty of an offence and is liable" to a fine of $100 to $500 and, for every subsequent offence within two years, to a fine of $250 to $1000. The penal provisions do contain an exculpatory clause to the effect that "an error or omission made in good faith does not constitute an offence within the meaning of this Act."[42] Section 57 of Ontario's Bill 34, An Act to provide for Freedom of Information and Protection of Individual Privacy prohibits any person from willfully disclosing personal information in contravention of the Act, willfully maintaining a personal information bank in contravention of the Act, or making a request for access to or correction of personal information under false pretenses. Persons convicted of such an offence will be liable to a fine not exceeding $2000. These provisions for three separate criminal sanctions are consistent with the thoughtful recommendations of the Ontario Commission on Freedom of Information and Individual Privacy.[43]

The intent of the Committee's recommendation to incorporate criminal penalties in the *Privacy Act* is to allow the heads of government institutions and the Privacy Commissioner to be in a position to

recommend the use of criminal sanctions for willful and egregious cases of violation of the *Privacy Act*, such as a government employee who steals personal records or otherwise uses them or discloses them in an unauthorized fashion.

Recommendation:

5.12 The Committee recommends that the *Privacy Act* be amended to provide criminal penalties for willful breaches of the statute. Such an offence should prohibit any person from willfully disclosing personal information in contravention of the Act, wilfully maintaining a personal information bank in contravention of the Act, or making a request for access to or correction of personal information under false pretenses.

Civil Remedies

Most privacy and data protection statutes, including those in Quebec, the United States, and Europe, impose civil liability for breaches of the legislation, including compensation to an individual for loss or unauthorized disclosure or unauthorized destruction of data, such as under section 23 of the United Kingdom's *Data Protection Act* of 1984.[44]

The U.S. *Privacy Act* makes various civil remedies available for individuals against federal agencies. A 1985 Circular from the Office of Management and the Budget requires each head of an agency "to annually keep track of convictions and suits in order to determine the extent of the problem and to find the most effective way to prevent recurrences of the problem."[45]

The Canadian *Privacy Act* does not provide for civil remedies at present, nor would Canadians have an established right to sue the federal government for invasion of their privacy, since the tort of invasion of privacy does not exist at the federal level. Such a remedy should be available for wrongful collection, use, and disclosure of personal information.

Several examples illustrate the kinds of problems that currently arise under the Canadian *Privacy Act* and that are without obvious legal remedy. A member of the RCMP complained to the Privacy Commissioner that documents he received from an access request contained personal information about other members of the force. An investigation revealed that the material had been highlighted in preparation for its removal, but it was never erased. The Commissioner noted that "the RCMP took steps to ensure it does not improperly disclose personal information again."[46] But what if this erroneous release of personal data on others had resulted in harm or financial loss to them? They should be able to sue for damages. Moreover, if the Privacy Commissioner concluded that the release was malicious or intentional, he should be able to recommend prosecution of the responsible individual(s).

In another case, files from Employment And Immigration Canada were found in an alley behind its local office in Winnipeg; they contained personal data on individuals participating in various programs. The Privacy Commissioner "concluded that the EIC office was negligent in handling the out-of-date files by not properly supervising or instructing the cleaner about the disposal."[47] If individuals had suffered damages as a result of such negligence, they should have had a statutory cause of action. Similarly, the Privacy Commissioner should have had the option of recommending prosecution, if he considered the Commission, its officers, or particular employees to be criminally negligent.

The Ontario Commission on Freedom of Information and Individual Privacy also recommended the inclusion of a civil remedy of monetary damages in the province's privacy protection scheme. Its useful list of hypothetical cases in support of such a recommendation includes the instance of an agency which improperly discloses information relating to an individual's psychiatric treatment, with the result that the person loses his or her job or is denied an employment opportunity. The Commission offered examples of situations in which individuals suffered pecuniary loss and/or psychological injury of some

kind and recommended that monetary damages should be available for both types of claim. It further recommended that "the government should be liable, regardless of the intentions or *bona fides* of the public servants. We feel, however, that personal liability should only be imposed on a public servant if an act is committed in wilful disregard of a statutory duty.[48]

The Committee agrees with the Ontario Commission that the damages remedy should be available where identifiable harm to an individual has resulted from breaches of the following statutory duties under the federal *Privacy Act*:

1. The duty to collect only authorized or relevant data;
2. The duty to refrain from unauthorized disclosure or transfer of data;
3. The duty to give access to files and to make corrections.[49]

In order for civil liability to be meaningful, individuals should be granted the right to bring suit in as simplified a manner as possible in the Federal Court of Canada, preferably without the need to engage the services of counsel. The Committee notes that section 45 of the *Access to Information Act* contemplates summary rules for similar purposes. If possible, the measure of liquidated damages to be awarded for invasion of personal privacy should be stipulated in the statute for each infraction. The Federal Court should be given the right to award costs to the individual on a solicitor and client basis.

The Committee has taken into account the prospect that concerned senior managers may react negatively to the creation of civil liability in this fashion, thus possibly leading to reduced activity under both the *Access to Information Act* and the *Privacy Act*. It does not believe that this innovation will be counterproductive, since the experience to date suggests that the possible occasions for use of such a civil remedy will be rare. Indeed, the *Crown Liability Act* may already make it possible to sue the government under these circumstances. In addition, section 8 of the 1986 Government Security Policy also provides for administrative, disciplinary or statutory sanctions for the disclosure of sensitive information (when there has been misconduct or negligence). This Policy may also be applicable to breaches of the *Privacy Act*.[50] Nevertheless, the Committee has concluded that the *Privacy Act* should contain its own civil remedies.

Recommendations:

5.13 The Committee recommends that the *Privacy Act* be amended to provide data subjects with monetary damages for identifiable harm resulting from breaches of the following statutory duties:

1. The duty to collect only authorized or relevant data;

2. The duty to refrain from disclosure or transfer of data;

3. The duty to give access to files and to make corrections.

5.14 The Committee recommends that rules of court permit individuals the right to bring suit under the *Privacy Act* in as simplified a manner as possible. Furthermore, the Federal Court of Canada should, in the ordinary course, award costs on a solicitor and client basis to the successful applicant.

Consultation with the Privacy Commissioner

A matter not currently dealt with in the *Privacy Act* is the need for the government and Parliament to notify the Privacy Commissioner of proposed changes to statutes, draft legislation, regulations, and administrative practices that have implications for personal privacy.

The Privacy Commissioner gave the Committee five examples of important matters about which he was not consulted and urged that an amendment to the *Privacy Act* require consultation with his office over privacy-related matters in proposed legislation.[51] For example, he was not consulted in the enactment of the *Family Orders Enforcement Assistance Act* of 1986 or in the development of the 1985 "Conflict of Interest and Post-Employment Code for the Public Service." In both instances, the Privacy Commissioner had serious concerns.[52]

The Committee has concluded that the goals of the *Privacy Act* will be gradually eroded if an improved consultative mechanism with the Office of the Privacy Commissioner is not devised and implemented. Such activities also fit well with his audit and oversight functions for federal information activities. A good example of the contributions of the Commissioner are his comments on the new *Archives Act* (Bill C-7) in an appearance on November 4, 1986, before the House of Commons Legislative Committee considering the Bill.

The consultative and advisory role of the Office of the Privacy Commissioner should be better defined and strengthened by means of a policy directive from the Privy Council Office and the Treasury Board and by changes in the *Privacy Act*. Such consultation should probably be informal in most cases, since the Privacy Commissioner is directly accountable to Parliament and not a part of the Executive Branch of Government as such. Consultation, in the first instance, should require government institutions and the Department of Justice to consider the implications of all its drafting activities for the *Privacy Act*, and then require that the Privacy Commissioner be notified. He may then determine, at his discretion, whether to make comments thereon and the best forum for such comments.

A method must be developed to ensure that the *Privacy Act* is seriously considered by all government institutions in the legislative process, and that the Privacy Commissioner is consulted routinely before legislation or policies impinging upon the *Privacy Act* are introduced. At the stage when new or revised legislation and regulations are drafted, the Department of Justice should be required to consider any possible ramifications for the *Privacy Act*, just as it currently does for the *Canadian Charter of Rights and Freedoms*.

In the United States, the Office of Information and Regulatory Affairs (OIRA) of the Office of Management and Budget requires each notice of a new or altered system of records from an agency to contain an evaluation of probable or potential effects of the proposal on the privacy of individuals. OIRA then reviews this "privacy-impact statement" with the same criteria in mind.[53]

A similar requirement of a privacy-impact statement should be imposed on Canadian federal government institutions which are sponsoring comparable changes. The 1983 *Personal Privacy Protection Law* of New York State contains a useful list of specifications and rules for the contents of such a statement: the name of the agency maintaining the records; the name and title of the responsible official; the procedures for an individual to gain access to these records; the categories and approximate number of persons about whom records will be maintained; the categories of information to be collected; the purposes for which the records will be used; and the disclosures of such information that are intended and the legal authority for such disclosures.[54] Preparing such information will not impose additional duties on a federal government institution, since the same concerns must now be addressed before the notice of any new or revised personal information banks is issued in the *Personal Information Index*.

The process of government and legislative consultation with the Privacy Commissioner does raise some relevant questions about possible conflict of duties. If the Commissioner gives his imprimatur to a specific policy proposal, can he then independently investigate a complaint on the same matter, or an aspect thereof, at a later date? Will consultation become a form of cooptation? A brief answer is that subsequent developments, or the passage of time, may sometimes prove that the Commissioner was wrong or at least misguided in the advice originally given. An emphasis on notification and then

informal consultation with the Commissioner will also reduce the risk of such possible conflicts of interest.

It is also worth noting that the Privacy Commissioner may only give advice and does not make binding rulings. He provides a non-binding, advisory service for government institutions under the *Privacy Act*; they are still legally responsible for compliance with the law, whatever advice they may receive from the Commissioner. Complaints are also much more likely to occur when the Government and Parliament in fact ignore the Commissioner's advice, as regularly occurs in other countries.

The experience in a country like West Germany is somewhat comforting as to this problem of a possible conflict of interest between the Privacy Commissioner's advisory and investigative roles. The data protection authorities in that country are regularly consulted on pending matters of data protection and offer advice. The problems are not that they worry unduly about giving bad advice but about having the government agencies rely on the data protectors to do all the drafting work in the first place, about having too limited resources to provide timely advice on pressing matters, and about having the government or the legislature ignore most of their considered advice.

The Canadian Privacy Commissioner is more likely to be involved in a struggle to have his full recommendations followed rather than in a position of being seen at a later date as having been "too weak" or as having been coopted on a matter affecting personal privacy. The Commissioner may also have to rely on a standard *caveat* in his advice to the effect that he cannot guarantee that he will not change his opinion at a later date in light of new evidence or reconsideration of fundamental issues.

The Committee wishes to encourage informal but systematic consultation between drafters of government legislation and regulations and the Office of the Privacy Commissioner. The Committee's judgment is that the Privacy Commissioner should be notified and at least informally consulted on pending statutes and regulations, and that he should be willing to issue non-binding opinions on request. It may not always be possible for the Commissioner to be consulted in advance in the formulation of government policy, but he should monitor the implications of such policies as they are announced and reported to him and also offer his advice to relevant parliamentary committees. Whenever possible, these consultations should occur on an informal basis in order to avoid additional bureaucratic procedures.

Recommendations:

5.15 The Committee recommends that the Government, government institutions, and Parliament take the requirements of the *Privacy Act* into account, and notify the Privacy Commissioner, concerning any draft or final legislation, regulations, or policies that have implications for the personal privacy of Canadians.

5.16 The Committee recommends that all legislation before Parliament which has implications for the collection, retention, protection, and disposal of personal information be accompanied by a privacy-impact statement prepared by the sponsoring government institution for review and comment by the Office of the Privacy Commissioner.

The Canadian Police Information Centre

One of the most sensitive data bases is the Canadian Police Information Centre (CPIC). It affects all Canadians, directly or indirectly. CPIC is operated as a centralized, automated index to local police records, by the Royal Canadian Mounted Police, at the expense of the federal government, on behalf of police forces across Canada. CPIC itself contains personal information in a variety of interrelated data bases, but it is also an index to the original records kept by local police forces. It is the most visible police information system in Canada and illustrates the general problems of implementing good data

protection practices in all police data systems. CPIC policy is set by an advisory committee composed of twenty-six senior police officers from across Canada. In practice, it is the RCMP that primarily makes policy for CPIC.[55]

One of the issues that arose during the Committee's hearings is the extent to which CPIC is subject to the *Privacy Act* and thus to the jurisdiction of the Privacy Commissioner for purposes of auditing and investigating complaints. The Privacy Commissioner and the Solicitor General claimed that CPIC was at least partially exempt from such scrutiny, because certain data in it originated with local and provincial police forces.

A legal opinion from the legal advisor to the Privacy Commissioner, dated November 21, 1986, asserts that "information provided to the Canadian Police Information Centre by police agencies other than the Royal Canadian Mounted Police could not be investigated pursuant to the *Privacy Act*." The opinion claims that some of the data accessible through CPIC is not in the "control" of the RCMP. In the view of the legal advisor, this jurisdictional problem primarily concerns Investigation Files on persons (covering 1.5 million persons in 1985) and provincial motor vehicle data bases (containing 4.4 million registrations in 1985) that are located in provincial computers and accessible through CPIC. There is no jurisdictional problem for the Privacy Commissioner for Investigation Files entered in CPIC by the RCMP acting as a local or provincial police force, or for the major category of Identification Files (containing 2.9 million criminal records in 1985) maintained on CPIC by the RCMP.[56] But a significant percentage of Investigation Files contains information placed in the CPIC system by municipal police agencies across Canada, especially the large metropolitan police forces (excluding those in Quebec).

The legal advisor to the Privacy Commissioner also expressed the view that amending the *Privacy Act* to give the Commissioner the right to investigate those parts of the CPIC system which, in his view, are beyond the Privacy Commissioner's jurisdiction, will require consultations with the provinces to resolve potential constitutional problems.

The Committee's view is that the concerns raised about the Privacy Commissioner's jurisdiction over CPIC should not be allowed to impair his oversight role with respect to this sensitive and ubiquitous personal information system. The practical realities are that the RCMP operates the CPIC system and controls policy for its use, and federal taxpayers alone finance its operation. It is arguable that all personal information that enters the CPIC system is under the control of the RCMP for all practical purposes and should thus be regarded as being subject to the *Privacy Act*.

The Privacy Commissioner expressed the following opinion to the Committee: "If it would give some sense of security that the information in CPIC will not be abused, I think perhaps the Privacy Act could be changed to make specific our involvement, our jurisdiction."[57] The Committee is of the opinion that any ambiguities on this sensitive matter should be clarified by an amendment to the Act, following negotiations with the appropriate provincial authorities. The Committee also notes that the various exemptions under the *Privacy Act*, including section 19(1) covering personal information obtained in confidence from the government of a province or an institution thereof and section 22 on law enforcement and investigatory data, would provide the necessary protection of CPIC information.

By noting its concern about CPIC, the Committee does not intend to suggest that it is the only data base of this type which merits attentive and continuing oversight by the Privacy Commissioner. Other relevant systems include the Automated Criminal Intelligence System (ACIIS), the Police Information Retrieval System (PIRS), the Automated Intelligence Drug System (AIDS), and the Canadian Security Intelligence Service Records.[58] The problem is that the general public knows relatively little about any of these automated systems, and there is no evident external oversight of their operations for purposes of data protection.

5.17 The Committee recommends that the *Privacy Act* be amended to specify that all personal data stored in the Canadian Police Information Centre is fully subject to the requirements of the *Privacy Act*.

5.18 The Committee further recommends that the Privacy Commissioner evaluate and audit the policies and practices of the CPIC system, and other comparable automated data bases, in order to ensure that the privacy interests of individual Canadians are being adequately protected.

Access Requests from Government Employees

One of the central features of a code of fair information practices is that individuals should have a right of access to their own personal records in the hands of government institutions. Sections 12 to 17 of the *Privacy Act* provide a formal regime to facilitate such requests.

The 375,000 federal government employees are the subject of considerable data collection by the federal government. In practice, however, one anomaly under the legislation is that some government institutions require their own employees to make *formal* requests for access in order to see their own personnel records. This is especially true for the Department of National Defence. In some cases, ironically, this formal policy replaces practices of informal access to personnel records that have existed for many years.

The Committee considers that it is a normal feature of good management practices to allow government employees access to their own personnel files. Government employees should only be required to satisfy the formal requirements of the *Privacy Act* if problems are encountered with these informal procedures. In fact, the Committee urges that government institutions grant individuals informal access to their own records, whenever possible. The Committee's intent is to save time and money and to discourage unnecessary use of formal bureaucratic régimes. Under normal circumstances, only persons outside the employ of the federal government should have to resort to the formal access procedures under the *Privacy Act* in order to see their own records in a personal information bank.

The model of encouraging informal access by individuals to their own records has been well developed in the United States at the federal level, especially by the Department of Defence (DoD). Generally, the number of access requests under the U.S. *Privacy Act* is declining, since informal access procedures have been encouraged. The DoD has concluded that;

> ... the Privacy Act is not being used as a primary method of access to DoD records by individuals. The DoD policy is to encourage granting individuals access to records about themselves without forcing them to use the rather formal procedures of the Privacy Act .... Several component Privacy Officers have indicated that they feel most Privacy Act requests are being filed by former members and employees or by personnel not associated with the Department. This is an indication that current members and employees have general ready access to records about themselves and, therefore, may ... not feel the need to file Privacy Act requests to get access.[59]

The U.S. Office of Management and Budget concludes that this Defense Department assessment is consistent with the experience of other agencies with informal access procedures, especially in personnel programs and benefits programs where individuals have traditionally enjoyed access to their own records.

Recommendations:

5.19 The Committee recommends that all government institutions presently subject to the *Privacy Act* permit their employees to have informal access to their own personnel records, instead of requiring a formal request for access under the *Privacy Act*.

5.20 The Committee recommends that in accordance with its earlier recommendations all government institutions to be covered by the *Privacy Act*, as well as Crown corporations and the federally-regulated private sector, permit employees to have informal access to their own personnel records instead of requiring a formal request for access under the *Privacy Act*.

Consistent Uses of Personal Information

Perhaps one of the surprising aspects of the *Privacy Act* is the fact that the law devotes considerable attention to the conditions under which personal information may in fact be disclosed by government institutions.

Under section 8(2)(a) of the *Privacy Act*, personal information under the control of a government institution may be disclosed "for the purposes for which the information was obtained or compiled by the institution or for a use consistent with that purpose." In the Committee's view, it is unsatisfactory that the Act contains no further definition of a "consistent use," because of the possibility that this provision is being used to evade the clear statutory mandate of closely regulating the disclosure of personal information.

Government institutions are required to list consistent uses of personal information in the annual *Personal Information Index*. If this has not been done, section 9(3) of the *Privacy Act* requires the government institution to "forthwith notify the Privacy Commissioner of the use for which the information was used or disclosed," and "ensure that the use is included in the next statement of consistent uses set forth in the index." The Privacy Commissioner "suspects that a good deal of personal information changes hands for consistent uses .... However, he has received only two notifications under subsection 9(3)." His conclusion is that departments are not notifying him as required and that perhaps the Treasury Board should highlight new consistent uses in the next edition of the *Personal Information Index*.[60]

The Committee is concerned that the Privacy Commissioner received only three such notices of consistent uses in 1985-86: he successfully objected to one and was awaiting clarification from the government institution about a second. The Privacy Commissioner himself noted that "the scale of changes to the latest edition of the Personal Information Index suggests that many institutions have overlooked the obligation to notify the Commissioner of new 'consistent' uses ...."[61] The Committee is concerned that the monitoring mechanism for consistent uses is not functioning effectively.

Since the concept of consistent uses derives from the notion of "routine use" in the U.S. *Privacy Act*, it is useful to note persistent concerns in that country that the term must be made clearer and more meaningful. The U.S. *Privacy Act* defines a "routine use," with respect to the nonconsensual disclosure of a record, as "the use of such record for a purpose which is compatible with the purpose for which it was collected."[62] As a recent Presidential Report on the *Privacy Act* makes clear, "compatibility is the sole standard for agencies to use in deciding whether a disclosure can be appropriately made as a rountine use." But, the Report continues, there are real problems in discerning what Congress originally intended, and "even a casual examination of agencies' routine uses suggests that agencies interpret the concept of compatibility to permit uses that are neither functionally or programmatically related to the original collection purpose."[63] This is the problem which the Committee seeks to address in Canada.

In 1977 the U.S. Privacy Protection Study Commission recommended that, in addition to compatibility with the purpose for which the information was collected or obtained, a routine use should also be "consistent with the conditions or reasonable expectations of use and disclosure under which the information in the record was provided, collected, or obtained."[64] As noted in the previous paragraph, the President's Annual Report to Congress in 1985 called on Congress to reconsider this problem. The Office of Management and Budget's own Guidelines in 1986 on the implementation of programs for monitoring employee use of government telephone systems added the concept of "functionally equivalent uses" and "uses that are necessary and proper."[65]

New York's *Personal Privacy Protection Law* of 1983 defines routine uses as follows:

> The term "routine use" means, with respect to the disclosure of a record or personal information, any use of such record or personal information relevant to the purpose for which it was collected, and

which use is necessary to the statutory duties of the agency that collected or obtained the record or personal information, or necessary for that agency to operate a program specifically authorized by law.[66]

Section 39(a) of Ontario's Bill 34, An Act to Provide for Freedom of Information and Protection of Individual Privacy, employs the concept of "consistent purpose" and defines it as follows:

> Where personal information has been collected directly from the individual to whom the information relates, the purpose of a use or disclosure of that information is a consistent purpose under clauses 38(b) and 39(ab) only if the individual might reasonably have expected such a use or disclosure.

In addition, the Treasury Board's *Interim Policy Guide on the Privacy Act* specifies some criteria for identifying consistent uses and disclosures, which may assist in placing controls on consistent uses in the Act itself. The guidelines state that consistent uses are "related purposes .... For a use or disclosure to be consistent it must have a reasonable and direct connection to the original purpose(s) for which the information was obtained or compiled."[67]

Recommendations:

5.21 The Committee recommends that the following definition of "consistent use" be added to the *Privacy Act*:

> **The term "consistent use" means, with respect to the disclosure of a record or personal information, any use of such record or personal information relevant to the purpose for which it was collected, and which use is necessary to the statutory duties of the agency that collected or obtained the record or personal information, or necessary for that agency to operate a program specifically authorized by law. For a use or disclosure to be consistent it must have a reasonable and direct connection to the original purpose(s) for which the information was obtained or compiled.**

5.22 The Committee further recommends that the Treasury Board forcefully remind government institutions of their obligation, under section 9(3) of the *Privacy Act*, to publish information about consistent uses in the *Personal Information Index* and to notify the Privacy Commissioner when such disclosures occur without such advance notification.

The Definition of Personal Information

Section 3 of the *Privacy Act* currently includes a definition of the meaning of "personal information" and a lengthy list of what constitutes personal information for purposes of the legislation. The Committee concurs in the approach taken by the drafters of the legislation, but believes that certain clarifications are necessary at present to respond to specific problems that have developed.

Testimony from the Canadian Historical Association and the Social Science Federation of Canada suggested that the date of death provisions in section 3(m) of the *Privacy Act* should be changed to 10 years (from 20 years), or 100 years since birth date, since a researcher requesting a private letter may often find it impractical to prove that the writer has been dead for more than 20 years.[68]

The Working Group of Federal Access to Information and Privacy Officials recommends in its Report to the Treasury Board that the definition of personal information should be improved and made more precise in certain areas. In particular, it recommended that the definition should permit the disclosure of personal information at the discretion of the head of the government institution for reasons of public safety and health. The Working Group also recommended certain corrections to paragraphs (k) and (l) of section 3 where there are practical difficulties with the application of the current language, which involves government services contracts and financial benefits of a discretionary nature.[69]

Recommendation:

5.23 The Committee recommends that the definition of personal information in section 3 of the *Privacy Act* be amended as follows:

> **1. The date of death provisions in section 3(m) of the *Privacy Act* be changed to 10 years (from 20 years), or 100 years since birthdate.**
>
> **2. The head of the government institution be permitted to disclose personal information for reasons of public safety and health.**

Defining Privacy

At present, the purpose of the *Privacy Act*, as stated in section 2, "is to protect the privacy of individuals with respect to personal information about themselves held by a government institution," but the term "privacy" is nowhere defined in the legislation. In fact, this problem of lack of definition of the central concept of privacy is endemic in data protection legislation.

The Committee is of the view that a simple definition of privacy, adapted to the purposes of data protection, should be added to section 3 of the *Privacy Act* in order to facilitate and guide implementation and interpretive activities. This is an especially important exercise since the right to personal privacy remains largely undeveloped in Canadian law. Since the concept of privacy can be extended to cover such a broad range of human behaviour and activities, the need is even more pressing.

In his seminal work, *Privacy and Freedom*, Alan F. Westin of Columbia University defines privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[70] Especially as applied to claims by individuals, this definition is both useful and more fruitful than earlier formulations based on a vague notion of the right to be left alone.

Recommendation:

5.24 The Committee recommends that the following definition of privacy be added to section 3 of the *Privacy Act*:

> **Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is to be communicated to others.**

Security Considerations

At present, the *Privacy Act* makes no mention of the need to maintain adequate security for personal information as a normal part of privacy protection. This is a surprising omission when the situation in other national legislation is considered. For example, the Organization for Economic Co-operation and Development's *Guidelines on the Protection of Privacy*, to which Canada has formally adhered, require that "personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data."[71]

The U.S. *Privacy Act* requires government agencies to:

> 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.[72]

Recent events and concerns about the security of income tax records maintained by Revenue Canada, Taxation are a reminder of the central importance of security considerations for maintaining the integrity of manual personal records, including microfiche, and automated records. In November 1986, an employee of Revenue Canada, Taxation removed 2,000 microfiche records from a locked reading room in the Toronto District Taxation Office. These records contained the name, address, Social Insurance Number, an employment code, last tax filing year, and name of spouse of 16 million individual taxpayers. Although the actual records were quickly recovered, the episode revealed a significant problem with security procedures and shocked the general public. The RCMP has laid criminal charges against the employee in question.

Inclusion of a provision on security in the *Privacy Act* will facilitate the oversight by the Privacy Commissioner of this essential condition for protecting the confidentiality of personal information held by government institutions.

Recommendation:

5.25 The Committee recommends that the following provision be added to the *Privacy Act* to require all government institutions covered by the Act to maintain appropriate security standards for personal information:

> **Government institutions are required to establish appropriate administrative, technical, and physical safeguards to ensure 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 about whom information is maintained.**

END NOTES

[1] Part IV of the *Canadian Human Rights Act*, the original federal measure for data protection, was repealed in 1982 and replaced by the current *Privacy Act*.

[2] This statement was provided in response to a written question from the Committee.

[3] This information was provided in response to written questions posed by the Committee.

[4] See Privacy Commissioner of Canada, *Privacy Act Audit Guide* (Ottawa, 1986, mimeographed).

[5] *Oversight of Computer Matching to Detect Fraud and Mismanagement in Government Programs*, Hearings before the Subcommittee on Oversight of Government Management of the Committee on Governmental Affairs, United States Senate, 97th Congress, 2nd Session, 15-16 December 1982 (Washington, D.C.: Government Printing Office, 1983), pp. 1-2.

[6] U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Electronic Record Systems and Individual Privacy* (Washington, D.C., June 1986, OTA-CIT-296).

[7] Privacy Commissioner, *Annual Report 1985-86* (Ottawa, 1986), p. 7. See also *Minutes of Proceedings and Evidence of the Standing Committee on Justice and Solicitor General*, Issue No. 11 (May 13, 1986): 6-7 (Hereafter cited as *Hearings*).

[8] *Ibid.*, pp. 7-8; see *James Richardson and Sons* v. *Minister of National Revenue*, (1984) 1 S.C.R. 614.

[9] See: Department of Justice, Information Law and Privacy Section, *Communiqué*, No. 6 (June, 1984), p. 9.

[10] Privacy Commissioner, *Annual Report 1985-86*, p. 7.

[11] 99th Congress, 2nd Session, S. 2756, The Computer Matching and Privacy Protection Act of 1986.

[12] A major finding of a recent study of computer matching by the U.S. General Accounting Office is relevant here: "We did not discover any agency documentation providing specific, written criteria that had been used by inspectors general or other agency decisionmakers in determining whether or not a proposed match should be implemented." (U.S. General Accounting Office, *Computer Matching. Factors Influencing the Agency Decision-Making Process* [Washington, D.C., Nov. 1986, GAO/PEMF-87-3BR], p. 2).

[13] Treasury Board Canada, *Report on Data-Matching, May 3, 1985.* The President of the Treasury Board made this Report available during his appearance before the Committee on May 6, 1986.

[14] *Hearings*, 8: 13, 24.

[15] This paragraph is based on David H. Flaherty, *The Origins and Development of Social Insurance Numbers in Canada*, Department of Justice, Ottawa, 1981, chapter 6. This study was prepared for the Privacy Commissioner.

[16] Privacy Commissioner, *Report of the Privacy Commissioner on the Use of the Social Insurance Number* (Department of Justice, Ottawa, 1981).

[17] Privacy Commissioner, *Annual Report 1985-86*, p. 44.

[18] See D.B. Scott, "The Wages of Sin," *The Financial Post Magazine*, October 1, 1985, pp. 36b-36f.

[19] Flaherty, *The Origins and Development of Social Insurance Numbers in Canada*, p. 182.

[20] Privacy Commissioner, *Annual Report 1985-86*, p. 8.

[21] See the list in *ibid.*, p. 8. The inclusion in the list of such diverse activities as race track supervision, student loans, and the Canadian Wheat Board suggests that Parliament should also review existing uses.

[22] *Ibid.*, pp. 8, 9.

[23] U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Electronic Record Systems and Individual Privacy*, especially pp. 111-12.

[24] House of Commons, Bill C-535, An Act to extend the present laws of Canada that protect the privacy of individuals and that provide individuals with a right of access to government files containing personal information relating to themselves, May 2, 1980, section 9.

[25] Bill C- 537, An Act respecting the use of Social Insurance Numbers, May 2, 1980 (Hnatyshyn); Bill C-586, An Act respecting the use of Social Insurance Numbers, May 2, 1980 (Gamble); Bill C-245, An Act respecting the use of Social Insurance Numbers, June 27, 1985 (Stackhouse); Bill C-236, An Act respecting the use of Social Insurance Numbers, October 21, 1986 (Stackhouse). The language of the three Bills is identical, except for the addition of section 3(1) to the 1986 Bill, prohibiting any "person, organization, group or body that is not a federal body" from requesting any person to disclose his Social Insurance Number.

[26] Canadian Bar Association, *National* (September, 1986), 1986 Annual Meeting, Resolution No. 2.

[27] *La Ligue des Droits et Libertés*, Press Release, Montreal, December 10, 1986.

[28] This section is based on section 7 of U.S. *Privacy Act* of 1974.

[29] The concept of exempt banks originated under Part IV of the *Canadian Human Rights Act* of 1977.

[30] One of the ironies of the Privacy Commissioner's systematic examination of all exempt banks is that he is "unable to examine the documents which established the basis upon which the Governor in Council closed the banks because these documents are confidences of the Queen's Privy Council." Privacy Commissioner, *Annual Report 1985-86*, p. 23).

[31] President of the Treasury Board to the Chairman of the Standing Committee on Justice and Solicitor General, November 6, 1986.

[32] *Re Ternette and Solicitor General of Canada*, (1984) 10 D.L.R. (4th) 587. Details are from Privacy Commissioner, *Annual Report 1985-86*, pp. 21-3, 54.

[33] *Re Ternette and Solicitor General of Canada*, (1984) 10 D.L.R. (4th) 587 at p.592.

[34] Privacy Commissioner, *Annual Report 1985-86*, p. 23.

[35] The U.S. government does allow "exempt" systems to exist under the *Privacy Act* of 1974, but individuals may seek access to their records in them. Of over 73,000 access requests to exempt systems in 1982, only one percent were totally denied (*Oversight of the Privacy Act of 1974*, p. 60).

[36] *Hearings*, 11: 30-1; 20: 19.

[37] See: France, *Act 78-17 of 6 January 1978 on data processing, data files and individual liberties*, (7 January 1978 *Official Journal of the French Republic*, 227), c. VI; Sweden: *Data Act*, 1982, ss. 20-1, 24.

[38] One federal official in Louisiana was prosecuted for releasing administrative information on an identifiable individual (*Privacy Journal*, Feb., 1977, p. 1). In St. Louis in 1982 four detectives and one private investigator pleaded guilty under the *Privacy Act* to obtaining personal records from the FBI under false pretences and selling them (*Privacy Times*, Oct. 6, 1982, p. 1).

[39] 5 U.S.C. 552a(i)(1)(2)(3)

[40] *Federal Register*, vol. 50, no. 247 (Dec. 24, 1985), 52739.

[41] *An Act respecting Access to documents held by public bodies and the Protection of personal information*, R.S.Q., c. A-2.1, chapter VII, Division I.

[42] R.S.Q., c. A-2.1, Chapter VII.

[43] *Public Government for Private People: The Report of the Commission on Freedom of Information and Individual Privacy/1980* (3 vols., Toronto, 1980), III, 764-68. These Ontario recommendations explicitly follow and accept the model of the sanctions in the U.S. *Privacy Act*, as described above.

[44] See: Sweden, *Data Act*, 1982, ss. 22-23; Quebec, *An Act respecting Access to documents held by public bodies and the Protection of personal information*, R.S.Q., c. A-2.1, articles 166-67; Ontario, Bill 34, An Act to provide for Freedom of Information and Protection of Individual Privacy, 1986, section 58(3).

[45] 5 U.S.C. 552a, section (g)(1); Circular A-130, *Federal Register*, vol. 50, No. 247 (December 24, 1985), Appendix I, section 3(7), p. 52739. New York's *Personal Privacy Protection Law* of 1983 includes civil remedies for data subjects. (1983 N.Y. Laws, c. 652, s. 97.

[46] Privacy Commissioner, *Annual Report 1985-86*, p. 35.

[47] *Ibid.*, p. 43.

[48] *Public Government for Private People*, III, 763 and, generally, 761-8.

[49] *Ibid.*, III, 764, 768.

[50] Treasury Board Canada, Circular No. 1986-26, June 18, 1986: "Government Security Policy," s. 8.1.

[51] Privacy Commissioner, *Annual Report 1985-86*, pp. 16-20; *Hearings*, 11: 9-10, 20, 22-3, 28.

[52] The recent revision of the *Young Offenders Act* is another example of failure to consult the Privacy Commissioner on a privacy-related matter. The new amendments give insurance companies the right to see the driving and conviction records of young offenders; See: *The Globe and Mail*, Aug. 12, 1986, p. 1.

[53] See: *Federal Register*, vol. 50, 52740 (Dec. 24, 1985).

[54] *Personal Privacy Protection Law*, 1983 N.Y. Laws, c. 652, s. 93(4).

[55] Further details concerning CPIC are available in David H. Flaherty, "Protecting Privacy in Police Information Systems: Data Protection in the Canadian Police Information Centre," *University of Toronto Law Journal*, XXXVI (1986), 116-48.

[56] The data on the size of CPIC files is from Flaherty, "Protecting Privacy in Police Information Systems," pp. 146-7.

[57] *Hearings*, 11: 25.

[58] See the references to these data bases in Canada, *Personal Information Index 1985* (Ottawa, 1985), pp. 27-2. 85-2, and 85-3.

[59] *President's Annual Report on the Privacy Act, 1982-83*, p. 20.

[60] These statements were offered in response to written questions posed by the Committee.

[61] Privacy Commissioner, *Annual Report 1985-86*, pp. 48-9.

[62] *Privacy Act*, 5 U.S.C. 552a(a)(7).

[63] *President's Annual Report on the Privacy Act, 1982-83*, pp. 118-21.

[64] U.S. Privacy Protection Study Commission, *The Privacy Act of 1974: An Assessment* (Washington, D.C., 1977), pp. 120, 154.

[65] 51 F.R. 18985, May 23, 1986.

[66] *Personal Privacy Protection Law*, 1983 N.Y. Laws, c. 652, s. 92(10).

[67] Treasury Board Canada, *Interim Policy Guide: Access to Information Act and the Privacy Act*, (Ottawa, 1983), Part III, section .3.6.

[68] *Hearings*, 22: 6; 28: 16.

[69] See: *Personal information: Whose business is it?, Report of the Working Group of Federal Access to Information and Privacy Officials* (Ottawa, 1986), pp. 1-8.

[70] Alan F. Westin, *Privacy and Freedom* (New York, 1967), p. 7.

[71] Organization for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Paris, 1981), p. 10.

[72] 5 U.S.C. 552a(e)(10).

CHAPTER 6

PARTICULAR ISSUES UNDER THE ACCESS TO INFORMATION ACT

A Matter of Form

In exercising the right of access, the *Access to Information Act* itself is unclear as to whether or not a specific form must be completed. Section 6 merely provides that requests for access are to be made in writing and "shall provide sufficient detail to enable an experienced employee of the institution with a reasonable effort to identify the record." However the Act contemplates that regulations be made "prescribing the procedure to be followed in making and responding to a request for access."[1] The Access to Information Regulations make the use of an "Access to Information Request Form" mandatory, unless the head of the government institution chooses to waive the requirement that the form be used.

The Committee considers the requirement of a form to be misguided. Canadians living in outlying regions may have difficulty obtaining the requisite form. The spirit of the Act is better promoted by permitting a written statement referring to the *Access to Information Act* to constitute a formal request under the Act. The distinction between a request for records under the Act and a general information request has important practical effects. If the *Access to Information Act* is not mentioned in the request, then the applicant loses all rights under the Act—the right to timely release of records, the right to review by the Information Commissioner and so forth.

Recommendations:

6.1 The Committee recommends revising the relevant Regulations so that no mandatory form be required to make a request under the *Access to Information Act*.

6.2 The Committee recommends that for statistical and administrative purposes, a written request for records which refers to the *Access to Information Act* be deemed to constitute a request under the Act.

Fees

The Committee is very concerned that the spirit of the Act not be defeated by the expense facing legitimate applicants seeking to exercise their statutory rights. At present, regulations under the Act stipulate that an application fee of $5.00 be paid as a "toll" in order to utilize the Act. Other fees may be charged, such as $10.00 for each hour in excess of five hours taken to search for and prepare the record for disclosure or examination. Regulations also stipulate $0.20 per page for photocopying the record provided. There are various fees for microfiche copies and computer processing of records stored in machine-readable form. No fees are to be charged for time incurred in considering whether exemptions from access should apply. Fees may be waived, although the Act gives no indication of the circumstances in which a "fee waiver" should be granted.

The general principle of requiring users to pay fees is found in most freedom of information schemes. The laudable objective of cost recovery, however, must be balanced against other considerations. Implementation of the *Access to Information Act* costs an estimated $3.65 million per year, whereas the average amount of fees collected amounts to less than $28,000 a year.[2] The administrative cost in processing a cheque exceeds $25.00 and, accordingly, the Treasury Board has advised in its *Interim Policy Guide* that the first $25.00 in fees generally should be waived.

Presumably the Act contemplates an application fee in order to deter frivolous requests. The Committee notes that in other jurisdictions, such as the United States, there is no initial fee. In the

spirit of promoting access, the Committee recommends that the requirement for this initial application fee be rescinded. The application fee may deter worthy access requests. In any event, the amount of money collected by application fees is minuscule: an average of less than $8,500 per year has been collected to date.[3]

Under the Act as it is presently drafted, a government institution is obliged to consider even the most frivolous requests, once the application fee is paid and any deposit lodged with the agency. The Committee notes that the Quebec *Act Respecting Access to Documents held by Public Bodies and the Protection of Personal Information* enables the *Commission d'Accès à l'Information* to authorize a government institution "to disregard requests that are obviously improper because of their repetitious or systematic nature."

In an effort to reduce the obstacle of costs, Access Coordinators appointed pursuant to the Act should be encouraged to assist users in narrowing their requests wherever possible. Section 12 of the Act allows successful applicants either to examine the record or be given a copy of the record. The Regulations, however, confirm that the government institution, not the applicant, determines which option applies. Although the Regulations are acceptable in this regard, the Committee would encourage Access Coordinators to alert applicants to their right to inspect documents rather than purchase copies. There does not appear to be a uniform practice in this regard. The Committee is also concerned that the right of inspection be made available as much as possible to those Canadians not residing in or near the National Capital Region. Government institutions should be encouraged to inform applicants of the possibility of inspecting records in regional offices or, where no regional office of the agency in question exists, in the office of the Government of Canada nearest to the applicant's residence.

Recommendation:

6.3 The Committee recommends that the *Access to Information Act* be amended to rescind the requirement of an application fee. However, the *Access to Information Act* should be amended to authorize the Information Commissioner to make a binding order enabling a government institution to disregard frivolous or vexatious requests under the Act. Such an order should be appealable to the Federal Court.

Search Fees

In keeping with the principle of cost recovery, the *Access to Information Act* contemplates that $10.00 per hour be paid for search and preparation. After more than three years of experience with the legislation, the record keeping in the various government institutions should now be better organized, making it easier for them to discharge their statutory obligations under the Act. It would be intolerable if applicants were to subsidize an agency for its poor records management. At present, the Act authorizes the Information Commissioner to investigate complaints concerning unreasonable fees. No judicial review of these matters is allowed.

Two specific problems should be noted. One arises when individuals are asked to pay fees, or deposits, and end up with no records. Another concern arises when more than one applicant seeks the same record. There appears to be no mechanism to collect from subsequent applicants and provide a proportionate refund to the first applicant, or at least to ensure that the subsequent applicants not be required to pay for a record that has already been released.

Recommendations:

6.4 The Committee recommends that there continue to be no fee levied for the first five hours of search and preparation time.

6.5 The Committee recommends that no fees be payable if a search does not reveal any records.

6.6 The Committee recommends that once a document has been released to a particular applicant, subsequent applicants should be able to review this record in the reading room of the government institution. A list of records released under the *Access to Information Act* should be available in the reading room and in the Annual Report of the government institution. Should a copy be desired by subsequent applicants, they should be required at most to pay reasonable photocopying expenses without any additional expense for search and preparation.

Photocopying Fees

The Regulations under the Act have recently been amended to reduce the photocopying charges from $0.25 per page to $0.20. In keeping with the cost recovery principle, the Committee recommends that a market rate for photocopying should become the standard. The Committee understands that the Public Archives of Canada, for example, currently charges $0.10 per page. Commercial outlets in the National Capital Region often charge less than this amount and often considerably less than the $0.20 per page stipulated in the Access to Information Regulations.

Recommendation:

6.7 The Committee recommends that the Access to Information Regulations be amended to stipulate a market rate for photocopying. The rates for photocopying should generally be consistent with the rate charged by the Public Archives of Canada, so long as this rate generally reflects prevailing market conditions in the National Capital Region.

Fee Waivers

Although the Act enables a government institution to waive the requirement to pay fees, no criteria are established. The Regulations are silent on this point as well, although the *Interim Policy Guide* prepared by the Treasury Board indicates that fees are to be waived "in the public interest". The Treasury Board does not appear to have articulated criteria for the waivers. The *Interim Policy Guide* merely states that waivers should be made on a case by case basis by assessing the following: "whether the information is normally made available without a charge; and (b) the degree to which a general public benefit is obtained through the release of the information."

As indicated above, the Treasury Board policy is that government institutions should consider waiving fees, other than the application fee, if the amount payable is less than $25.00. However, the Committee notes that the Treasury Board itself does not appear to adhere consistently to this recommendation in addressing fee waivers in connection with requests for access to its own records.

In formulating the following recommendation, the Committee has reviewed U.S. experience with fee waivers under the *Freedom of Information Act* and considered the legal decisions and pertinent legal commentary.[4] On October 27, 1986, President Ronald Reagan signed into law the *Anti-Drug Abuse Act*, part of which substantially alters the provisions of the *Freedom of Information Act* concerning fees and fee waivers.[5] Under the new law, agencies will not be able to charge search fees to educational or noncommercial scientific institutions or requesters from the news media. The general fee waiver standard will provide for fee waivers where disclosure "is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the requester." Noncommercial requesters will be entitled without charge to two hours of search time and 100 pages of duplication per request. An agency will not be permitted to demand a deposit unless the requester's prior failure to pay

a fee makes such a deposit warranted or unless the fee exceeds $250. The Committee urges the Treasury Board to monitor these developments in the United States in formulating the fee waiver policy recommended in this Report.

Recommendations:

6.8 The Committee recommends that a fee waiver policy be enacted by an amendment to the *Access to Information Act* or by regulation so that a consistent standard is applied across the Government of Canada. The following criteria should be considered:

1. Whether there will be a benefit to a population group of some size, which is distinct from the benefit to the applicant;

2. Whether there can be an objectively reasonable judgment by the applicant as to the academic or public policy value of the particular subject of the research in question;

3. Whether the information released meaningfully contributes to public development or understanding of the subject at issue;

4. Whether the information has already been made public, either in a reading room or by means of publication;

5. Whether the applicant can make some showing that the research effort is likely to be disseminated to the public and that the applicant has the qualifications and ability to disseminate the information. A mere representation that someone is a researcher or "plans to write a book" should be insufficient to meet this latter criterion.

6.9 The Committee further recommends that complaints to the Information Commissioner on fee waivers continue to be available, and that the Commissioner be empowered to make binding determinations in this regard, without further recourse to judicial review.

A Matter of Time

Under the Act, the government institution has thirty days to respond to an access request. It may be extended if the request is for a large number of records and responding within thirty days would interfere with the government institution's operations. Similarly, if necessary consultations cannot be completed within the period, or if notice is required to a third party whose interests are protected under the Act, an extension may be made unilaterally by the government institution "for a reasonable period of time, having regard to the circumstances." Notice must be given to the applicant within the thirty-day period, specifying that the applicant is entitled to complain to the Information Commissioner about the extension. An unreasonable delay may be deemed a refusal to grant access. All complaints to the Information Commissioner concerning applications for access under the Act shall be made within one year from the time when the request in question was received by the government institution.

For some users, information delayed is information denied. The Committee has heard testimony concerning delays which are clearly unacceptable, even though it must be recognized that a certain start-up time was required for many government institutions to have prepared record-keeping systems to meet the demands of the *Access to Information Act*. By now, however, problems of inadequate record keeping and inexperienced personnel can no longer justify lengthy delays. Very often it appears that the difficulties arise not with Access Coordinators but with senior officials in particular government institutions. The extent of the delay problem is perhaps best captured by Treasury Board statistics: approximately one in five complaints to the Information Commissioner involved delay.[6]

Should the initial thirty-day response period be altered? The Committee notes that a shorter period is stipulated in several jurisdictions. For example, the U.S. *Freedom of Information Act*

stipulates that an agency is to make a determination on any request for records under the Act within ten working days of receipt. Nevertheless, there are some reports to the effect that not all U.S. government agencies meet this deadline on a regular basis. Since several years have now passed since the *Access to Information Act* was proclaimed, the Committee believes that government institutions generally should be able to respond to requests on a more expeditious basis. Therefore, the Committee recommends that the initial time period in which the government institution must respond to a request be reduced to twenty days. However, it also urges the Treasury Board to monitor the cost implications of this measure and to report to the Committee on its findings within one year of the implementation of this measure.

The Committee is concerned that some government institutions appear to wait until the 29th day before informing the applicant that an extension is required. For example, the Committee was referred to correspondence contained in the Brief of the National Union of Provincial Government Employees (NUPGE). The applicant there filed its request on April 11, 1985. It was received on April 15, 1985. A letter in response was sent out by the Deputy Minister of Labour on May 14, 1985 — exactly 29 days after the request was received.[7] Similar concerns were raised by the Public Interest Research Centre [8] and by Iain Hunter, a journalist with the *Ottawa Citizen*.[9] To compound difficulties, the legislation does not formally indicate when the thirty-day period begins.

Access Coordinators and other officials in government institutions should be encouraged in concrete terms to make every effort to comply with access requests in a timely manner. The Committee recognizes that often delays are not caused by the Access Coordinators but rather by other factors. Positive incentives must be given to Access Coordinators and other officials who have endeavoured to comply with the spirit of the *Access to Information Act*. For example, the Performance Review and Appraisal Reports for public servants who administer the *Access to Information Act* should reflect their success in achieving timely compliance.

Recommendations:

6.10 The Committee recommends that the *Access to Information Act* be amended to specify that the period for processing an application commences on receipt of the application.

6.11 The Committee recommends that where the government institution fails to provide access within the time limits set out in the Act, the applicant should thereupon be notified of his or her right to complain to the Information Commissioner.

6.12 The Committee recommends that the initial response period available to government institutions be reduced from thirty days to twenty days, with a maximum extension period of forty days, unless the Information Commissioner grants a certificate as to the reasonableness of a further extension. The onus for justifying such extensions shall be on the government institution. The Treasury Board is urged to monitor the cost implications of this recommendation and to report to the Standing Committee on Justice and Solicitor General on its findings within one year of the implementation of this measure.

6.13 The Committee recommends that the *Access to Information Act* be amended to authorize the Information Commissioner to make an order waiving all access fees if a government institution fails to meet specified time limits without adequate justification.

6.14 The Committee recommends that the Treausry Board, in conjunction with the Public Service Commission, undertake a study to investigate methods for enhancing timely compliance with the *Access to Information Act*. This investigation should commence as soon as possible and a report to the Standing Committee on Justice and Solicitor General be submitted within one year.

Delays at the Office of the Information Commissioner

Any complaint under the *Access to Information Act* must be lodged with the Information Commissioner within one year from the time when the request for a particular record was received. There is no equivalent limitation imposed upon the Information Commissioner; her investigations are subject to no deadline. However, as the Act is presently worded, an applicant may not seek judicial review of a denial of access until the results of the Information Commissioner's investigation of the complaint are reported to the complainant.

The initial difficulties at the Office of the Information Commissioner may have been caused by a shortage of personnel. In addition, various government institutions appear to have inadequately grasped the importance of severing exempt portions of records from portions that could be released under the Act. This difficulty has accounted for a significant volume of delays. Another major cause of delays is the need to notify third parties and ensure that fair procedures are adopted. Often third parties are unaware of the *Access to Information Act*. Now that the Act is better understood, it is hoped that there will be some reduction in these delays. In addition, recommendations elsewhere in this Report will address some of the difficulties in notifying third parties which, in turn, should streamline procedures within the Office of the Information Commissioner.

One difficulty in imposing a specific time limitation on investigations by the Information Commissioner is that less thorough investigations may result. In the words of the Information Commissioner, Inger Hansen, Q.C., "It is a lot easier to give a fast 'no' than to mediate a 'yes'."[10] Nevertheless, the Information Commissioner has herself acknowledged that delays in her office are a matter of concern. She has also indicated that, although the current average time to complete an investigation is about four or five months, she hopes to achieve a median average time of about two or three months.[11] Although complaints about delay have been directed primarily at the Office of the Information Commissioner, any reform measures in this regard should address the Office of the Privacy Commissioner as well. At some point, similar concerns may also emerge there. In addition, the laudable attempts by those drafting the legislation to establish a uniform framework for the *Access to Information Act* and the *Privacy Act* should be endorsed by an attempt to retain a similar approach for both Offices in the legislation.

Recommendation:

6.15 The Committee recommends that both Acts be amended to impose a time limitation of sixty days on investigations by the Information Commissioner and the Privacy Commissioner. If a report of the investigation is not forthcoming within this period, a certificate shall be given to the applicant permitting a direct resort to judicial review. The certificate should contain no recommendations but simply a statement that the investigation could not be completed within the allotted sixty-day period. The applicant would then have the choice either to wait until the investigation has been completed or to seek immediate review in the courts.

Going Beyond Access Applications

The general scheme of the *Access to Information Act* is that records will be disclosed only upon an application brought by an individual. The Committee notes that the proposed Ontario Freedom of Information and Protection of Privacy Act, (Bill 34) contains an innovative provision:

> Despite any other provision of this Act, a head shall, as soon as practicable, disclose any record to the public or persons affected if the head has reasonable and probable grounds to believe that it is in the public interest to do so and that the record reveals a grave environmental, health or safety hazard to the public.

This provision goes considerably farther than the public interest override currently contained in section 20(6) of the *Access to Information Act*. The latter subsection applies only to bar the government institution from withholding certain types of confidential business information. It is triggered only when an individual applies for a record under the Act. In the proposed Ontario provision, on the other hand, there is an affirmative duty imposed on the Minister or agency head to disclose records in the circumstances specified. Such a provision would override all exemptions.

The Committee is in substantial agreement with this Ontario provision. It is fundamentally wrong for certain kinds of information to be withheld and only made available if and when it is requested formally under the *Access to Information Act*. It may be difficult, however, to enforce this obligation. At minimum, the provision would serve to protect those relying upon it from legal difficulties, if information were disclosed under the terms specified in the provision.

Recommendation:

6.16 The Committee recommends that the *Access to Information Act* be amended to add a provision requiring a government institution to reveal information as soon as practicable where there are reasonable and probable grounds to believe that it is in the public interest to do so and that the record reveals a grave environmental, health or safety hazard.

END NOTES

[1] Section 77(1)(b).

[2] Treasury Board of Canada, *Report to the Standing Committee on Justice and Legal Affairs on the Access to Information Act and the Privacy Act* (March, 1986) at p.3. A total of $61,420 was collected in fees over a 27-month period (July 1, 1983 to Sept. 30, 1985).

[3] *Ibid.* A total of $19,081 was collected in the 27-month reporting period.

[4] See, especially, *Better Government Association* v. *Department of State* 780 F.2d 86, D.C. Cir. 1986; *Ettlinger* v. *F.B.I.* 596 F. Supp. 867 (1984); the Attorney General's memorandum on the 1974 amendments to the F.O.I.A., Part II-A, and the Department of Justice Guidelines (January 7, 1983); J. Bonine, "Public Interest Fee Waivers Under the *Freedom of Information Act*" (1981) *Duke L.J.* 211.

[5] *Freedom of Information Reform Act*, being part of the *Anti-Drug Abuse Act* of 1986, Pub.L. No. 99-570.

[6] Treasury Board of Canada, *Report to the Standing Committee on Justice and Legal Affairs in the Access to Information Act and Privacy Act* (March 1986) at p.2, reporting that 18% of complaints to the Information Commissioner in the reporting period involved delays in response.

[7] *Brief* of the National Union of Provincial Government Employees (March 1986), Exhibit 2.

[8] *Brief* of the Public Interest Research Centre, (March 19, 1986), at p. 9.

[9] *Brief* of Iain Hunter (February, 1986) at p. 2.

[10] Testimony of Inger Hansen, Q.C., *Minutes of Proceedings and Evidence of the Standing Committee on Justice and Solicitor General* (May 14, 1986), 12:17.

[11] Testimony of Inger Hansen, Q.C., *Minutes of Proceedings and Evidence of the Standing Committee on Justice and Solicitor General*, 12:11

CHAPTER 7

EMERGING PRIVACY ISSUES

Electronic Surveillance

One of the newest forms of invasion of personal privacy in the 1980s involves the electronic surveillance of employees by some combination of computers, cameras, and telecommunication devices. The Privacy Commissioner pointed out in his Brief to the Committee that "Privacy protection in the workplace is an issue of quickly growing concern, a quintessential issue of the times and technology. Electronic monitoring or surveillance in the federal workplace—or anywhere else—poses a challenge to privacy protection beyond the present reach of the *Privacy Act*."[1]

Since electronic monitoring involves various aspects of personal privacy, it is necessary to distinguish between physical privacy and data protection issues and to tie electronic surveillance to data protection. The *Privacy Act* is in fact a data-protection statute in the sense that it deals with the challenges posed to individual privacy by the collection, use, storage, and dissemination of personal data. But the law does not, for example, regulate wiretapping or invasion of privacy through the use of cameras or sound-recording devices. At present, section 3 explicitly covers the fingerprints and blood type of an individual. Moreover, the definition of personal information in section 3 of the *Privacy Act* covers "information about an identifiable individual that is recorded in any form...." Thus it is possible that videotapes, urine specimens, photographs, tape recordings, and electronically-recorded personal data are covered, especially when they are recorded as personal data.

Electronic surveillance, in this context, in fact involves the collection of personal data on employees' use of computers to perform their work and also the use of computers to produce profiles of employees for various purposes. To the extent that electronic surveillance involves the collection and storage of personal data, the problem indeed represents a data-protection issue; accordingly, it clearly should be brought under the umbrella of the *Privacy Act* and should be subject to the investigatory powers of the Privacy Commissioner. With respect to the problem of electronic surveillance, the Commissioner noted that "It is at least an anomaly that someone called the Privacy Commissioner can speak out against one kind of breach of privacy but has no mandate to speak out against, much less prevent, breaches which are different only in method and may in fact be much more insidious."[2] It is apparent to the Committee that clarifications of the *Privacy Act* are in order.

The best explored examples of electronic surveillance to date concern airline reservations clerks, who work in an environment in which their every activity and conversation at a work station is monitored. At the end of each day, a profile of an individual's productivity is produced and compared to the norm. This technology may illustrate the extent to which innovations of this sort can have both positive and negative consequences.[3] Other sources of monitoring noted by the Privacy Commissioner include the use of telephones, video cameras, security and locator systems, computer terminals, parabolic microphones, as well as beepers and tonal pagers.[4]

One basic problem is that electronic surveillance or monitoring is often being introduced without consultation with the relevant employee groups and without taking into account the privacy interests of individuals and how these can best be protected in a new technological environment. All employees should have the right to consent to work in a heavily-monitored environment and to be consulted about the uses of data derived from any surveillance process. The discussion should not be what the Privacy Commissioner termed a "one-sided combat" between employer and employee.[5] There will clearly be job conditions in which security needs dictate a high level of monitoring, and others in which electronic surveillance is a dramatic form of overkill in terms of protecting human rights.

Electronic monitoring or surveillance in government institutions and in the federally-regulated workplace poses a challenge to privacy protection beyond the present reach of the *Privacy Act*.

According to the Privacy Commissioner, the present relationship between the *Protection of Privacy Act* (a 1974 law, incorporated into the *Criminal Code*, designed to control the use of wiretapping) and the *Privacy Act* is untidy and unsatisfactory. For example, it would obviously be difficult for any person to distinguish between the two statutes by their titles alone.[6] Privacy protection against electronic monitoring and surveillance is not explicitly contemplated in the *Privacy Act*.[7]

The Committee wishes to encourage the development of the *Privacy Act* into a broad-based vehicle for protecting a wide range of privacy rights claimed by residents of this country. *No longer should the Act remain solely a data protection statute.* Canada is rapidly becoming an Information Society; therefore, it is vital that additional statutory protections for the privacy of Canadians be recognized under the umbrella of the *Privacy Act*.

Recommendations:

7.1 The Committee recommends that the definition of "personal information" in section 3 of the *Privacy Act* be broadened to include all types of electronic surveillance that involve the collection of personal data in any form. To this end, videotapes, urine specimens, photographs, and tape recordings about an identifiable individual should be added explicitly to the list of "personal information" under section 3.

7.2 The Committee recommends that the Privacy Commissioner be explicitly empowered in the *Privacy Act* to monitor relevant developments in surveillance practices and to investigate complaints about these aspects of electronic monitoring and surveillance in the federal government, Crown corporations, and in the federally-regulated workplace.

Urinalysis for Drug Testing and the Use of the Polygraph

As noted above in our discussion of electronic surveillance in the federal workplace, many new technological developments result in the collection and storage of personal data pertaining to individuals; therefore, they are subject to the *Privacy Act*. This is true of the use of polygraphs in employment interviews and security screening as well as the use of urinalysis as a method for drug testing. Both practices raise fundamental issues for the protection of privacy and for data protection.

Since the *Privacy Act* is a data protection law, it is appropriate for the use of such novel practices to be subject to the legislation and to the oversight of the Privacy Commissioner through self-initiated investigations and the receipt of complaints from concerned individuals. Scrutiny of proposals to use the polygraph and urinalysis should permit a careful analysis, by informed persons, of the privacy interests that are at stake in specific situations. It is possible that the Commissioner may need to make various recommendations to Parliament to cope with these emerging problems.

There are various proposals to introduce drug testing-programs for certain federal employees, such as members of the Canadian Armed Forces, inmates in federal prisons, and applicants for employment with Air Canada and Canadian National Railways.[8] The Committee notes that the Department of National Defence and Correctional Service of Canada have plans and programs to conduct widespread compulsory drug testing, relying on the use of urinalysis in particular. It is also aware that a Quebec Superior Court judge ruled against such testing at Correctional Service of Canada's Cowansville prison on August 14, 1986, on the basis of the *Canadian Charter of Rights and Freedoms*.[9]

The Committee acknowledges as a general matter that some high risk positions may require drug testing as a periodic, and even continuing, part of the employment process. The crucial variable is that such testing has to have some reasonable and meaningful connection to the tasks or employment in question. The Committee considers it unlikely that uniform, blanket testing of all applicants for employment or all employees would be necessary or desirable.

The Committee recognizes that the results of urinalysis and polygraph tests are already subject to the *Privacy Act*, if the information is collected by a government institution subject to the Act. But these practices pose such fundamental challenges to personal privacy that they merit explicit coverage in the legislation.

Recommendation:

7.3 The Committee recommends that those aspects of the use of the polygraph and of urinalysis that involve the collection and use of personal data be fully subject to the *Privacy Act* and to the supervisory oversight of the Privacy Commissioner. The Commissioner's jurisdiction should extend to federal government institutions, crown corporations, and the federally-regulated private sector.

The OECD Guidelines on the Protection of Privacy

The starting point for Parliament to demonstrate the seriousness of its desire to protect the personal information of citizens from abuse either inside or outside the country is to extend the reach of the *Privacy Act* to include all federal government institutions (as recommended in this Report) and, in addition, to encourage the provinces and the private sector to adopt codes of fair information practices. As a country which committed itself formally on June 29, 1984 to adherence to the Organization for Economic Co-operation and Development's (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Canada accepted the obligation, among others, "to encourage private sector corporations to develop and implement voluntary privacy protection codes."

These influential *Guidelines*, which were adopted by the OECD Council in 1980, contain a minimum set of principles for the protection of individual privacy, the same sort of standards incorporated in the *Privacy Act*. In simple terms, the basic OECD principles require the following limits on the contents and methods of personal data collection:

1. Informed consent of individuals for the use of information about themselves, where appropriate;

2. The collection of only relevant, accurate and timely data, related to the purpose for which they are to be used;

3. Identification in advance of the purpose for data collection;

4. Restrictions on the re-use of data for new purposes without the consent of the individual or without legal authority;

5. Reasonable security safeguards;

6. Openness about practices with respect to the collection, storage or use of personal data;

7. A right of access for individuals to information about themselves; and

8. The accountability of the data controller for compliance with data protection measures.[10]

The Committee concurs with the following declaration by the Privacy Commissioner: "Canada played an admirable leadership role in the formulation of the (OECD) guidelines. It is difficult to understand the reluctance not to continue this role by having the guidelines implemented. Agreeing to the guidelines will seem like mere posturing, if not bad faith, unless there is a sign that Canada takes its commitment more seriously."[11] As the Privacy Commissioner stated in his last Annual Report, "there has been no evidence of even minimum encouragement by the government. No visible effort has been made to discharge this obligation ...."[12]

This bleak situation changed somewhat in late November 1986, when the Secretary of State for External Affairs, the Right Honourable Joe Clark, sent a letter to leading companies in the private sector urging voluntary support for complying with and implementing the federal government's commitment to the OECD *Guidelines*. The Department of Justice's publication entitled *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: Implications for Canada* was also distributed to the private sector along with a copy of the *Guidelines*.[13]

The United States initiated a similar program to promote private sector compliance with the OECD *Guidelines* in 1981. Approximately 200 firms subsequently indicated to the National Telecommunications and Information Administration of the Department of Commerce that they subscribed to the OECD Guidelines. Such firms are now able to pressure the U.S. federal government to protect their interests, particularly when European competitors are concerned, when there is talk of restricting transborder flows of personal data.

Recommendation:

7.4 The Committee recommends that the federal Government's 1984 commitment to foster voluntary privacy codes in the private sector in compliance with the OECD Guidelines be discharged with conviction and vigour. The burden of action falls on the Department of External Affairs and the Department of Justice. They should prepare a Report to Parliament within eighteen months of the tabling of the Committee's Report in the House of Commons on the commitments received from the private sector.

Coverage of the Federally-Regulated Private Sector

Upon introducing Bill C-43, the *Privacy Act*, for third reading in the House of Commons on June 28, 1982, the Honourable Francis Fox, then Minister of Communications, stated that "the next stage in the development of privacy legislation, (is) extension of the principles respecting the protection of personal information to the federally-regulated private sector."[14] The Committee believes that, after some ten years of experience with data protection in the federal public sector, the time is now ripe for such an extension to occur.

Other major industrial nations, including the United Kingdom, France, and West Germany, have extended their data protection laws to the entire private sector. The British *Data Protection Act* of 1984, for example, requires all personal data users and computer bureaus in both the public and private sectors to register their activities with the Data Protection Registrar.[15]

By contrast, the collection and use of personal information by the private sector in Canada is almost totally unregulated. This was the finding most recently of the *Groupe de recherche informatique et droit* (GRID) of the *Université du Québec à Montréal*, which prepared a major Report for the Quebec Government on private sector data protection problems.[16] GRID basically recommended that the Quebec Government should apply data protection rules to the entire private sector by means of legislation that would apply the OECD *Guidelines* and create a government office to oversee the private sector.[17] Professor René Laperrière of GRID also submitted a Brief and testimony to the Committee on the legal situation, favoring the application of the federal *Privacy Act* to the entire private sector.[18] He drew particular attention to the privacy problems posed by automation in the banking system.

The *Privacy Act* can and should be extended to the federally-regulated private sector in this country without adopting the licensing and registration schemes characteristic of a number of European countries. The model is the moderate type of private-sector controls incorporated in the West German Federal *Law on Data Protection of 1977* (which is discussed below).

Some examples of current problems within the federally-regulated private sector reinforce the Committee's point. At the present time, there are no statutory requirements whereby telephone companies or banks have to implement fair information practices of the type included in sections 4 to 8 of the *Privacy Act* or in the Organization for Economic Co-operation and Development's rules for the protection of personal information.[19]

In 1986, the Canadian Radio-Television and Telecommunications Commission, in a model ruling, required federally-regulated telephone companies to follow strict rules concerning the confidentiality of subscriber information.[20]

However, the primary federal statute regulating banks, the *Bank Act*, is silent as to the need for the confidentiality of customer information. Despite the customary, common-law tradition and theory of banking confidentiality, this is an unsatisfactory state of affairs.[21] There is thus a need to provide Canadians with such legal and practical protections.

The Committee is sensitive to the argument that legislative remedies should not exist or be created, if no practical problems can be demonstrated. Even the Privacy Commissioner stated in his written submission to the Committee that "arguments for extending the *Privacy Act*'s domain into the private sector at this time would seem to be doctrinaire, rather than based upon hard evidence of widespread indifference to privacy protection or horror stories."[22]

There are a variety of ways of addressing this argument. Most importantly, ensuring data protection is largely a matter of formalizing "good housekeeping" practices in personal information management and giving individuals effective remedies, if and when problems occur. The *Privacy Act* itself was not enacted in response to a series of demonstrated abuses. In fact, data protection activities in Western countries have not uncovered severe abuses of the privacy of individuals on a systemic basis. The notable exception is the path-breaking 1980 Report of the Krever Commission in Ontario on the confidentiality of health records.[23] With its subpoena power, the Krever Commission uncovered some extraordinarily offensive practices. It is thus plausible to argue that a comparable investigative Commission for the federally-regulated private sector would reveal much more customer concern about their privacy, especially in the banking system, than is currently known to the general public.[24] Individuals are known to complain to banks about perceived invasions of their privacy, but they are doing so without a full range of fair information practices at their effective disposal.

At present, only the Bank of Montreal has published a privacy code. Testimony before the Committee by the Royal Bank of Canada indicated that it was in the process of introducing and formalizing fair information practices in the form of its own privacy code. The Canadian Bankers Association further testified that it was formulating a privacy code for all federally-chartered banks.[25]

The Committee applauds these efforts at self-regulation by banks but recommends that these rights be brought within the broad scope of the *Privacy Act* for the federally-regulated private sector, including the right to complain to the Privacy Commissioner about alleged invasions of privacy.

The federally-regulated private sector in fact covers a broad range of interprovincial activities, including corporations involved in banking, cable television, pipelines, shipping, telephony, transportation, and trucking. Section 2 of the *Canada Labour Code* defines a "federal work, undertaking or business" as including navigation and shipping; interprovincial railways, canals, and telegraphs; interprovincial ferries; air transportation; radio broadcasting; and banks.[26] The Department of Labour estimates that there are approximately 25,000 employers covered by the *Canada Labour Code*, but the largest number of these are small enterprises.[27]

The Committee recognizes that there are some problems in determining how the *Privacy Act* in its current form can be made applicable to the private sector since it was designed for federal government institutions. Nonetheless, the Committee is of the view that it is necessary to create a separate section of the *Privacy Act* to cover the federally-regulated private sector in a manner

comparable to the West German system. The latter example is important because the West German model of data protection is directly comparable to the Canadian *Privacy Act*.

In West Germany, the 1977 federal *Data Protection Act* creates rules for fair information practices in the *entire* private sector, but it is primarily the responsibility of that sector to see that these requirements are implemented.[28] Each company has to appoint a senior person responsible for data protection. The office of the federal Data Protection Commissioner plays a coordinating role in implementing the requirements for the private sector under the third section of the *Data Protection Act*. It does not have actual supervisory powers, except in the areas noted below, but endeavours to remain informed of the supervision exercised by the Länder (states) with a view to ensuring coherent application of the statutory standards. The federal office does advise the federal government on data protection in the private sector and directly supervises the application of the *Data Protection Act* to certain insurance companies and banks that are a federal responsibility.

The state Ministries of the Interior are the usual authorities for the supervision of data protection in the private sector in the Länder, but their role is essentially passive. The law relies on the companies in the private sector to implement the Act themselves for the most part. The internal data protection official in each company (the controller) has responsibility for ensuring the observance of statutory rules, a right to contact the relevant state supervisory authority about a particular data protection problem, and, finally, to consult with his or her counterparts in other companies on current issues. The Länder authorities do not have the power to stop a particular practice but can investigate complaints when they are received from individuals. This latter function has resulted in some positive improvements for data protection in the private sector.

After ten years of experience, some critics in West Germany believe that the state authorities need the power to initiate investigations on their own and to conduct random audits of personal information systems. The lack of sanctions in the legislation is also viewed as a problem. Some legislative remedies are being proposed in these areas.

By applying the standards of fair information practices established in the federal *Data Protection Act*, litigation in the West German courts has influenced the private sector to strengthen data protection measures. In a September 19, 1985 decision, for example, the federal Supreme Court voided the consent clause on the blanket form for consumer consent to credit registration, which is carried out on a nationwide system covering almost the entire population. The Court held that the consent form was too general, which led the industry to produce a new form. The decision is thought to have direct implications for information collection by the rest of the private sector.[29]

The Committee wishes to take a step in the direction of the West German regulatory system for the private sector. The primary need in Canada, for the present, is to apply data protection practices equivalent to sections 4 to 9, 12 to 17, and 29 to 35 of the *Privacy Act* to the federally-regulated private sector. This would create a code of fair information practices, guarantee to individuals a right of access to their own data, and establish a mechanism for complaints to be made to the Privacy Commissioner. Such a separate part of the *Privacy Act* for the federally-regulated private sector could also be amended in the future as new problems are identified. The *Privacy Act* would thus establish general rules for fair information practices for the federally-regulated private sector, and the Office of the Privacy Commissioner would oversee compliance, including the investigation of complaints that were not settled internally and the protection of individual rights of access to data. Each organization subject to the new part of the *Privacy Act* would be required to establish the purposes and uses of the personal data it collects and to designate a senior person to be responsible for data protection within the corporation. At present, the Committee does not think it necessary to apply those sections of the *Privacy Act* that permit appeals to the Federal Court or the conduct of audits of information systems by the Privacy Commissioner to the federally-regulated private sector .

The burden and costs of extending such a stream-lined system of data protection to the federally-regulated private sector appear to be manageable and commensurate with the interests of Canadians

that merit protection. The Privacy Protection Study Commission in the United States made wide-ranging recommendations for fair information practices in the private sector during and after its hearings.[30] According to what is known about the experience of companies that implemented these recommendations on a voluntary basis, the process was not very expensive. It primarily involved reshaping existing forms and procedures when they were otherwise being reviewed and reprinted. There was apparently no sense in the United States that such data protection practices in the private sector were too expensive to implement, if reasonable lead times were followed for phasing in the requirements.

Recommendations:

7.5 The Committee recommends that the rights to data protection provided in sections 4 to 9 (the code of fair information practices), 12 to 17 (individual rights of access to data), and 29 to 35 (a mechanism for the Privacy Commissioner to receive and investigate complaints) of the *Privacy Act* be extended to the federally-regulated private sector by means of a separate part of the Act.

7.6 The Committee further recommends that the Privacy Commissioner be empowered to review and approve implementation schemes developed by organizations in the federally-regulated private sector to comply with the *Privacy Act*. He should also be authorized to report to Parliament on the degree of progress in developing satisfactory data protection plans in the same sector.

The Impact of Information Technology on Individual Rights

It is evident to the Committee that the ever-increasing use of information technology, in all its forms, by the federal government, Crown corporations, and the private sector will have a strong impact on the rights of individuals, including the right to privacy. This matter has already been addressed in part in the discussion of previous issues. No single federal government institution has responsibility for monitoring the impact of technology on civil liberties, although the Department of Communications, the Science Council of Canada, and the Canadian Radio-Television and Telecommunications Commission do pay some attention to such matters. In 1972, it should be noted, the U.S. Congress created the Office of Technology Assessment to undertake such analytical tasks on its behalf.[31]

The Committee believes that it is necessary to undertake certain research and monitoring activities on a continuing basis in order to ensure that the rights of Canadians are properly protected in the emergence of our Information Society.

A 1986 consultant's Report to the OECD's Committee for Information, Computer and Communications Policy identified significant problems for data protection in the development of the following forms of new technology: expert systems used on personal information data bases; optical character recognition methods of computerizing manual records; distributed data processing and *ad hoc* data communication; two-way electronic services; and electronic mail. The Report noted that such issues go well beyond traditional data protection problems and require oversight and monitoring by data protection authorities.[32]

The Committee would add the following practices to the list of forms of information technology that require continued monitoring for their privacy implications: the use of call-tracking devices by telephone companies and others; the installation of office automation, including mail-answering systems; the use of electronic tags and bracelets on individuals, particularly for purposes of probation; and the requirement of machine-readable passports.[33]

The Committee recognizes that assigning such additional tasks to the Privacy Commissioner will have implications for the limited resources of his Office. However, given the current period of

government restraint, the Committee believes that at least some of the relevant monitoring should be carried out by the staff of this Office in the process of conducting audits and investigations. Staff visiting government institutions can make standard inquiries about such matters as the use of microcomputers and telecommunications devices to store and transmit personal information and the extent of personal data transmissions with foreign countries.

In the Committee's view, the Office of the Privacy Commissioner should also continue to develop close working relationships with specialists in the social impact of information technology in such agencies as the Department of Communications, the Canadian Radio-Television and Telecommunications Commission, and the Science Council of Canada.

The Office of the Privacy Commissioner must also continue to develop its own expertise in the fields of information systems, automation, computers, and telecommunications, especially by encouraging existing staff to take training courses in relevant subjects. One of the deficiencies of data protection agencies in all countries is lack of sophisticated understanding of information technology, and the Committee is concerned to prevent the development of such a situation in Canada. The Office of the Privacy Commissioner is also in an excellent position to develop a network of working relationships with computer experts already in the employ of the federal government. As necessary, the Office should also retain the services of experts from the private sector and universities.

Another aspect of the impact of new forms of information technology on personal privacy and access to government information is the problem of accessing general and personal records that only exist in automated form, or exist only temporarily. This condition may become an increasing problem in future as multiple data bases are created on an *ad hoc* basis from distributed data networks and/or certain personal information banks that exist only in an automated form. Further developments may make the very concept of a personal information bank thoroughly outmoded. The basic principle remains that individuals should be able to access their own information and general government records that are automated, presumably by using a terminal in a government office or their own computer. The former scheme is in place in Swedish governmental institutions, at least on an experimental basis.[34]

Recommendations:

7.7 The Committee recommends that the *Privacy Act* be amended to provide the Privacy Commissioner with the jurisdiction to oversee the impact of information technology on personal privacy in the public sector, Crown corporations, and the federally-regulated private sector. The Committee urges that such oversight occur in consultation with the appropriate government institutions, such as the Department of Justice, the Treasury Board, Supply and Services Canada, the Department of Communications, the Canadian Radio-Television and Telecommunications Commission, and the Science Council of Canada.

7.8 The Committee further recommends that section 60 of the *Privacy Act* be amended to authorize the Privacy Commissioner to undertake related research studies on his own initiative.

7.9 The Committee further recommends the amendment of section 60 of the *Privacy Act* to permit the House of Commons to have the power to request or refer research studies to the Office of the Privacy Commissioner. It is understood that references of this type would require the allocation of appropriate resources in order to prevent the diversion of existing resources from other implementation activities undertaken by the Privacy Commissioner.

Oversight of the Use of Microcomputers

"Vastly increased numbers of decentralized (even portable) computers and undeclared collections of personal information constitute a profound new threat to principles of fair information practice enunciated in the Privacy Act."[35] This statement by the Privacy Commissioner is primarily meant to express legitimate doubts as to whether the *Privacy Act* can adequately cope with the burgeoning use of computer and telecommunications technology.

The federal government is purchasing large numbers of microcomputers or personal computers that can store and use personal data as readily as traditional, large mainframe computers. As the Commissioner noted, "the personal computer's ability to develop its own records systems and share information without leaving an audit trail raises new and far-reaching threats to privacy protection."[36]

Neither the Department of Communications nor any other government institution submitted any evidence to the Committee on the social impact of microcomputers, although they were invited to do so. Even though the use of microcomputers to store personal data is fully covered under the terms of the current *Privacy Act*, the practical problem facing the Committee is to determine whether the implementation activities under the legislation are adequate to meet the challenge.

In Canada and the United States, the growth in the use of computers by the federal governments has been exponential. Treasury Board's annual review of information technology and systems estimates that the "installed base of microcomputers in the federal government was about 6,700 units on March 31, 1985." During 1984-85, the federal government acquired some 1,700 microcomputers at a cost of $20 million. It was estimated that in fiscal year 1985-86, some $25 million would be spent on computers.[37]

The Privacy Commissioner's testimony to the Committee about the impact of microcomputers should be emphasized:

> The exponential growth of microcomputers inside and outside of government imposes a new and still unquantifiable challenge to privacy protection. Personal information, accurate or inaccurate, can be compiled, retrieved, disclosed or manipulated without the subject's knowledge in microcomputers as easily as in mainframes.
>
> The new concern, of course, is that micro or personal computers confer this power upon ever-increasing numbers of individuals.... Anyone with a personal computer on a desk is the master of a machine with the storage capacity of many filing cabinets, with the potential for linking up with other similar computers and, even, access to centralized record systems.[38]

The Committee shares the concerns of the Privacy Commissioner and applauds his continuing efforts to identify such problems.

Recommendations:

7.10 The Committee recommends that the Department of Justice, the Treasury Board, government institutions, and the Privacy Commissioner develop new policies and practices to cope with the emerging data protection problem posed by personal information held and used in microcomputers.

7.11 The Committee recommends that the Department of Justice, the Treasury Board, and the Privacy Commissioner make separate reports to Parliament on appropriate responses to this emerging problem within eighteen months of the tabling of the Committee's Report in Parliament.

The Regulation of Transborder Data Flows

Canadians are especially sensitive to the movement of their personal data in and out of the country by governments and the private sector by various modes of communication, including computer and satellite transmissions. There is an understandable fear that various kinds of personal information are being removed from the geographical confines of this country and beyond of the control of Canadian law. Although there are many other economic and trade aspects of transborder data flows that may deserve a high priority at present, the privacy aspects have not received adequate governmental attention to date.

The type of privacy problem addressed under the rubric of transborder data flows is really rather simple. Personal data on Canadians is routinely being transferred and stored outside of the country by federal or provincial governments and the private sector. Since such activities do occur, to at least a certain extent, what data protection measures, if any, are in place?

It is sometimes suggested that such personal data transfers rarely occur from Canadian shores. The Royal Bank of Canada, for example, states that it does not routinely move identifiable customer data in connection with transactions. But European countries, with a longer tradition of effective data protection than Canada, have discovered significant transfers in such fields as labour and the personnel data of multinational companies as well as medical and health research.

Canadians in particular deserve to know more about transborder data flows of their personal information in such varied fields as banking, credit information systems, credit card services, health care information, labour unions, personnel and payroll records, airline travel reservations, and general government activities. Such international data transfers are subject to controls under European data protection laws.

A specific example of a data protection problem is presented by the Medical Information Bureau (MIB), which has its principal offices in Greenwich, Connecticut and its computers for storing data in Boston. Life insurance companies routinely query the data base on bad insurance risks maintained by MIB on behalf of North American life insurance companies. This practice requires a Canadian insurer to send sensitive data on the health experience of identifiable individuals to a foreign destination. If this is indeed the case, then Canadians have the right to know what fair information practices are in place at the MIB. As of 1977, 6.2 percent of the 10 million reports on file with MIB were on Canadians. As noted by Mr. Justice Horace Krever, such information is "beyond the reach and protection of Canadian law."[39] The Committee agrees with the Privacy Commissioner that it is at least somewhat premature to raise alarms about transborder data flow and privacy, when Canada has done so little to implement the OECD *Guidelines*, nine of the ten provinces do not have data protection laws, the *Privacy Act* has not been extended to cover all government institutions, and too few non-government institutions have established and honored their own effective privacy codes.[40] However, since the Committee is recommending action on a number of these matters in this Report, it also wants to encourage the Government to study prospective remedial measures on transborder data flows in areas where they may be necessary. It notes with interest that the recent study for the Quebec Government by the *Groupe de recherche informatique et droit* recommended that the provincial government itself should take responsibility for oversight of transborder data flows.[41]

The Committee has resisted the temptation to ask the Privacy Commissioner to conduct and table in Parliament such a special study under section 60 of the *Privacy Act*, since the resources and expertise needed for such an undertaking are spread across the government. Indeed, a number of major government institutions, especially the Department of External Affairs and the Department of Justice, already have significant responsibilities for the privacy aspects, and other important aspects, of transborder data flows. Unfortunately, these oversight roles have not attracted adequate attention or resources in recent years.

What is needed is for these lead agencies to coordinate a study of the privacy implications of transborder data flows, spreading their net wide enough to include representatives from the Department of Communications, the Office of the Privacy Commissioner, the Canadian Radio-Television and Telecommunications Commission, and the Science Council of Canada, as well as appropriate provincial agencies and private-sector associations. One of the first tasks for such a study group should be an examination of the implications for Canada of the coming into force on October 1, 1985, of the Council of Europe's *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.*[42] Since this Convention has the force of law in member countries, it is quickly becoming the major international statement on data protection.

Recommendation:

7.12 The Committee recommends that the Government conduct a review and study of the implications of transborder data flows by the public and private sectors for the personal privacy of residents of this country. Such a study should be tabled in Parliament within one year of the tabling of the Committee's Report.

END NOTES

[1] Privacy Commissioner, *Annual Report 1985-86* (Ottawa, 1986), p. 9.

[2] *Ibid.*, p. 10.

[3] For details of this practice and expressions of concern by organized labour in southern Alberta, see Peter Lowrey, "Messages give unions Big Brother visions," *Calgary Herald*, Oct. 20, 1986; and, more generally, Wilfred List, "Electronic monitoring sparks new debate in the workplace," *The Globe and Mail*, Sept. 22, 1986, p. B4.

[4] Privacy Commissioner, *Annual Report 1985-86*, p. 9.

[5] *Ibid.*

[6] In a related development, the British Columbia Police Commission, in a Report to the provincial Attorney General, has urged the federal government to amend the *Protection of Privacy Act* to control the use of video surveillance of private conduct by police in Canada (*The Globe and Mail*, Jan. 14, 1987, p. A4). In 1986, the Deputy Chief of the Niagara Regional Police and the Canadian Civil Liberties Association had lobbied the Solicitor General of Ontario to the same end (*ibid.*, March 7, 1986).

[7] For a very timely study of the *Protection of Privacy Act*, see Law Reform Commission of Canada, *Electronic Surveillance* (Working Paper 47, Ottawa, 1986.

[8] On drug testing by the Canadian Armed Forces, see *The Globe and Mail*, Aug. 18, 1986, p. A3; for Correctional Services Canada, see *ibid.*, Oct. 1, 1986, p. A11; for Air Canada, see *ibid.*, Oct. 1, 1986, p. A11; for the CNR, see *ibid.*, Sept. 9, 1986, p. A8. In June, 1986, the Office of the Judge Advocate General, Department of National Defence, submitted an eighteen page document entitled, "Canadian Forces Proposed Urinalysis Programme," to the Standing Joint Committee of the Senate and of the House of Commons on Regulations and Other Statutory Instruments. The Commissioner of Correctional Services Canada had correspondence on the same subject with the same Committee in the spring of 1986.

[9] *Jean-Pierre Dion* v. *Attorney General of Canada and Correctional Services Canada*, Quebec Superior Court, Aug. 18, 1986, reported at (1986) R.J.Q. (C.S.) 2196.

[10] See Organization for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Paris, 1981); and Department of Justice, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: Implications for Canada* (Ottawa, 1985). The latter is also available as Ministère de la Justice, *Les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de l'OCDE: Incidences pour le Canada* (Ottawa, 1985).

[11] Privacy Commissioner, *Annual Report 1985-86*, p. 13; *Minutes of Proceedings and Evidence of the Standing Committee on Justice and Solicitor General*, Issue No. 11 (May 13, 1986): 25. Hereafter cited as *Hearings*.

[12] Privacy Commissioner, *Annual Report 1985-86*, p. 13.

[13] Department of Justice, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: Implications for Canada.*

[14] *House of Commons Debates*, vol. 124, No. 370, column 18854.

[15] *Data Protection Act* 1984, c. 35, section 4.

[16] Groupe de recherche informatique et droit, *L'identité piratée: Étude sur la situation des bases de données à caractère personnel dans le secteur privé au Québec et sur leur réglementation en droit comparé et international* (Société québécoise d'information juridique, Montréal, 1986), pp. 189 and, generally, 119-89.

[17] *Ibid.*, pp. 278-317, 320-26.

[18] *Hearings*, Issue No. 16 (May 27, 1986): 7-22.

[19] See: Organization for Economic Co-operation and Development, *Guidelines on the Protection of Privacy.*

[20] According to section 11 of the newly-effective Terms of Service:

> 11.1 Unless a customer consents in writing or disclosure is pursuant to a legal power, all information kept by the Company regarding the customer, other than the customer's name, address and listed telephone number, are confidential and may not be disclosed by the Company to anyone other than:
>
> - the customer;

- a person who, in the reasonable judgement of the Company, is seeking the information as an agent of the customer;

- a company involved in supplying the customer with telephone directories, provided the information is required for that purpose; or

- an agent retained by the Company in the collection of the customer's account, provided the information is required for that purpose.

11.2 The Company's liability for disclosure of information contrary to Article 11.1 is not limited by Article 16.1.

11.3 Upon request, customers are permitted to inspect any Company records regarding *their service*. (Telecom Decision CRTC 86-7, *Review of the General Regulations of the Federally-Regulated Terrestrial Telecommunications Common Carriers, Terms of Service* [March 26, 1986]).

[21] The classic case is English: *Tournier* v. *National Provincial and Union Bank of England*, (1924) 1 K. B. 461 (C.A.). The case was cited with approval in *Haughton* v. *Haughton*, [1965] 1 O.R. 481 at 482.

[22] The issue is discussed in somewhat more muted language in Privacy Commissioner, *Annual Report 1985-86*, p. 11.

[23] Ontario, *Report of the Commission of Inquiry into the Confidentiality of Health Information* 3 vols., Toronto, 1980.

[24] Some detailed information on the public's concerns about the treatment of personal information by banks can be found in a national survey conducted by the Royal Bank of Canada in 1984. See: *1984 Royal Bank of Canada Privacy Study*, Public Affairs Department, Royal Bank of Canada, Montreal, August, 1984. The Bank submitted a copy of this survey to the Committee.

[25] See: *Hearings*, Issue No. 25 (June 10, 1986), 5, 9, 18.

[26] *Canada Labour Code*, R.S.C. 1970, c. L-1.

[27] The Department of Labour maintains a list of such employers. As of January 3, 1987, only 65 of these employers, including some Crown corporations already subject to the *Privacy Act*, had more than 500 employees.

[28] *Act on Protection against the Misuse of Personal Data in Data Processing of January 27, 1977*, Parts III and IV. See Dr. Werner H. Ruckriegel, "Private Sector Data Protection Control in Germany," *Transnational Data Report*, V. March, 1982, 95-6.

[29] See: *Transnational Data and Communications Report*, IX, No. 10 (Oct., 1986), 24.

[30] See: *Personal Privacy in an Information Society. The Report of the Privacy Protection Study Commission* (Washington, D.C., 1977).

[31] For examples of relevant publications, see the Office of Technology Assessment's three-part study of "Federal Government Information Technology: Congressional Oversight and Civil Liberties," published between October, 1985 and June, 1986.

[32] See: Dr. J. Bing, *Impact of Developing Information Technology on Data Protection Legislation* (OECD: Committee for Information, Computer and Communications Policy, Paris, 1986, ICCP[86]5), pp. 14-31, 49.

[33] Stories on each of these practices can be found in *The Globe and Mail*, Jan. 17, 1986; Oct. 1, 1985; Nov. 1, 1985; and Feb. 7, 1986.

[34] See: Cecilia Magnusson, *Offentlighetsprincipens tillämpning på myndigheters dataregister. En fälstudie och enkätundersökning* [The Application of the Swedish Principle of Publicity to Computer Records Kept by Public Authorities-A Field Study] (Stockholm: Institutet för Rättsinformatik, Stockholms Universitet, 1983, IRI-rapport 1983: 7).

[35] Privacy Commissioner, *Annual Report 1985-86*, p. 7.

[36] *Ibid.*, p. 7.

[37] *Ibid.*, p. 6. See also the discussion of the impact of microcomputers in Office of Technology Assessment, *Federal Government Information Technology: Electronic Record Systems and Individual Privacy* (Washington, D.C., June, 1986), pp. 24-5, 109-11.

[38] Privacy Commissioner, *Annual Report 1985-86*, p. 7.

[39] Ontario, *Report of the Commission of Inquiry into the Confidentiality of Health information*, III, 221, 231 and, generally, chapter 20.

[40] Privacy Commissioner, *Annual Report 1985-86*, p. 12.

[41] Groupe de recherche informatique et droit, *L'identité piratée*, pp. 304-5.

[42] See: Council of Europe, *Explanatory Report on the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (Strasbourg, 1981). Compare Nigel Savage and Chris Edwards, "Transborder Data Flows: The European Convention and United Kingdom Legislation," *International and Comparative Law Quarterly*, XXXV (1986), 710-17.

CHAPTER 8

OTHER ACCESS ISSUES

The Committee's mandate has been set out in section 75 of the *Access to to Information Act*. It has not only been able to examine the "administration" of the legislation but it has also endeavoured to undertake a "comprehensive review of the provisions and operation of this Act". However, the Committee's jurisdiction has not extended beyond the four corners of the *Access to Information Act*. Nevertheless, there have been substantial developments both in Canada and abroad within the field broadly defined as the public's right to know. Accordingly, the Committee has noted a few of these developments for future consideration by Parliamentarians.

Official Secrets Act

The *Official Secrets Act*[1] is a loosely-drafted statute which imposes a serious restraint on public servants. This statute is virtually identical to a British statute of 1911 and its restrictions are couched in language virtually the same as that used by the British parliamentary drafters on the eve of World War I. The legislative intent in passing the *Official Secrets Act* was to deter espionage. However, since it is couched in very sweeping and ambiguous language, the Act encompasses much more than the traditional notions of spying. Similarly, the Act embraces far more than classified information; the communication of *any* information in the public domain may attract the criminal sanction of fourteen years' imprisonment.[2] The Act also makes it an offence for one to *receive* information, knowing or having reasonable grounds to believe it has been illegally procured.[3] The Royal Commission on Security[4] and the Franks Committee[5] in England and the McDonald Commission of Inquiry concerning certain activities of the RCMP[6] have all recommended substantial reform of the *Official Secrets Act*. It appears that only the sparing exercise of the Crown's discretion to prosecute has tempered the rigidity of this statute.

Recently, the Government has indicated that it is re-examining the *Official Secrets Act* for the purposes of reform. The Law Reform Commission of Canada has also made sweeping recommendations in this regard.[7] The Law Reform Commission notes in its Working Paper that the *Official Secrets Act* "can fairly be condemned as one of the poorest examples of legislative drafting in the statute books."[8] Although it may be technically possible for the *Official Secrets Act* to co-exist with the *Access to Information Act*, the Committee encourages the Government of Canada to pursue its reform efforts in this regard.

The System for the Classification of Documents

The Royal Commission on Security released its Report in 1969.[9] The Report analyzed the categories for the classification of official information. It noted that there is no statutory authority for classification - the entire system was set out in a Cabinet Directive which constituted an exercise of the Royal Prerogative. There was considerable confusion as to who has authority to classify documents into the four categories of Top Secret, Secret, Confidential, and Restricted.[10]

The classification system was extremely ambiguous and difficult to apply with any degree of precision. Before an individual could be permitted access to material classifed higher than "Confidential", he or she had to pass a security clearance undertaken by the RCMP; a field investigation was also required for those granted access to "Top Secret" information. The Royal Commission on Security recommended that the lowest of the four categories, "Restricted" be abolished.[11] Another concern was that there was no explicit system for the declassification of documents.

On June 18, 1986, the Honourable Perrin Beatty, then Solicitor General of Canada, announced substantial reforms to the administrative security policies. Although these policies do not affect requests for records or personal information under the *Access to Information Act* and *Privacy Act*, they have an indirect impact on this legislation, since the new policies are designed to reduce the amount of information which is classified and, accordingly, more likely to be withheld under certain exemptions in the legislation. Under the new policy, information will only be security classified if it falls into one of six areas: national defence, international affairs, national security (including hostile and subversive activities and threats to the security of Canada), Cabinet confidences, federal-provincial affairs, and selected economic interests of Canada. In defining these categories, the language in the exemptions contained in the *Access to Information Act* and the *Privacy Act* has been followed.

Fewer government positions now require security clearances; the level of security clearance is tied directly to the degree of injury the official could cause if the information in question were wrongly disclosed. Based on the degree of injury, there are now only three levels in the classification system: Top Secret, Secret, and Confidential.

The Committee will closely monitor these recent reforms to the classification system and administrative security policies.

Oath of Secrecy

Upon joining the Public Service, every public servant must swear the oath of office and secrecy in which he or she affirms:

> I... will not, without due authority...disclose or make known any matter that comes to my knowledge by reason of such employment.[12]

Earlier Committees of Parliament have heard considerable criticism of this oath. For example, D.F. Wall, then of the Privy Council Office, has testified: "The oath [of secrecy] has no basis in law as I understand it, so there are no legal sanctions. There are administrative sanctions...".[13] Likewise, Gordon Robertson, then Secretary to the Cabinet for Federal-Provincial Relations, testified: "...[T]he oath is too sweeping in its terms. It is unrealistic and it lends itself to ridicule really, and a failure to abide by it because of that."[14]

Despite such assessments of the oath of secrecy, its existence undoubtedly contributes to the aura of secrecy in the public service. The Committee is of the view that reform in this area is warranted. A future Committee of Parliament should assess the impact of the oath of secrecy.

"Whistleblowing"

Should one prosecute a public servant who violates the oath of office by releasing information that demonstrates wrongdoing? If the public servant acts in good faith, and it is later determined on an objective basis that the disclosure was indeed in the public interest, should the public servant be disciplined? This issue has been the subject of considerable debate in recent years. So-called "whistleblowers" have been granted statutory protection in the United States under the *Civil Service Reform Act*,[15] which is designed to encourage federal employees who make disclosures that serve the public interest by bringing about reductions in government expenditures, fraud, waste and other abuse.

The Committee heard some testimony on the issue of whistleblowers. For example, the Public Interest Research Centre sought protection for whistleblowers from possible prosecution under section 111 of the *Criminal Code* and from their dismissal from employment.[16] Similarly, in a private members' Bill, Bill Vankoughnet, M.P. has sought to amend the *Canadian Human Rights Act*, the *Canada Labour Code*, and the *Public Service Employment Act* specifically to provide appropriate

sanctions against retaliatory discharges of public sector employees who "blow the whistle" on serious misconduct by their employers.[17] Among other things, this Bill would stipulate that there would be no breach of the oath of secrecy where a public servant in good faith is found to have reported serious misconduct on the part of his or her employer.

Similarly, the Ontario Law Reform Commission has recently recommended an elaborate framework for the protection of whistleblowers.[18] Under both the *Access to Information Act* and the *Privacy Act* the disclosure in good faith of any record or personal information is not to attract either civil or criminal consequences.[19] The Committee encourages Parliament to consider fully the implications of legislation designed to protect "whistleblowing" and urges the House of Commons to refer the issue to an appropriate Committee for thorough consideration.

Canada Evidence Act and Crown Privilege

When the *Access to Information Act* and the *Privacy Act* were introduced, they constituted two Schedules to Bill C-43.[20] The third Schedule to the Bill constituted amendments to the *Canada Evidence Act* which were introduced to deal with the disclosure of information in judicial proceedings. Section 41 of the *Federal Court Act* [21] was repealed and replaced by new provisions of the *Canada Evidence Act*. As Mr. Justice Mahoney has observed,

> ...Parliament has manifestly found it expedient to substitute a judicial discretion for what was heretofore an absolute right on the part of the executive to refuse disclosure. ...The executive had been unable to sustain the credibility of the system of absolute privilege codified in subsection 41(2) [of the *Federal Court Act*].[22]

Under the new provisions, a Minister of the Crown "or other person interested" may object to the disclosure of information before a court, person or body with jurisdiction to compel its production by certifying that the information should not be disclosed on the grounds of a specified public interest. Where this objection is made in a superior court, the court may examine or hear the information and order its disclosure if, in the circumstances, it concludes that "the public interest in disclosure outweighs in importance the specified public interest."[23] Where an objection to the disclosure of information is made on grounds pertaining to international relations or national defence or security, the objection may be determined only by the Chief Justice of the Federal Court or his designate. Where a Minister of the Crown or the Clerk of the Privy Council objects to the disclosure of information before a court or other body with the power to compel its production, he or she may certify in writing that the information constitutes a "Cabinet confidence," which is currently defined in the same manner as this term is defined in the *Access to Information Act* and the *Privacy Act*. In this case, the disclosure of the information shall be refused without examination or hearing of the information by the court or other body.[24]

The latter provision pertaining to Cabinet confidences appears to be completely at odds with common-law developments in Canada. The notion of an absolute statutory bar to judicial examination of an entire class of records is inconsistent with recent judicial authority. The Supreme Court of Canada in a unanimous judgment has determined that it may inspect certain provincial Cabinet documents, despite a claim by a provincial government that the entire class of Cabinet documents was protected.[25] The Supreme Court recognized that there may be certain Cabinet records, such as those relating to national security or diplomatic relations, which might well be withheld even without judicial inspection.[26] Nonetheless, the Court rejected any concept of an entire class of records being off-limits; in each case, it reserved the right to inspect the documents and determine whether, on balancing the competing interests, they should be produced.

Accordingly, the Committee recommends that the *Canada Evidence Act* be brought into conformity with these common-law developments. There would appear to be little reason why the same approach contained in the *Canada Evidence Act* for considering the disclosure of information concerning international relations, national defence or national security could not be applied to Cabinet records.

Recommendation:

8.1 The Committee recommends that section 36.3 of the *Canada Evidence Act* [Cabinet confidences] be deleted and that section 36.2 of this Act be amended to add a reference to disclosure on the grounds that the disclosure would reveal Cabinet confidences. For the purpose of this provision the definition of "confidence of the Queen's Privy Council for Canada" should be amended to conform with the amended definition of this provision as recommended in Chapter 3 of this Report.

Difficulties have arisen in the litigation context when courts are called upon to examine the same personal information or records requested under the *Access to Information Act* or the *Privacy Act*. Is a certificate filed by a Minister under the *Canada Evidence Act* conclusive as to issues that a court is to determine on appeal pursuant to the *Access to Information Act* or the *Privacy Act*? This issue is currently before the Federal Court of Canada.[27] The resolution of this issue should be carefully analyzed by Parliament in order to clarify the relationship between the three statutes.

"Sunshine" Legislation

Over ten years ago, an overwhelming majority of the U.S. Congress signed into law a statute entitled the *Government in the Sunshine Act*.[28] "Open meeting laws" have been enacted by almost all state governments in the United States as well. This legislation has made a considerable difference to the way in which these governments transact the public's business.[29] The U.S. federal Act stipulates that most federal agencies must be open to the public and may be closed only if the majority of the agency's members vote to close the proceedings on certain specific grounds. The public is required to have advance notice of all meetings and, if a meeting is to be closed, an explanation must be provided. Where meetings are closed to the public, records of deliberations must be kept and the records that do not reflect exempt matters must be released on request.

The Committee considers that the U.S. experience with "sunshine" legislation should be carefully considered by a future parliamentary committee in order to determine whether analogous legislation should be implemented for the various institutions and agencies of the Government of Canada.

END NOTES

[1] R.S.C. 1970, c.0-3

[2] British cases tend to support this interpretation. For example, in *Rex* v. *Crisp and Homewood* (1919) 83 J.P. 121, [1921] 1 K.B. 451, a War Office clerk was convicted of passing information concerning the procurement of officers' uniforms to a firm of tailors. The court rejected a submission that this kind of information was not intended to be covered by the Act. See also the Canadian cases of *R.* v. *Biernacki* (1962) 37 C.R. 226, and *R.* v. *Boyer* (1946) 94 C.C.C. 195.

[3] *Official Secrets Act*, R.S.C. 1970, c. 0-3, section 4(3).

[4] *Report of the Royal Commission on Security* (Abridged), June, 1969 (the "MacKenzie Report"), at 77.

[5] *Departmental Committee on section 2 of the Official Secrets Act*, 1911 (1972) HMSO, Cmmd. 5104 (the "Franks Report"), at p. 37.

[6] *Commission of Inquiry concerning Certain Activities of the Royal Canadian Mounted Police* (The McDonald Commission) (Ottawa, 1981), Part IX, Chapter 2.

[7] Law Reform Commission of Canada, *Crimes Against the State*, Working Paper 49, Ottawa, 1986.

[8] *Ibid.* at p. 30.

[9] *Report of the Royal Commission on Security* (Abridged), June, 1969 ("the MacKenzie Report").

[10] *Ibid.* at p. 69-70.

[11] *Ibid.* at p. 72.

[12] *Public Service Employment Act*, R.S.C. 1970, c. P-32, schedule III.

[13] *Minutes of Proceedings and Evidence of Standing Joint Committee on Regulations and Other Statutory Instruments*, (30th Parl. 1st sess.) (1974-75); 48:26 (Nov. 18, 1976).

[14] *Ibid.*, 32:15 (June 25, 1975).

[15] 5 U.S.C. sections 1206-1208 and 2302 (1982).

[16] *Brief* of the Public Interest Research Centre, (March 19, 1986), at p. 23.

[17] Bill C-229, First reading, October 20, 1986.

[18] Ontario Law Reform Commission, *Report on Political Activity, Public Comment and Disclosure by Crown Employees* (1986) at pp. 332-352.

[19] Section 74, *Access to Information Act*; and section 74, *Privacy Act*.

[20] Bill C-43 received Royal Assent on July 7, 1982, and became c. 111 of S.C. 1980-83. The *Access to Information Act* was Schedule I in this Bill, the *Privacy Act* Schedule II and the amendments to the *Canada Evidence Act* constituted Schedule III.

[21] R.S.C. 1970 (2nd supp.), c. 10.

[22] *Gold* v. *The Queen in Right of Canada* (1986) 18 *Admin. L.R.* 212 at 221 (Federal Court of Appeal, per Mahoney J.).

[23] Section 36.1(2) of the *Canada Evidence Act*.

[24] Section 36.3 of the *Canada Evidence Act*.

[25] *Carey* v. *Her Majesty the Queen in Right of Ontario* (unreported decision of the Supreme Court of Canada, December 18, 1986 per La Forest, J.).

[26] In this connection, the Supreme Court of Canada has endorsed the judgment of the Federal Court of Appeal in *Goguen* v. *Gibson* [1983] 2 F.C. 463.

[27] *Re Gold and the Minister of National Revenue* and *Re Gold and the Director of the Canadian Security Intelligence Service* (Federal Court Trial Division, T-236-85 and T-1335-86).

[28] *Government in the Sunshine Act*, Pub.L. No. 94-409, 90 Stat. 1241 (1976).

[29] See: S. Stephenson, *"Government in the Sunshine Act*: Opening Federal Agency Meetings" (1976) 26 *Am. U.L.Rev.* 154.

CHAPTER 9

CONCLUSIONS

It is appropriate to begin this chapter with several general considerations.

First, the Committee would like to emphasize its awareness that Canadians do not as yet enjoy an explicit constitutional right to privacy under the *Canadian Charter of Rights and Freedoms*. In the Special Joint Senate-House of Commons Committee on the Constitution in 1981, the Honourable David Crombie, M.P., proposed the inclusion of a constitutional right of privacy in the *Canadian Charter of Rights and Freedoms*, but this amendment was defeated by a vote of fourteen to ten.[1] More recently, the Supreme Court of Canada has discussed the "reasonable expectation of privacy" in its decision in the case of *Hunter* v. *Southam*.[2] The absence of a common-law and/or Charter-based right to personal privacy in Canada is a significant impediment to the protection of individual rights; therefore, the specific kinds of protections incorporated in such legislation as the *Privacy Act* are increasingly important.

When the time arrives to consider amendments to the *Canadian Charter of Rights and Freedoms*, the Committee believes that serious consideration should be given to creating a simple constitutional right to personal privacy. The California constitution, for example, says that residents of that state have a right to privacy.[3] Individuals can then use the courts to assert all their claims to privacy.

Even though the Supreme Court of Canada has already begun to use privacy language in its interpretation of the Charter, which may lead to the gradual development of an acknowledged constitutional right to privacy, the idea of amending the Charter explicitly for this purpose has much to recommend it.

Resource Implications

In the Committee's view, it is necessary to discuss the resource implications of its recommendations concerning the *Access to Information Act* and the *Privacy Act*. We are well aware that the 1980s continue to be a period of budgetary restraint, in which careful control of expenditures is one of the major concerns of government.

It is fortunate that many of the Committee's recommendations can be adopted within the existing structure for implementation of the legislation, including the Information Law and Privacy Section of the Department of Justice, the Information Management Division of the Administrative Policy Division of the Treasury Board, and the Access to Information and Privacy Coordinators in individual government institutions.

The Committee acknowledges that its recommendations have significant implications for the Offices of the Information Commissioner and the Privacy Commissioner, particularly the latter. Both Commissioners have been urged to scrutinize the information practices of Crown corporations, However the Privacy Commissioner has also been asked to oversee the federally-regulated private sector. Moreover, there will be need for at least a modest increase in their travel and public information budgets in order to allow for the promotion of public knowledge and understanding of the legislation.

The current staff and budget of the Privacy Commissioner may also need to be increased in order to handle the additional tasks that the Committee has recommended, even if, as expected, these tasks are phased-in over a period of years in order to allow for appropriate training of staff. The new tasks that will create significant additional work include: oversight and investigation of complaints about the use of electronic surveillance of employees, of urinalysis for drug testing, and of the polygraph as a lie detector. It seems likely that the latter category will not prove to become an onerous burden once

guidelines have been developed on the use of such technology under the *Privacy Act*. Here again, the Office of the Privacy Commissioner will be less the initiator of policy than a respondent to and critic of what government institutions are proposing. It is also true that such data protection problems are unlikely to appear in Canada without other countries also encountering similar problems. The Privacy Commissioner's regular contacts with his counterparts in other countries and provinces should facilitate the solution of such problems in an expeditious manner.

The Office of the Privacy Commissioner will also have to strengthen the research side of its operation in order to continue to monitor and report on developments in information technology with implications for personal privacy, including the increasing storage of government data on microcomputers and transborder data flows of personal information, and to carry out studies on its own initiative or at the direction of Parliament and/or the Minister of Justice. It is obvious that such studies cannot be carried out without adequate budgetary and human resources.

It is also important, in the Committee's view, for the Privacy Commissioner to carry out such monitoring and research using existing federal government resources, whenever possible, such as the expertise available from the Department of Communications, Supply and Services Canada, the Canadian Radio-Television and Telecommunications Commission, and the Science Council of Canada. The Committee believes that such activities can and should take place under multiple sponsorship and direction in order to relieve the burden on the Office of the Privacy Commissioner.

Perhaps the most significant new task assigned to the Office of the Privacy Commissioner as a consequence of the Committee's recommendations is the extension of his oversight to the federally-regulated private sector, since this includes such widespread institutions as banks, cable television companies, and telephone companies, among others. The Committee has no inclination to undermine and bureaucratize the Privacy Commissioner's office, but it also is insistent on the need for such general oversight and investigation of complaints. The Committee is of the tentative view that oversight of the federally-regulated private sector might not involve too much work on a continuing basis, if, as the Committee intends, the new scheme is designed to be largely self-executing. If a section of the *Privacy Act* is designed for this part of the private sector, then commercial banks, for example, will be in the same position vis-à-vis the Office of the Privacy Commissioner as federal government institutions currently are, that is, they will receive advice rather than directives.

The 1983 organization chart for the Office of the Information and Privacy Commissioners, which was designed by Treasury Board, listed 59 positions: 20 for the Privacy Commissioner, 15 for the Information Commissioner, and 24 for their joint management and personnel services. If one divides these figures for support staff proportionately between the two Commissioners, the Privacy Commissioner was intended to have a total staff of 34.

In practice, both Commissioners have been resistant to bureaucratic tendencies and reluctant to expand staff too quickly. Actual total staff strength was 51 person-years in the year ending March 31, 1986 versus 57 person-years allocated in the 1985-86 Main Estimates.[4] Thus there were positions already available to the Privacy Commissioner that had not been used.

As of January 1, 1987, the Office of the Privacy Commissioner had a staff of 23 persons, the Information Commissioner had 20, and corporate management had 14, for a total of 57 person-years. If one attributes to the Privacy Commissioner a proportionate number of the corporate staff currently shared with the Information Commissioner, the total number of staff currently working for his office is about 31.

The foregoing information is relevant both to the issue of resources necessary for the accomplishment of statutory tasks under the *Privacy Act* and for comparisons with staffing in data protection agencies in other countries. The Federal Republic of Germany operates a federal-state data protection system that is comparable to the Canadian federal advisory system. On January 1, 1987, the Federal Data Protection Commissioner's Office had a total staff of 31 (23 professionals) for a

population of about 61 million. The data protection office for the State of North Rhine-Westphalia, the largest and most important state with a population of 17 million, has a staff of 32 (21 professionals). Hesse, the first state anywhere to have a data protection law, has a staff of 21 (16 professionals) for a population of 5.6 million.[5]

The statutory tasks and staff sizes of the Federal Date Protection Office in West Germany and the Office of the Canadian Privacy Commissioner are almost the same. One major difference in how the two federal systems operate, however, which is hard to evaluate in terms of the need for staff, is that a number of federal constitutional responsibilities in West Germany are in fact carried out by the Länder, and thus subject to the oversight of the state data protection authorities. Another significant difference is the much larger physical expanse of Canada, which places additional burdens on the Office of the Canadian Privacy Commissioner in carrying out its auditing responsibilities for personal information systems held in widely-dispersed locations across the country.

The West German office also has oversight of certain companies that are somewhat equivalent to Canadian Crown corporations and relatively modest oversight of certain spheres somewhat comparable to the federally-regulated private sector in Canada. These are the main areas in which the Committee has recommended significant expansion of the Privacy Commissioner's work, and it seems obvious that these new tasks will require additions to the staff of the Canadian office.

Improving Parliamentary Oversight

Section 75(1) of both the *Access to Information Act* and the *Privacy Act* requires a Committee of Parliament to review the "administration" of the legislation "on a permanent basis". The Standing Committee on Justice and Solicitor General was the designated Committee for this purpose. However, since the *Access to Information Act* and the *Privacy Act* went into effect in July, 1983, the Committee has not held any hearings on their administration.

The Committee recognizes that effective parliamentary oversight is essential to the successful implementation of the legislation. Because the Information Commissioner and the Privacy Commissioner are directly accountable to Parliament, it is most important that Parliament hear from them regularly every year in the form of an Annual Report as well as in the form of annual hearings.

The positive experience of the Federal Data Protection Commissioner in West Germany and his counterpart for the state of Hesse indicates the great value of creating a regular annual link between the legislature and a data protection agency. This is especially important in Canada and West Germany, where the data protection officials only have the power to give advice and cannot order a federal government institution to act in a certain way.

The credibility of the Information Commissioner and the Privacy Commissioner in their relations with government institutions will be considerably enhanced by the Committee's recommendation of a regular annual series of hearings. Any institution tempted to flaunt the advice of the Commissioners will run the risk of incurring the wrath of the parliamentary committee as well. The new Standing Orders governing the operations of such Standing Committees as this one should facilitate more regular contacts with both the Information and Privacy Commissioners.

A useful precedent for such actions is the annual series of hearings held by the Public Accounts Committee on the Annual Report of the Auditor General. The same Committee also hears from specific government institutions with regard to particular issues. Its mandate is based on a permanent Order of Reference, and it has the service of full-time professional staff which carries out research and analysis on its behalf. Another precedent is the role played by the Standing Joint Committee on Regulations and Other Statutory Instruments in ensuring that delegated legislation adopted by government institutions is consistent with a number of broad criteria set out in the *Statutory Instruments Act*.

Recommendations:

9.1 The Committee recommends the revision of the *Access to Information Act* and the *Privacy Act* to require the Standing Committee on Justice and Solicitor General to hold hearings on the Annual Reports of the Information Commissioner and the Privacy Commissioner within 90 sitting days of their being tabled in the House of Commons. This review should occur on the basis of a permanent Order of Reference and should provide for engaging the professional staff necessary to assist the Committee.

9.2 The Committee recommends that the Standing Committee on Justice and Solicitor General, on a cyclical basis or with respect to specific issues, hold hearings to review the Annual Reports from institutions and organizations that are subject to the *Access to Information Act* and the *Privacy Act*.

Improving Annual Reports From Government Institutions

Under section 72 of the *Access to Information Act* and the *Privacy Act*, the head of every government institution subject to the Acts is required to submit an Annual Report on the administration of both statutes to Parliament. Such reports are referred to the Standing Committee on Justice and Solicitor General. To this point in time, such Annual Reports have been received by the Committee, but they have not been reviewed in detail, except in connection with the current three-year review process.

The Committee considered several choices in pursuing its goal of promoting effective implementation of the *Access to Information Act* and the *Privacy Act*. It favours requiring the preparation of Consolidated Annual Reports by the Treasury Board, based on Annual Reports from individual government institutions, which would facilitate Parliament's oversight process. The Treasury Board had such a responsibility under Part IV of the *Canadian Human Rights Act* of 1977, the original version of the current *Privacy Act*; one person prepared such a Consolidated Report. An excellent model is found in Australian practice; the Attorney-General's Department produces a very useful Annual Report of this type concerning the *Freedom of Information Act, 1982*.[6] The Committee rejected the idea of itself overseeing the preparation of Annual Reports from individual government institutions and vetting their contents, since this task is much better suited to the Treasury Board than to a Parliamentary Committee.

An existing precedent for the preparation of Consolidated Annual Reports is the duty imposed on the President of the Treasury Board, by the new Part XII of the *Financial Administration Act*, to prepare an Annual Report on the business and activities of all parent Crown corporations. Such Annual Reports must be tabled in Parliament not later than December 31 of each year and must cover the financial years ending on or before the previous July 31.[7]

Another model for the Committee's recommendation is the Annual Report on the U.S. *Privacy Act* prepared by the U.S. Office of Information and Regulatory Affairs of the Office of Management and Budget (OMB), which is part of the Executive Office of the President. As in Canada, the Annual Report is based on Annual Reports submitted to the Office of Management and Budget by the individual departments. OMB has given specific directives to government institutions about what to emphasize in their Annual Reports.[8] It is also noteworthy that section (p) of the U.S. *Privacy Act* was amended in 1982 to strengthen the reporting requirements under the legislation.[9]

Thus the Committee believes that government institutions should still be required to prepare and submit Annual Reports.[10] In particular, it urges that the following reporting practices adopted by certain government institutions in their Annual Reports should become more widespread and form an integral part of all reporting carried out by government institutions under the *Access to Information Act* and the *Privacy Act*:

— departmental guidelines or manuals for day to day ATIP administration;

— indications of particular problems confronted in administering the Acts;

— workload analysis charts setting out staff and resource allocation;

— text of fee waiver policies;

— multi-year cumulative statistics;

— flow chart indicating to the applicant how the government institution deals with access requests;

— statistics on the subject matter of access requests;

— descriptive examples of requests received;

— indication of the geographical origin of requests by province or region; and

— breakdown of the type of personal information files to which access is requested.

Recommendations:

9.3 The Committee recommends that government institutions continue to prepare Annual Reports on the *Access to Information Act* and *Privacy Act* under section 72 and that these continue to be sent to Parliament, the Information and/or Privacy Commissioner, as appropriate, the Department of Justice, and the Treasury Board.

9.4 The Committee recommends that, on a periodic and rotating basis, and as the need arises, the Standing Committee on Justice and Solicitor General review and hold hearings on specific Annual Reports received from government institutions under section 72 of the *Access to Information Act* and the *Privacy Act*.

9.5 The Committee recommends that section 72 of the *Access to Information Act* and the *Privacy Act* be amended to require the Treasury Board to prepare Consolidated Annual Reports on the administration of the legislation, based on Annual Reports received from government institutions. The Treasury Board should issue specific instructions to such institutions about the contents of such Annual Reports. Such a Consolidated Annual Report should be submitted to Parliament by October 1 of each year.

9.6 The Committee recommends that the Standing Committee on Justice and Solicitor General hold annual hearings and prepare a Report, if necessary, on the Consolidated Annual Reports of the Treasury Board on the administration of the *Access to Information Act* and the *Privacy Act* within ninety days of their receipt by the House of Commons.

Parliamentary Review

Section 75(2) of the *Access to Information Act* and the *Privacy Act* currently requires that the Committee designated or established by Parliament to review the administration of the legislation on a permanent basis should also undertake a comprehensive review of the provisions and operation of these Acts within three years after their coming into force.

The Committee has undertaken such a statutory review in the period 1985-87. It is of the opinion that this review process has identified a number of substantive issues, as indicated in this Report, and also raised the consciousness of government institutions concerning the existence and meaning of the *Access to Information Act* and the *Privacy Act*. In the Committee's view, this salutary experience should be repeated in four years' time, which is likely to be early in the life of the next Parliament.

One of the major reasons for scheduling another review of the provisions and operation of the Access and Privacy legislation in four years' time is the relative youth of the legislation. Not enough experience has yet been acquired in a number of areas in order to determine satisfactorily whether both the structure and provisions of the Acts are truly adequate. For example, a few more years experience with the application of broad exemptions should make it much clearer whether the current system promotes freedom of information or whether the present scope of the exemptions needs to be further curtailed.

The slow pace of implementation of the Access and Privacy legislation has also had an impact on judicial decision making by the Federal Court of Canada. Despite some significant cases, judicial treatment of important issues has only just begun. A review in four years' time will thus have to look very carefully at what the courts have done with this legislation.

It is also evident that the major privacy problems presented by the application of new information technology to the processing of personal data will require continuing attention by Parliament. The recommendation below ensures that Parliamentarians will again find time to consider issues pertaining to the *Access to Information Act* and the *Privacy Act* within a reasonable time frame.

Recommendations

9.7 The Committee recommends that section 75(2) of the *Access to Information Act* and the *Privacy Act* be amended to require the Committee established by Parliament under section 75(1) to undertake a comprehensive review of the provisions and operation of these Acts within four years of the tabling of the present Report in Parliament and, within a year after the review is undertaken, to submit a Report to Parliament thereon, including a statement of any changes the Committee would recommend.

END NOTES

[1] The debate can be followed in *Minutes of Proceedings and Evidence of the Special Joint Committee of the Senate and House of Commons on the Constitution of Canada*, Issue No. 43 (Jan. 22, 1981); 7, 55-6.

[2] *Hunter* v. *Southam* (1984) 2 S.C.R. 145 at p. 159-60; see also *James Richardson and Sons* v. *Minister of National Revenue* (1984) 1 S.C.R. 614.

[3] "All people are by nature free and independent, and have certain inalienable rights, among which are those of enjoying and defending life and liberty; acquiring, possessing, and protecting property; and pursuing and obtaining safety, happiness, and privacy." (Article 1, section 1, *California Constitution*, November 1972).

[4] Privacy Commissioner, *Annual Report 1985-86* (Ottawa, 1986), p. 57.

[5] The data used in this paragraph is derived from information received from the Data Protection Commissioner in North Rhine-Westphalia and the Office of the Federal Data Protection Commissioner in December 1986.

[6] *Annual Report by the Attorney-General on the Operations of the Freedom of Information Act, 1983-84* (Canberra, 1985)

[7] See: President of the Treasury Board, *Annual Report to Parliament on Crown Corporations and Other Corporate Interests of Canada, Public Accounts of Canada, 1986*, III (Ottawa, 1986)

[8] *Oversight of Computer Matching to Detect Fraud and Mismanagement in Government Programs*, Hearings before the Subcommittee on Oversight of Government Management of the Committee on Governmental Affairs, United States Senate, 97th Congress, 2nd Session, 15-16 December 1982 (Washington, DC: Government Printing Office, 1983), p. 615.

[9] 5 U.S.C. 552a (p).

[10] The problem in the U.S. has been the timeliness of the consolidated report, and similar problems may arise at the Treasury Board in Canada. The last published report in the United States was for two calendar years (rather than one), 1982-83, and it became available two years late — at the end of 1985. (*The President's Annual Report on the Agencies' Implementation of the Privacy Act of 1974. CY [Calendar Year] 1982-1983* [Washington, DC, 1985, mimeographed].) It is worth noting that this report was primarily produced by one person, who is otherwise fully engaged in regular administrative duties.

APPENDIX A

RECOMMENDATIONS

THRESHOLD CONCERNS

2.1 The Committee recommends that, for purposes of clarification, the *Access to Information Act* and the *Privacy Act* mandate that the Treasury Board, the Information Commissioner, and the Privacy Commissioner foster public understanding of the *Access to Information Act* and the *Privacy Act* and of the principles described in section 2 of each Act. Such education should be directed towards both the general public and the personnel of government institutions. The appropriate provision in the statutes should follow the model of section 22 of the *Canadian Human Rights Act*. (p. 7)

2.2 The Committee further recommends that the Treasury Board undertake a public education campaign in conjunction with the proclamation of any amendments to the *Access to Information Act* and the *Privacy Act* and also consider printing notices about individual rights under both the *Access to Information Act* and the *Privacy Act* to be included in standard government mailings. (p. 8)

2.3 The Committee recommends that all federal government institutions be covered by the *Access to Information Act* and the *Privacy Act*, unless Parliament chooses to exclude an entity in explicit terms. Thus the Committee recommends the repeal of Schedule I to the *Access to Information Act* and the Schedule to the *Privacy Act*. The criteria for inclusion should be as follows: Firstly, if public institutions are exclusively financed out of the Consolidated Revenue Fund, they should be covered. Secondly, for agencies which are not financed exclusively in this way, but can raise funds through public borrowing, the major determinant should be the degree of government control. (p. 9)

2.4 The Committee recommends that the *Access to Information Act* cover all federal government institutions, including all administrative tribunals, the Senate, the House of Commons (but excluding the offices of Senators and Members of the House of Commons), the Library of Parliament, and such offices directly accountable to Parliament as the Auditor General, the Official Languages Commissioner, the Chief Electoral Officer and the Office of the Information and Privacy Commissioners. The criteria for inclusion should be as follows: Firstly, if public institutions are exclusively financed out of the Consolidated Revenue Fund, they should be covered. Secondly, for agencies which are not financed exclusively in this way, but can raise funds through public borrowing, the major determinant should be the degree of government control. (p. 9)

2.5 The Committee recommends that the *Privacy Act* cover all federal government institutions, the Supreme Court of Canada, the Federal Court of Canada, the Tax Court of Canada, all administrative tribunals, the Senate, the House of Commons (including the employees only of Senators and Members of the House of Commons), the Library of Parliament, and such offices directly accountable to Parliament as the Office of the Information and Privacy Commmissioners. The criteria for inclusion should be as follows: Firstly, if institutions are exclusively financed out of the Consolidated Revenue Fund, they should be covered. Secondly, for agencies which are not financed exclusively in this way, but can raise funds through public borrowing, the major determinant should be the degree of government control. (p. 9)

2.6 The Committee recommends that the *Access to Information Act* and the *Privacy Act* be extended to cover those Crown corporations and wholly-owned subsidiaries as are listed in the Treasury Board's *Annual Report to Parliament on Crown Corporations and Other Corporate Interests of Canada*. For this purpose, the Committee recommends that the *Access to Information Act* and the *Privacy Act* be amended to include such a definition of "Crown corporation". (p. 11)

2.7 The Committee further recommends that if the Government of Canada controls a public institution by means of a power of appointment over the majority of the members of the agency's governing body or committee, then both the *Access to Information Act* and the *Privacy Act* should apply to such an institution. (p. 11)

2.8 The Committee recommends that, with respect to the Canadian Broadcasting Corporation (CBC), the *Access to Information Act* not apply in relation to program material; otherwise, the Corporation should be fully subject to both the *Access to Information Act* and the *Privacy Act*. (p. 11)

2.9 The Committee recommends that any natural or legal person be eligible to apply for access to records under the *Access to Information Act*. The location of the applicant should no longer be relevant. Corporations, non-profit associations, employee associations, and labour unions should also be able to avail themselves of this legislation. (p. 12)

2.10 The Committee further recommends that section 12(1) of the *Privacy Act* be amended so that access and correction rights for their own personal information are available to all individuals, regardless of citizenship or residence. (p. 12)

2.11 The Committee recommends that the *Access Register* be combined with such other government publications as the *Index of Programs and Services* and the *Organization of the Government of Canada*. (p. 13)

2.12 The Committee further recommends that this omnibus access tool and the *Personal Information Index* be made available by the Treasury Board and individual government institutions on an on-line basis and/or through their sale in digital form for use on computers. (p. 13)

2.13 The Committee further recommends that the Treasury Board and individual government institutions make available segments of these various user guides on a customized basis to suit the needs of particular user groups. (p. 13)

2.14 The Committee recommends that the status and role of Access and Privacy Coordinators be given explicit recognition in section 73 of the *Access to Information Act* and section 73 of the *Privacy Act*, since they are the prime movers for implementation of the legislation within government institutions. (p. 15)

2.15 The Committee recommends, in light of the Treasury Board's 1986 consultation with Access and Privacy Coordinators, that the Treasury Board directly address the problem of ensuring that Coordinators, who should be senior level officials wherever possible, have direct reporting and working relationships with senior management and senior program officials of government institutions in order to ensure necessary support for, and understanding of, their complicated, demanding, and expanding tasks in information management. The Treasury Board should also update its requirement statement concerning the role of Coordinators, especially in such areas as information collection policy, information inventories, privacy protection, and security issues. (p. 15)

2.16 The Committee recommends that the Treasury Board organize standard, formal training for Access and Privacy Coordinators, perhaps using automated training modules, audiovisuals, and films. (p. 15)

2.17 The Committee further recommends that the Treasury Board and the Department of Justice become more active in central coordination and policy leadership on issues with government-wide implications for Access and Privacy legislation. (p. 15)

EXEMPTIONS AND CABINET CONFIDENCES: SAYING NO

3.1 The Committee recommends that subject to the following specific proposals, each exemption contained in the *Access to Information Act* and *Privacy Act* be redrafted so as to contain an injury test and to be discretionary in nature. Only the exemption in respect of Cabinet records (which is proposed later in this Report) should be relieved of the statutory onus of demonstrating that significant injury to a stated interest would result from disclosure. Otherwise, the government institution may withhold records or personal information only "if disclosure could reasonably by expected to be significantly injurious" to a stated interest. (p. 20)

3.2 The Committee recommends that the exemption contained in section 13 of the *Access to Information Act* and section 19 of the *Privacy Act* be redrafted to be discretionary in nature and to contain an injury test. In addition, the exemption should permit other governments to be notified of an application for the disclosure of records or personal information that they have submitted in confidence and also permit them to dispute recommendations for the release of such information before the Information Commissioner or Privacy Commissioner and the Federal Court. The burden of proof in such cases should be placed upon the other governments. Where foreign governments are concerned, a time period of three months should be allowed for response and the Secretary of State for External Affairs should be served with the notice of application. (p. 21)

3.3 The Committee further recommends that section 13 of the *Access to Information Act* and section 19 of the *Privacy Act* be redrafted to clarify that institutions or governments of component elements of foreign states (such as State governments in the United States and their agencies) are included for purposes of this exemption. (p. 22)

3.4 The Committee further recommends that section 13 of the *Access to Information Act* and section 19 of the *Privacy Act* be amended so that institutions of native self-government are accorded the same protection as other governments for purposes of this exemption. (p. 22)

3.5 The Committee recommends that the Privacy Commissioner be requested to continue monitoring the exchange of personal information between the provinces and the federal government in order to promote the uniform reciprocal application of fair information practices. (p. 22)

3.6 The Committee recommends that the term "affairs" in section 14 of the *Access to Information Act* and section 20 of the *Privacy Act* be deleted and be replaced by the term "negotiations". (p. 22)

3.7 The Committee recommends that the Acts be amended to clarify that the classes of information listed in section 15 of the *Access to Information Act* and incorporated by reference in section 21 of the *Privacy Act* are merely illustrations of possible injuries; the overriding issue should remain whether there is an injury to an identified state interest which is analogous to those sorts of state interest listed in the exemption. (p. 23)

3.8 The Committee recommends that minor amendments to the definition of "personal information" be considered in order to address certain technical issues which have arisen in submissions to this Committee and to the Department of Justice. (p. 24)

3.9 The Committee recommends that the substance of sections 3 and 8 of the *Privacy Act* be incorporated in the body of the *Access to Information Act*. (p. 24)

3.10 The Committee recommends that section 19(2) of the *Access to Information Act* be amended to provide as follows: "Notwithstanding subsection (1) the head of a government institution shall disclose...." (p. 24)

3.11 The Committee recommends that the definition of "personal information" under the *Privacy Act* be amended so that the exact salaries of order in council appointments be available pursuant to a request under the *Access to Information Act*, and that only the salary range of other public servants be excluded from this definition. (p. 24)

3.12 The Committee recommends that section 8(5) of the *Privacy Act* be amended to require that individuals generally be notified of the impending disclosure of personal information about them and be entitled to contest this disclosure before the Privacy Commissioner and Federal Court. When considerable numbers of people are affected, the Privacy Commissioner should have the authority to determine whether the disclosure of personal information under section 8(2)(m) constitutes an unwarranted invasion of personal privacy. If the Commissioner so determines, he shall order the government institution to make reasonable attempts to notify the individuals concerned, who should have such time as the Commissioner stipulates to contest the disclosure before the Federal Court. (p. 26)

3.13 The Committee further recommends that the head of the government institution be permitted to appeal the Privacy Commissioner's determination that a particular disclosure of personal information under section 8(2)(m) of the *Privacy Act* constitutes an unwarranted invasion of personal privacy to the Federal Court in the event of a disagreement. (p. 26)

3.14 The Committee recommends that the following definition of "trade secrets" should be contained in the *Access to Information Act*:

> A secret, commercially valuable plan, formula, process or device, that is used for the making, preparing, compounding or processing of trade commodities and that can be said to be the end product of either innovation or substantial effort. (p. 26)

3.15 The Committee recommends that section 18 of the *Access to Information Act* require disclosure of the results of product or environmental testing, along the lines of section 20(2). (p. 27)

3.16 The Committee recommends that the public interest override contained in section 20(6) of the *Access to Information Act* extend to all types of third-party information set out in section 20. (p. 27)

3.17 The Committee recommends that, where many third parties are involved or such parties reside outside of Canada, the *Access to Information Act* be amended to provide for substitutional service of notification by means of notice in the Canada Gazette and advertisement in any relevant trade journal, periodical or newspaper. (p. 28)

3.18 The Committee further recommends that the *Access to Information Act* be amended to clarify that third parties bear the onus of proof before the Federal Court when they challenge decisions to disclose records that may contain confidential business information. (p. 28)

3.19 The Committee recommends that section 21 of the *Access to Information Act* be amended not only to contain an injury test but also to clarify that it applies solely to policy advice and minutes at the political level of decision making, not factual information used in the routine decision-making process of government. The exemption should be available only to records that came into existence less than ten years prior to a request. (p. 29)

3.20 The Committee recommends that section 23 of the *Access to Information Act* and section 27 of the *Privacy Act* be amended to clarify that the solicitor-client exemption is to apply only where litigation or negotiations are underway or are reasonably foreseeable. (p. 29)

3.21 The Committee recommends that section 10(2) of the *Access to Information Act* and section 16(2) of the *Privacy Act* be amended to permit the government institution to refuse to confirm or deny the existence of a record only when disclosure of the record's existence would reveal information otherwise exempt under sections 13, 15, 16 or 17 of the *Access to Information Act* or sections 19, 21, 22 or 25 of the *Privacy Act* (information from other governments, international affairs and national defence, law enforcement and investigations, and safety of individuals). (p. 29)

3.22 The Committee recommends that the exclusion of Cabinet records found in section 69 of the *Access to Information Act* and section 70 of the *Privacy Act* be deleted. In its place, an ordinary exemption for Cabinet records should be added to the *Access to Information Act* and the *Privacy Act*. No injury test should be included in this exemption. (p. 32)

3.23 The Committee recommends that section 69(1)(a) [Cabinet memoranda], section 69(1)(b) [discussion papers] and section 69(1)(e) [Ministerial briefing notes], as well as section 69(3)(b) of the *Access to Information Act* [section 70(1)(a), (b) and (e) and section 70(3)(b) of the *Privacy Act*] be deleted. The amended exemption for Cabinet confidences should be drafted in the following terms:

> (1) The head of a government institution may refuse to disclose a record requested under this Act where the disclosure would reveal the substance of deliberations of the Queen's Privy Council for Canada, contained within the following classes of records:
>
> (a) agenda of Council or records recording deliberations or decisions of Council;
>
> (b) a record used for or reflecting consultation among Ministers of the Crown on matters relating to the making of government decisions or the formulation of government policy;
>
> (c) draft legislation or regulations;
>
> (d) records that contain information about the contents of any records within a class of records referred to in paragraph (a) to (c).
>
> (2) For the purposes of subsection (1) "Council" means the Queen's Privy Council for Canada, committees thereof, Cabinet and committees of Cabinet. (p. 32)

3.24 The Committee recommends that the twenty-year exemption status for Cabinet confidences be reduced to fifteen years. (p. 33)

3.25 The Committee recommends that the *Access to Information Act* and the *Privacy Act* be amended to contain a specific framework for the review of Cabinet records. Appeals of decisions under the Cabinet records exemption should be heard solely by the Associate Chief Justice of the Federal Court, with procedures similar to those contemplated in section 52 of the *Access to Information Act* and section 51 of the *Privacy Act*. (p. 33)

THE COMMISSIONERS AND THE COURT

4.1 The Committee recommends that the central mandate of the Information Commissioner and Privacy Commissioner to make recommendations on disclosure be confirmed, but that the power allowing the Information Commissioner to make binding orders for certain subsidiary issues (relating specifically to delays, fees, fee waivers, and extensions of time) be provided in amendments to the *Access to Information Act*. (p. 38)

4.2 The Committee recommends that the Information Commissioner be statutorily authorized to conduct audits of government institutions, *inter alia*, to assess the degree to which the policy of open government contained in the *Access to Information Act* has been implemented. The resources necessary to undertake this additional responsibility should be provided. (p. 38)

4.3 The Committee recommends that the Office of the Information Commissioner and Privacy Commissioner be separated in order to avoid any real or perceived conflict of interest in the discharge of the Commissioners' two mandates. A separate parliamentary vote for each Office should likewise be required. (p. 38)

4.4 The Committee recommends that sections 49 and 50 of the *Access to Information Act* and sections 48 and 49 of the *Privacy Act* be amended so as to provide a single *de novo* standard of judicial review. (p. 39)

4.5 The Committee further recommends that the Acts clarify the Federal Court's general jurisdiction to substitute its judgment for that of the government institution in interpreting the scope of all exemptions. (p. 39)

PARTICULAR ISSUES UNDER THE PRIVACY ACT

5.1 The Committee recommends that the Treasury Board update the *Interim Policy Guide* and issue it in permanent form as a full-fledged *Policy Guide* in the *Administrative Policy Manual* within twelve months of the tabling of this Report in Parliament. (p. 42)

5.2 The Committee recommends that the Treasury Board prepare a written submission to the Standing Committee on Justice and Solicitor General on the detailed operational activities of Statistics Canada and the Public Archives of Canada in implementation of records management policies under the *Privacy Act*. (p. 42)

5.3 The Committee further recommends that the Treasury Board continue to publish its *Implementation Reports* and that the Department of Justice continue to publish its *Communiqué*, because of their importance in assisting government institutions with the implementation of the *Access to Information Act* and *Privacy Act*. (p. 42)

5.4 The Committee recommends that the Privacy Commissioner undertake continuing audits to ensure compliance with sections 4 to 8 of the *Privacy Act*. To make this responsibility explicit, the Committee recommends that section 37(1) be clarified by adding the italicized words to the existing section: "The Privacy Commissioner may, ... carry out *audits and* investigations in respect of personal information under the control of government institutions to ensure compliance with sections 4 to 8." (p. 42)

5.5 The Committee further recommends that the "may" in section 37(1) of the *Privacy Act* be changed to "shall" in order to emphasize the central place of this auditing and investigative responsibility for successful implementation of the Act (without depriving the Privacy Commissioner of any discretion in his initiation of specific compliance audits and investigations). (p. 42)

5.6 The Committee recommends that the President of the Treasury Board issue guidelines requiring government institutions to follow the requirements listed below and also recommends that a specific section incorporating these requirements, and a definition of computer matching, be added to the *Privacy Act*:

Government institutions should be required:

a) to give sixty days advance public notice (a comment period) of intended matches in the Canada Gazette and to describe all current matching activities and the type of information resulting from the match in the annual *Personal Information Index*;

b) to report in sufficient detail in the announcement of proposed matches to identify clearly the authority under the *Privacy Act* permitting the match; and

c) to register any new bank resulting from data-matching. (p. 44)

5.7 The Committee further recommends that the *Privacy Act* prohibit all but the most carefully circumscribed data matching, especially with respect to those matches involving the use of personal data from another government institution. (p. 44)

5.8 The Committee recommends that the Privacy Commissioner be especially vigilant in his oversight of computer matching and make a particular point of drawing perceived abuses to the attention of Parliament, both in his Annual Report and in his appearances before the Standing Committee on Justice and Solicitor General. (p. 44)

5.9 The Committee recommends that a new section of the *Privacy Act* limit the collection and use of Social Insurance Numbers to those activities explicitly authorized by federal Act or regulations. Otherwise, there should be a statutory prohibition against the federal government, the provinces, or the private sector denying services or goods to an individual, because of a refusal to provide a Social Insurance Number. The Committee also urges the creation of a statutory cause of action under the *Privacy Act* for individuals faced with such refusals. (p. 46)

5.10 The Committee recommends that the *Privacy Act* be amended as follows:

It shall be unlawful for any federal, provincial or local government institution or the private sector to ask any person for his or her Social Insurance Number, unless such a request is authorized by law.

It shall be unlawful for any federal, provincial or local government institution or the private sector to deny to any individual any right, benefit, or privilege provided by law, because of such individual's refusal to disclose his or her Social Insurance Number, unless such disclosure is required by federal statute.

Any federal government institution which requests an individual to disclose his or her Social Insurance Number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it. (p. 46)

5.11 The Committee recommends that the concept of exempt banks be removed from the *Privacy Act* by repealing sections 18 and 36, since there is no compelling need to retain such a concept in light of the other strong exemptions on disclosure that exist in the legislation. (p. 49)

5.12 The Committee recommends that the *Privacy Act* be amended to provide criminal penalties for willful breaches of the statute. Such an offence should prohibit any person from willfully disclosing personal information in contravention of the Act, wilfully maintaining a personal information bank in contravention of the Act, or making a request for access to or correction of personal information under false pretenses. (p. 50)

5.13 The Committee recommends that the *Privacy Act* be amended to provide data subjects with monetary damages for identifiable harm resulting from breaches of the following statutory duties:

1. The duty to collect only authorized or relevant data;
2. The duty to refrain from disclosure or transfer of data;
3. The duty to give access to files and to make corrections. (p. 51)

5.14 The Committee recommends that rules of court permit individuals the right to bring suit under the *Privacy Act* in as simplified a manner as possible. Furthermore, the Federal Court of Canada should, in the ordinary course, award costs on a solicitor and client basis to the successful applicant. (p. 51)

5.15 The Committee recommends that the Government, government institutions, and Parliament take the requirements of the *Privacy Act* into account, and notify the Privacy Commissioner, concerning any draft or final legislation, regulations, or policies that have implications for the personal privacy of Canadians. (p. 53)

5.16 The Committee recommends that all legislation before Parliament which has implications for the collection, retention, protection, and disposal of personal information be accompanied by a privacy-impact statement prepared by the sponsoring government institution for review and comment by the Office of the Privacy Commissioner. (p. 53)

5.17 The Committee recommends that the *Privacy Act* be amended to specify that all personal data stored in the Canadian Police Information Centre is fully subject to the requirements of the *Privacy Act*. (p. 54)

5.18 The Committee further recommends that the Privacy Commissioner evaluate and audit the policies and practices of the CPIC system, and other comparable automated data bases, in order to ensure that the privacy interests of individual Canadians are being adequately protected. (p. 55)

5.19 The Committee recommends that all government institutions presently subject to the *Privacy Act* permit their employees to have informal access to their own personnel records, instead of requiring a formal request for access under the *Privacy Act*. (p. 55)

5.20 The Committee recommends that, in accordance with its earlier recommendations, all government institutions to be covered by the *Privacy Act*, as well as Crown corporations and the federally-regulated private sector, permit employees to have informal access to their own personnel records instead of requiring a formal request for access under the *Privacy Act*. (p. 55)

5.21 The Committee recommends that the following definition of "consistent use" be added to the *Privacy Act*:

> The term "consistent use" means, with respect to the disclosure of a record or personal information, any use of such record or personal information relevant to the purpose for which it was collected, and which use is necessary to the statutory duties of the agency that collected or obtained the record or personal information, or necessary for that agency to operate a program specifically authorized by law. For a use or disclosure to be consistent it must have a reasonable and direct connection to the original purpose(s) for which the information was obtained or compiled. (p. 57)

5.22 The Committee further recommends that the Treasury Board forcefully remind government institutions of their obligation, under section 9(3) of the *Privacy Act*, to publish information about consistent uses in the *Personal Information Index* and to notify the Privacy Commissioner when such disclosures occur without such advance notification. (p. 57)

5.23 The Committee recommends that the definition of personal information in section 3 of the *Privacy Act* be amended as follows:

1. The date of death provisions in section 3(m) of the *Privacy Act* be changed to 10 years (from 20 years), or 100 years since birthdate.

2. The head of the government institution be permitted to disclose personal information for reasons of public safety and health. (p. 58)

5.24 The Committee recommends that the following definition of privacy be added to section 3 of the *Privacy Act*:

Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is to be communicated to others. (p. 58)

5.25 The Committee recommends that the following provision be added to the *Privacy Act* to require all government institutions covered by the Act to maintain appropriate security standards for personal information:

Government institutions are required to establish appropriate administrative, technical, and physical safeguards to ensure 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 about whom information is maintained. (p. 59)

PARTICULAR ISSUES UNDER THE ACCESS TO INFORMATION ACT

6.1 The Committee recommends revising the relevant regulations so that no mandatory form be required to make a request under the *Access to Information Act*. (p. 63)

6.2 The Committee recommends that for statistical and administrative purposes, a written request for records which refers to the *Access to Information Act* be deemed to constitute a request under the Act. (p. 63)

6.3 The Committee recommends that the *Access to Information Act* be amended to rescind the requirement of an application fee. However, the *Access to Information Act* should be amended to authorize the Information Commissioner to make a binding order enabling a government institution to disregard frivolous or vexatious requests under the Act. Such an order should be appealable to the Federal Court. (p. 64)

6.4 The Committee recommends that there continue to be no fee levied for the first five hours of search and preparation time. (p. 64)

6.5 The Committee recommends that no fees be payable if a search does not reveal any records. (p. 65)

6.6 The Committee recommends that once a document has been released to a particular applicant, subsequent applicants should be able to review this record in the reading room of the government institution. A list of records released under the *Access to Information Act* should be available in the reading room and in the Annual Report of the government institution. Should a copy be desired by subsequent applicants, they should be required at most to pay reasonable photocopying expenses without any additional expense for search and preparation. (p. 65)

6.7 The Committee recommends that the Access to Information Regulations be amended to stipulate a market rate for photocopying. The rates for photocopying should generally be consistent with the rate charged by the Public Archives of Canada, so long as this rate generally reflects prevailing market conditions in the National Capital Region. (p. 65)

6.8 The Committee recommends that a fee waiver policy be enacted by an amendment to the *Access to Information Act* or by regulation so that a consistent standard is applied across the Government of Canada. The following criteria should be considered:

1. Whether there will be a benefit to a population group of some size, which is distinct from the benefit to the applicant;

2. Whether there can be an objectively reasonable judgment by the applicant as to the academic or public policy value of the particular subject of the research in question;

3. Whether the information released meaningfully contributes to public development or understanding of the subject at issue;

4. Whether the information has already been made public, either in a reading room or by means of publication;

5. Whether the applicant can make some showing that the research effort is likely to be disseminated to the public and that the applicant has the qualifications and ability to disseminate the information. A mere representation that someone is a researcher or "plans to write a book" should be insufficient to meet this latter criterion. (p. 66)

6.9 The Committee further recommends that complaints to the Information Commissioner on fee waivers continue to be available, and that the Commissioner be empowered to make binding determinations in this regard, without further recourse to judicial review. (p. 66)

6.10 The Committee recommends that the *Access to Information Act* be amended to specify that the period for processing an application commences on receipt of the application. (p. 67)

6.11 The Committee recommends that where the government institution fails to provide access within the time limits set out in the Act, the applicant should thereupon be notified of his or her right to complain to the Information Commissioner. (p. 67)

6.12 The Committee recommends that the initial response period available to government institutions be reduced from thirty days to twenty days, with a maximum extension period of forty days, unless the Information Commissioner grants a certificate as to the reasonableness of a further extension. The onus for justifying such extensions shall be on the government institution. The Treasury Board is urged to monitor the cost implications of this recommendation and to report to the Standing Committee on Justice and Solicitor General on its findings within one year of the implementation of this measure. (p. 67)

6.13 The Committee recommends that the *Access to Information Act* be amended to authorize the Information Commissioner to make an order waiving all access fees if a government institution fails to meet specified time limits without adequate justification. (p. 67)

6.14 The Committee recommends that the Treausry Board, in conjunction with the Public Service Commission, undertake a study to investigate methods for enhancing timely compliance with the *Access to Information Act*. This investigation should commence as soon as possible and a report to the Standing Committee on Justice and Solicitor General be submitted within one year. (p. 67)

6.15 The Committee recommends that both Acts be amended to impose a time limitation of sixty days on investigations by the Information Commissioner and the Privacy Commissioner. If a

report of the investigation is not forthcoming within this period, a certificate shall be given to the applicant permitting a direct resort to judicial review. The certificate should contain no recommendations but simply a statement that the investigation could not be completed within the allotted sixty-day period. The applicant would then have the choice either to wait until the investigation has been completed or to seek immediate review in the courts. (p. 68)

6.16 The Committee recommends that the *Access to Information Act* be amended to add a provision requiring a government institution to reveal information as soon as practicable where there are reasonable and probable grounds to believe that it is in the public interest to do so and that the record reveals a grave environmental, health or safety hazard. (p. 69)

EMERGING PRIVACY ISSUES

7.1 The Committee recommends that the definition of "personal information" in section 3 of the *Privacy Act* be broadened to include all types of electronic surveillance that involve the collection of personal data in any form. To this end, videotapes, urine specimens, photographs, and tape recordings about an identifiable individual should be added explicitly to the list of "personal information" under section 3. (p. 72)

7.2 The Committee recommends that the Privacy Commissioner be explicitly empowered in the *Privacy Act* to monitor relevant developments in surveillance practices and to investigate complaints about these aspects of electronic monitoring and surveillance in the federal government, Crown corporations, and in the federally-regulated workplace. (p. 72)

7.3 The Committee recommends that those aspects of the use of the polygraph and of urinalysis that involve the collection and use of personal data be fully subject to the *Privacy Act* and to the supervisory oversight of the Privacy Commissioner. His jurisdiction should extend to federal government institutions, crown corporations, and the federally-regulated private sector. (p. 73)

7.4 The Committee recommends that the federal Government's 1984 commitment to foster voluntary privacy codes in the private sector in compliance with the OECD Guidelines be discharged with conviction and vigour. The burden of action falls on the Department of External Affairs and the Department of Justice. They should prepare a Report to Parliament within eighteen months of the tabling of the Committee's Report in the House of Commons on the commitments received from the private sector. (p. 74)

7.5 The Committee recommends that the rights to data protection provided in sections 4 to 9 (the code of fair information practices), 12 to 17 (individual rights of access to data), and 29 to 35 (a mechanism for the Privacy Commissioner to receive and investigate complaints) of the *Privacy Act* be extended to the federally-regulated private sector by means of a separate part of the Act. (p. 77)

7.6 The Committee further recommends that the Privacy Commissioner be empowered to review and approve implementation schemes developed by organizations in the federally-regulated private sector to comply with the *Privacy Act*. He should also be authorized to report to Parliament on the degree of progress in developing satisfactory data protection plans in the same sector. (p. 77)

7.7 The Committee recommends that the *Privacy Act* be amended to provide the Privacy Commissioner with the jurisdiction to oversee the impact of information technology on personal privacy in the public sector, Crown corporations, and the federally-regulated private sector. The Committee urges that such oversight occur in consultation with the appropriate government institutions, such as the Department of Justice, the Treasury Board, Supply and Services Canada,

the Department of Communications, the Canadian Radio-Television and Telecommunications Commission, and the Science Council of Canada. (p. 78)

7.8 The Committee further recommends that section 60 of the *Privacy Act* be amended to authorize the Privacy Commissioner to undertake related research studies on his own initiative. (p. 78)

7.9 The Committee further recommends the amendment of section 60 of the *Privacy Act* to permit the House of Commons to have the power to request or refer research studies to the Office of the Privacy Commissioner. It is understood that references of this type would require the allocation of appropriate resources in order to prevent the diversion of existing resources from other implementation activities undertaken by the Privacy Commissioner. (p. 78)

7.10 The Committee recommends that the Department of Justice, the Treasury Board, government institutions, and the Privacy Commissioner develop new policies and practices to cope with the emerging data protection problem posed by personal information held and used in microcomputers. (p. 79)

7.11 The Committee recommends that the Department of Justice, the Treasury Board, and the Privacy Commissioner make separate reports to Parliament on appropriate responses to this emerging problem within eighteen months of the tabling of the Committee's Report in Parliament. (p. 79)

7.12 The Committee recommends that the Government conduct a review and study of the implications of transborder data flows by the public and private sectors for the personal privacy of residents of this country. Such a study should be tabled in Parliament within one year of the tabling of the Committee's Report. (p. 81)

OTHER ACCESS ISSUES

8.1 The Committee recommends that section 36.3 of the *Canada Evidence Act* [Cabinet confidences] be deleted and that section 36.2 of this Act be amended to add a reference to disclosure on the grounds that the disclosure would reveal Cabinet confidences. For the purpose of this provision the definition of "confidence of the Queen's Privy Council for Canada" should be amended to conform with the amended definition of this provision as recommended in Chapter 3 of this Report. (p. 88)

CONCLUSIONS

9.1 The Committee recommends the revision of the *Access to Information Act* and the *Privacy Act* to require the Standing Committee on Justice and Solicitor General to hold hearings on the Annual Reports of the Information Commissioner and the Privacy Commissioner within 90 sitting days of their being tabled in the House of Commons. This review should occur on the basis of a permanent Order of Reference and should provide for engaging the professional staff necessary to assist the Committee. (p. 94)

9.2 The Committee recommends that the Standing Committee on Justice and Solicitor General, on a cyclical basis or with respect to specific issues, hold hearings to review the Annual Reports from institutions and organizations that are subject to the *Access to Information Act* and the *Privacy Act*. (p. 94)

9.3 The Committee recommends that government institutions continue to prepare Annual Reports on the *Access to Information Act* and *Privacy Act* under section 72 and that these continue to be sent to Parliament, the Information and/or Privacy Commissioner, as appropriate, the Department of Justice, and the Treasury Board. (p. 95)

9.4 The Committee recommends that, on a periodic and rotating basis, and as the need arises, the Standing Committee on Justice and Solicitor General review and hold hearings on specific Annual Reports received from government institutions under section 72 of the *Access to Information Act* and the *Privacy Act*. (p. 95)

9.5 The Committee recommends that section 72 of the *Access to Information Act* and the *Privacy Act* be amended to require the Treasury Board to prepare Consolidated Annual Reports on the administration of the legislation, based on Annual Reports received from government institutions. The Treasury Board should issue specific instructions to such institutions about the contents of such Annual Reports. Such a Consolidated Annual Report should be submitted to Parliament by October 1 of each year. (p. 95)

9.6 The Committee recommends that the Standing Committee on Justice and Solicitor General hold annual hearings and prepare a Report, if necessary, on the Consolidated Annual Reports of the Treasury Board on the administration of the *Access to Information Act* and the *Privacy Act* within ninety days of their receipt by the House of Commons. (p. 95)

9.7 The Committee recommends that section 75(2) of the *Access to Information Act* and the *Privacy Act* be amended to require the Committee established by Parliament under section 75(1) to undertake a comprehensive review of the provisions and operation of these Acts within four years of the tabling of the present Report in Parliament and, within a year after the review is undertaken, to submit a Report to Parliament thereon, including a statement of any changes the Committee would recommend. (p. 96)

APPENDIX B

COMMITTEE'S REPORT ON S.24 (JUNE 19,1986)

The Standing Committee on Justice and Solicitor General has the honour to present its

FIRST REPORT

In relation to its Order of Reference dated Monday, November 19, 1984 concerning the review of the *Access to Information and Privacy Acts*, and pursuant to section 24(2) of the *Access to Information Act*, your Committee has agreed to submit the following report.

Introduction

By an Order of Reference dated November 19, 1984, this Committee was assigned the responsibility of reviewing the *Access to Information Act and the Privacy Act*, being respectively S.C. 1980-81-82-83, c. 111, Schedules I and II. Such a comprehensive review is explicitly contemplated in s. 75(1) of each Act. In the case of the *Access to Information Act* [hereafter "the *Access Act*"], however, the Committee is also assigned a further and distinct responsibility. One of the exemptions in the *Access Act*, s. 24(1), requires the head of a government institution to refuse to disclose any record which is sought under the Act if it "contains information the disclosure of which is restricted by or pursuant to any provision set out in Schedule II". Under s. 24(2) of the *Access Act*, the Committee is required to review every provision set out in Schedule II to the Act and to report to Parliament "on whether and to what extent the provisions are necessary".

This second, more specific responsibility of the Committee is to be discharged "within three years after the coming into force of the Act or, if Parliament is not then sitting, on any of the first fifteen days next thereafter that Parliament is sitting". The *Access Act* came into force on July 1, 1983. Accordingly, the Committee is mandated by the statute to make its report on the issue of the statutory prohibitions contained in Schedule II by July 1, 1986, or, if Parliament is not then sitting, within fifteen days of its next sitting. Its more extensive report relating to the *Access Act* and the *Privacy Act* need only be laid before Parliament within a year of the commencement of its review.

This reporting sequence is somewhat unfortunate. In practical terms, it means that the Committee must indicate its views on a rather specific matter before it sets out its recommendations on the much broader "comprehensive review" of the legislation stipulated in section 75 of each Act.

Placing Section 24 in Context

Most so-called freedom of information Acts incorporate certain other exceptions to the rule of disclosure which are found outside the four corners of the access legislation. By way of example, the first statute of its kind in Canada, the *Nova Scotia Freedom of Information Act*, prohibits access to information which "would be likely to disclose information, the confidentiality of which is protected by an [other] enactment". New Brunswick's *Right to Information Act* also provides that there be no right to information under the Act "where its release would disclose information, the confidentiality of which is protected by [another] law". *Newfoundland's Freedom of Information Act* is quite similar.

The reasons for an umbrella exemption which incorporates other statutory exclusions are readily apparent. Rather than having to determine how each and every confidentiality provision found in myriad other statutes squares with the exemptions set out in the freedom of information legislation, the legislature needs merely to note the existence of these other secrecy provisions in the freedom of information law and a government official may later refer to them in justifying a decision to withhold records.

The obvious drawback to this approach is that the person applying for records under a disclosure statute is uncertain as to the scope of the rights that he or she enjoys. What are those other confidentiality provisions to which the disclosure law is subject? If they are mandatory exemptions, then the only major concern is to locate them in the statute books. But if the other statutory provisions confer a measure of discretion upon the official to determine whether or not to release the records sought, the exact scope of one's right to governmental records is extremely unclear. This uncertainty is compounded when the freedom of information statute provides that the government official "shall" refuse disclosure yet the confidentiality provision found in the other statute states that the official "may", in certain instances, release the record requested.

Legislative History

On October 24, 1979 the Progressive Conservative government introduced Bill C-15, the proposed *Freedom of Information Act*. The Bill contained a mandatory exemption which provided that records be withheld if they contained information "required under any other Act of Parliament to be withheld from the general public or from any person not legally entitled thereto"[s.25] However, this potentially vast exemption was explicitly made subject to certain conditions: if the other Act of Parliament provided the duty to withhold information in such a manner as to (1) leave no discretion or (2) set out particular criteria for refusing disclosure or (3) referred to particular types of information to be withheld, then the exemption in the Freedom of Information Bill applied. If one of these conditions was not satisfied, then the record could not be refused under this particular exemption. Perhaps it would have been possible nevertheless to withhold the record under another exemption. For example, if the confidentiality provision set out in some other Act dealt with a third party's business records found in federal government files but the provision could not be said to be of the type contemplated in the exemption in the Bill, the business records might still be withheld under the exemption dealing with confidential business information.

The approach taken in Bill C-15 was virtually identical to one that had been taken when the *United States Freedom of Information Act* was amended in 1976. When Bill C-43 was introduced by the Liberal government in 1980, it in turn copied the pertinent section of Bill C-15 verbatim. In addition, it added a provision equivalent to the present section 24(2), thereby mandating a Parliamentary review of all the confidentiality provisions contained in other Acts of Parliament. On November 4, 1981, the Hon. Francis Fox, then the Minister responsible for this legislation, tabled certain amendments to the Bill in the Justice and Legal Affairs Committee of the House of Commons. One of these proposals resulted in Schedule II appearing in the Bill for the first time.

This new approach was said to define more clearly the scope of the exemption at issue. It was stated in testimony that the revised exemption was to take precedence over any other sections of the *Access Act*; since existing legislation precluded the disclosure of certain information, the new *Access Act* was not designed to permit the same information to be disclosed if it could not be made to satisfy another exemption in the new Act.

The Minister noted, however, that it was the task of the future Parliamentary Committee to review each of the provisions enumerated in Schedule II and recommend "whether or not they ought to stay in the law". It was anticipated that some of these other provisions might be found no longer to merit the type of protection they had been afforded by previous Parliaments.

The Scope of Section 24.

The *Access Act* recognizes some of the difficulties in drafting a suitable exemption in this connection. In place of a broad reference to other statutory restrictions on disclosure, section 24(1) is explicitly limited to those specific provisions listed in Schedule II to the Act. Unlike other freedom of information statutes which appeal to categories of statutes to be covered by such an exemption, the scope of section 24(1) is exhaustively defined.

When the Act was passed initially, there were 33 other Acts listed in Schedule II, embracing some 40 identified sections and subsections in other federal statutes. Subsequently, due to consequential amendments to some of the enumerated statutes, the repeal or replacement of others, and the addition of new Acts to the Schedule, the list has been altered. At the time of writing, there are 38 statutes listed in the Schedule to the *Access Act*, incorporating in turn 47 specific confidentiality provisions. For a current list of these provisions and their text, see Appendix to this report.

There is a considerable variety of records exempted from disclosure by means of Schedule II. If the record sought in an Access Act request is one that "contains information the disclosure of which is restricted by or pursuant to" one of the 47 other provisions, then it must be withheld. Section 24(1) is a so-called mandatory, class exemption: once it is determined that a record contains information of a kind contemplated in one of these 47 other provisions, the government institution has no choice but to refuse its release. However, very few of these other provisions by their own terms absolutely bar disclosure; they usually only "restrict" disclosure in some manner. Indeed, most vest some measure of discretion in a government official to determine whether to release information—usually to other government officials or to the person who provided the information.

This varying degree of discretion fits awkwardly within a mandatory class exemption. In a very helpful brief submitted to the Committee by the Office of the Information Commissioner, the various provisions set out in Schedule II are placed along a spectrum. [See Part 7 of the Information Commissioner's Brief, May 1986]. The degree of discretion to disclose restricted information contained in each provision is examined and delineated in six categories of discretion, ranging from absolute prohibition to a generally unrestricted discretion to allow disclosure. This analysis would indicate that most provisions either allow disclosure to other government institutions or else allow a Minister or a senior official to disclose information outside the federal government in certain circumstances. For an example, see the *Investment Canada Act*, S.C. 1985, c.20, s. 36(3).

One may quarrel with the specific categories of discretion that have been articulated. One may also disagree with the exact placement of a specific provision within a particular category. Nonetheless, the Committee is in broad agreement with the approach that has been taken in this regard.

Recommendations

What flows from these observations? The Committee approaches its mandate in the spirit of the *Access Act*, which is articulated not in a mere preamble but rather in a distinct section of the statute:

> 2(1) The purpose of this Act is to extend the present laws of Canada to provide a right of access to information in records under the control of a government institution in accordance with the principles that government information should be available to the public, that necessary exceptions to the right of access should be limited and specific and that decisions on disclosure of government information should be reviewed independently of government.

Two of the three principles set out in this clause are violated to some degree by the existence of section 24(1). First, this exeception to the rule of open government cannot be termed "limited and specific". To the extent that these other statutory provisions contain broad discretion to disclose records, these

exceptions to the rule of openness will remain unclear until the discretion is actually exercised in each case. In the words of a leading American court decision interpreting the analogous provision in the *United States Freedom of Information Act*, the thrust of the exemption is "to assure that the basic policy decisions on governmental secrecy be made by the legislative branch rather than the executive branch", a thrust consistent with one of the major objectives of the Act which is "to substitute legislative judgment for administrative discretion". [American Jewish Congress v. Kreps 574 F. 2d 624 at 628.(1978)]

The other principle which is violated by section 24(1) is that of independent review. The scope of the Information Commissioner's review of government decisions to withhold records under this exemption is quite narrow. In investigating a refusal to disclose, all the Commissioner can do is to determine whether or not the disclosure is subject to some other statutory restriction. If it is, then even if the disclosure would in all likelihood cause no identifiable harm, the record must nonetheless be withheld. This follows even if the other statute merely restricts, but does not categorically bar, disclosure. The *Access Act* provides no authority for the Information Commissioner even to recommend that the discretionary power contained in the other statute be exercised in favour of disclosure in appropriate circumstances. The rights of an individual applying for information to have a discretionary decision reversed under the terms of these other statutes or by means of judicial review are extremely limited as well.

Both section 2 and section 24(2) contemplate a threshold issue: are the provisions contained in these other statutes "necessary"? As indicated, this Committee has been assigned the task of assessing whether each of the provisions listed in Schedule II needs to remain in the *Access Act*. We have reviewed these provisions carefully. It is beyond our authority to offer suggestions as to the policy merits of a particular section of another Act. For example, we cannot assess whether it is an appropriate policy for information contained in applications for wiretap authorizations to be protected under s. 178.14 of the *Criminal Code* to the extent and in the manner it is so protected. In order to assess the merits of the policy determination reflected in this provision, we would have to delve into general criminal law policy. Similarly, we cannot state authoritatively that it is a "good" policy decision for information regarding formulas, manufacturing processes and trade secrets to be withheld under s. 4(4) of the *Environmental Contaminants Act*.

However, the Committee can and must determine whether the fact of listing these and other statutory exemptions in the *Access Act* is appropriate. We have concluded that, in general, it is not necessary to include Schedule II in the Act. We are of the view that in every instance, the type of information safeguarded in an enumerated provision would be adequately protected by one or more of the exemptions already contained in the *Access Act*. Most of the enumerated provisions in Schedule II protect either confidential business information or personal information. The exemptions in sections 20 and 19 respectively of the *Access Act* provide ample protection for these interests. Less frequently, information pertaining to national security, law enforcement, federal-provincial relations or governmental economic interests is protected by certain Schedule II provisions. Once again, however, there are ample exemptions in the *Access Act* to address these important state interests.

For example, in the case of the Criminal Code provision noted above, law enforcement interests and personal privacy considerations may have dictated that information be strictly protected from unauthorized disclosure. The elaborate exemptions set out in sections 16 and 19 of the Access Act would serve adequately to provide the same degree of protection—without the necessity of retaining the specific provision drawn from the Criminal Code within the *Access Act*.

Similarly, in the case of the *Environmental Contaminants Act* provision noted above, section 20 of the *Access Act* provides sufficient protection—for purposes of the *Access Act*. It must be acknowledged that section 20 allows a residual balancing test for certain kinds of confidential business information, meaning that in theory some of the information described in this other Act could possibly be released should Schedule II be eliminated. However, two qualifications are necessary: 1) under the *Access Act*,

third parties must be notified if there is any possibility that sensitive business information might be released [s.28]; and 2) the *Environmental Contaminants Act* itself does not absolutely bar the disclosure of all relevant third party information. Only if it is specified in writing to have been given in confidence, is the information to be withheld—and even then, it can be disclosed if it "may be necessary for the purposes of the Act".

Despite our view that the interests protected by the Schedule II provisions could adequately be protected by other existing exemptions in the *Access Act*, we are persuaded that there should be three exceptions to the conclusion. The sections of the *Income Tax Act*, the *Statistics Act* and the *Corporations and Labour Unions Returns Act* which are currently listed in the Schedule deal with income tax records and information supplied by individuals, corporations and labour unions for statistical purposes. Even though the exemptions in the *Access Act* afford adequate protection for these kinds of information, the Committee agrees that it is vital for agencies such as Statistics Canada to be able to assure those persons supplying data that absolute confidentiality will be forthcoming. A similar case has been made for income tax information.

Accordingly, the Committee recommends that the *Access Act* be amended to repeal section 24/Schedule II and replace it with new mandatory exemptions which are drafted so as to incorporate explicitly the interests reflected in the three provisions found in these three other Acts of Parliament,that is the *Income Tax Act*, the *Statistics Act* and the *Coporations and Labour Unions Returns Act*.

The Committee has reviewed each of the other statutory provisions. It has concluded that several may no longer be necessary, even within their parent statutes. For instance, S.10(3) of the *Hazardous Products Act* protects the confidentiality of information provided by manufacturers of potentially hazardous products. There is no doubt that this kind of information should be kept confidential. However, there may be no need for the separate confidentiality provision found in this other Act in light of the exemption pertaining to confidential business information set out in the Access Act. Considering the diversity of other statutory restrictions, however, there are some which may justifiably be retained within their parent statutes for the regulatory purposes contemplated therein.

Accordingly, the Committee recommends that the Department of Justice undertake an extensive review of these other statutory restrictions and amend their parent Acts in a manner consistent with the *Access to Information Act*.

Section 4(1) gives primacy to the *Access to Information Act* over other Acts of Parliament. Therefore by removing S.24 of that Act, the result is clear: other conflicting provisions are subject to the code of disclosure elaborated in the *Access Act*.

The Committee is concerned about a "slippery slope" effect should the current approach of listing other statutory provisions in Schedule II be retained. During its deliberations, briefs were received from both public and private sector sources in which various additions to the Schedule were sought. The impact of permitting wholesale additions to the list of other statutory exemptions contained in the *Access Act* is obvious: the spirit of the legislation could readily be defeated. The *Access Act* would not be a comprehensive statement of our rights to the disclosure of government records. Instead, it would be amorphous. One of the benefits to be derived by listing all exemptions in the *Access Act* is that, in effect, the complete Act is brought under one roof. No longer would other legislation need to be consulted in order to determine one's rights in this vital area.

What of the future? What if a future Parliament wants to be absolutely certain that particular kinds of information is placed beyond the reach of the *Access Act*? It is hoped that these instances will be rare. Should they arise, however, Parliamentarians should be required to stipulate that they are deliberately evading the *Access Act*.

The Committee recommends that any legislation that would seek to provide a confidentiality clause which is not to be made subject to the *Access Act* should commence as follows: "Notwithstanding the *Access to Information Act*,...".

In this way, Parliament will be made explicitly aware of the impact of its actions. As a result, it is hoped that future provisions which are inconsistent with the code of disclosure established in the *Access Act* will be minimal.

APPENDIX

Access to Information Act
Schedule II
(section 24)

	Act	Provision
1.	Aeronautics Act	subsections 3.8(1) and 5.5(5)
2.	Anti-Inflation Act	section 14
3.	Atomic Energy Control Act	section 9
4.	Bank Act	section 251
5.	Banks, Quebec Savings, Act	section 59
6.	Canada Nova Scotia Oil and Gas Agreement Act	section 53
7.	Canada Pension Plan	section 107
8.	Canadian Aviation Safety Board Act	subsections 26(2) and 29(6)
9.	Canadian Ownership & Control Determination Act	section 49
10.	Canadian Security Intelligence Service Act	section 18
11.	Corporations and Labour Unions Returns Act	section 15
12.	Criminal Code	sections 178.14 and 178.2
13.	Criminal Records Act	subsection 6(2) and section 9
14.	Customs Act	section 172
15.	Defence Production Act	section 23
16.	Energy Administration Act	section 92
17.	Energy Monitoring Act	section 33
18.	Environmental Contaminants Act	subsection 4(4)
19.	Family Allowances Act, 1973	section 17
20.	Hazardous Products Act	subsection 10(3)

	Act	Provision
21.	Human Rights, Canadian, Act	subsection 37(3)
22.	Income Tax Act	section 241
23.	Industrial Research & Development Incentives Act	section 13
24.	Investment Canada Act	section 36
25.	Labour Code Canada	section 101(2)
26.	Motor Vehicle Fuel Consumption Standards Act	subsection 27(1)
27.	Oil and Gas, Canada, Act	section 50
28.	Old Age Security Act	section 19
29.	Patent Act	section 10, subsection 20(5) and section 74
30.	Petroleum Incentives Program Act	section 17
31.	Railway Act	subsection 254(2) section 331.3 and subsections 335(3) and (5)
32.	Regional Industrial Expansion, Department of, Act	section 6.1
33.	Statistics Act	section 16
34.	Tariff Board Act	subsection 5(10)
35.	Textile and Clothing Board Act	section 23
36.	Trade Marks Act	subsection 49(6)
37.	Transportation of Dangerous Goods Act	subsection 23(5)
38.	Yukon Quartz Mining Act	subsection 95(14)

Your Committee requests that the Government respond to this report in accordance with Standing Order 99(2).

A copy of the relevant Minutes of Proceedings and Evidence (*Issues Nos. 8, 10 to 18, 20, 22 to 29, and 30, which includes this report*) is tabled.

Respectfully submitted,

BLAINE A. THACKER
Chairman

APPENDIX C

WITNESSES

ISSUE NO.	DATE	ORGANIZATIONS AND WITNESSES
8	May 6, 1986	**Treasury Board** The Honourable Robert R. de Cotret, President of the Treasury Board Pierre Gravelle, Associate Secretary Gerald Bethell, Acting Director, Information Management Practices, Administrative Policy Branch Peter Gillis, Group Chief, Information Practices, Administrative Policy Branch
10	May 8, 1986	**Department of Justice** The Honourable John Crosbie, Minister of Justice and Attorney General of Canada Stephen Skelly, Senior Assistant Deputy Minister
11	May 13, 1986	**Office of the Privacy Commissioner** John Grace, Privacy Commissioner Gerard van Berkel, Legal Advisor
12	May 14, 1986	**Office of the Information Commissioner** Inger Hansen, Information Commissioner Bruce Mann, Assistant Information Commissioner Paul B. Tetro, General Counsel Célyne Riopel, Director, Information Complaints
13	May 20, 1986	Ken Rubin **La Ligue des droits et libertés** Pierrôt Péladeau Johanne Galipeau
14	May 21, 1986	Gerald Baldwin Thomas Riley
15	May 22, 1986	**Canadian Daily Newspaper Publishers Association** Tom Crowther, Chairman, President and publisher, Daily Gleamer, Fredericton Jeffrey Sallot, Ottawa Bureau Chief, Globe and Mail

ISSUE NO.	DATE	ORGANIZATIONS AND WITNESSES
		Peter Calamai, National Correspondent, Southam News David Vienneau, Parliamentary Correspondent, Toronto Star
15	May 22, 1986	**Centre for Investigative Journalism** Don McGillivray, President Leslie Sheppard, Chairman of Access to Information Committee Jane Waterston, Executive Director Jim Coughlin, Administrative Assistant
16	May 27, 1986	**Canadian Civil Liberties Association** Alan Borovoy, General Counsel **Groupe de Recherche Informatique et Droit** Professor René Laperrière
17	May 28, 1986	**National Union of Provincial Government Employees** John Fryer, President Michael Dagg
18	May 29, 1986	**Public Interest Advocacy Centre** Andrew Roman, General Counsel Elizabeth May, Associate General Counsel **Consumers Association of Canada** David McKendry, Director of Regulated Industries Program John Tyhurst, Counsel
20	June 3, 1986	**Canadian Bar Association** Peter Grant, Chairman, Task Force on the Access to Information Act/Privacy Act Ron Atkey, Member, Task Force Heather Mitchedll, Member, Task Force Penny Bonner, Member, Task Force
22	June 4, 1986	**Social Science Federation of Canada** Jack Granatstein, Chairman, Task Force on Access to Information John McCamus, Dean, Faculty of Law, Osgoode Hall, York University Don Rowat, Department of Political Science, Carleton University
23	June 5, 1986	**Ottawa/Hull Victims of Justice** David Nairn

ISSUE NO.	DATE	ORGANIZATIONS AND WITNESSES
		Prisoners' Rights Committee Jean-Claude Bernheim, Coordinator Stephen Fineberg, Staff member George Papadatos (Pappas), Resident, Ste-Anne des Plaines Institution
24	June 5, 1986	**Privy Council Office** Glen Shortliffe, Deputy Secretary to the Cabinet (Operations)
25	June 10, 1986	**Canadian Bankers' Association** Robert M. MacIntosh, President Robert R. Parker, Chairman, Task Force on Privacy **Royal Bank of Canada** Jack Burnett, Senior Vice President and General Counsel Robert R. Parker, Chief Advisor, Government Affairs and Public Policy Ken Morrison, Vice President, Planning, Technology and Financial Management
26	June 11, 1986	**Department of External Affairs** Derek Burney, Associate Under-Secretary of State Kenneth Brown, Access to Information and Privacy Coordinator Michael Bittle, Access to Information and Privacy Officer **Department of National Defence** Lieutenant-General, P.D. Manson, Assistant Deputy Minister (Personnel) Major-General C.W. Hewson, Chief Intelligence and Security C.J. Gauthier, Director General, Executive Secretariat, Access Coordinator S.P. Hunter, Director General Personnel, Privacy Coordinator Colonel P. Partner, Director Personnel Legal Services Colonel H. Rose, Director, Flight Safety
27	June 12, 1986	**Department of Employment and Immigration** Diana Monnet, Executive Secretary J.B. Bissett, Executive Director J.F. Walsh, Director, Public Rights Adminstration **Department of National Health and Welfare** David Kirkwood, Deputy Minister Donald G. Ogston, Directdor Genereal, Program Audit and Review Guy Demers, Directdor, Access to Information and Privacy Centre

ISSUE NO.	DATE	ORGANIZATIONS AND WITNESSES
28	June 17, 1986	**Canadian Rights and Liberties Federation** Don Whiteside, President Peter Rock Margot Young
	June 17, 1986	**Canadian Historical Association** Professor René Durocher, University of Montreal, President Professor Christopher Armstrong, York University
29	June 19, 1986	**Department of Solicitor General** The Honourable Perrin Beatty, Solicitor General of Canada Michael Shoemaker, Senior Assistant Deputy Solicitor General
30	June 19, 1986	**Department of Communications** James Edwards M.P., Parliamentary Secretary to the Minister of Communications Michael Binder, Assistant Deputy Minister, Corporate Management John Bélanger, Access to Information and Privacy Coordinator Stephanie Perrin, Coordinator, Access Information and Privacy Secretariat

APPENDIX D

WRITTEN SUBMISSIONS RECEIVED

Access to Information Centre

Air Canada

Auditor General of Canada

Baldwin, Gerald, W., Ottawa, Ontario

Bell Canada

Canada Packers Limited

Canada Post Corporation

Canadian Broadcasting Corporation

Canadian Agricultural Chemicals Association

Canadian Bankers' Association

Canadian Bar Association

Canadian Civil Liberties Association

Canadian Daily Newspaper Publishers Association

Canada Deposit Insurance Corporation

Canadian Historical Association

Canadian Rights and Liberties Federation

Canadian Sociology and Anthropology Association

Centre for Investigative Journalism

Church of Scientology

Comcheq Services

Comité des détenus de Leclerc

Consumers Association of Canada

Conseil de presse du Québec

Dagg, Michael, Ottawa, Ontario

Dearden, Richard, Ottawa, Ontario

Department of Communications

Department of Employment and Immigration

Department of Epidemiology, University of Ottawa

Department of External Affairs

Department of Justice

Department of National Defence

Department of National Health & Welfare

Department of National Revenue

Department of Regional Industrial Expansion

Department of the Solicitor General

Department of Supply and Services

Department of Transport

Department of Veterans Affairs

Fédération professionnelle des journalistes du Québec

Government of Alberta

Government of British Columbia

Government of Labrador and Newfoundland

Government of Manitoba

Government of Nova Scotia

Government of P.E.I.

Government of Saskatchewan

Government of Yukon

Guth, DeLloyd J., Vancouver, B.C.

Hunter, Iain, Ottawa, Ontario

IBM Canada Limited

Information Commissioner

Kempling, Bill, Member of the House of Commons

Labour Adjustment Review Board

Laperrière, René, Montreal, Quebec

Law Reform Commission

Léveillé, Jean-Jacques, Montreal, Quebec

Ligue des droits et libertés

Muthu, S., Regina, Saskatchewan

Nairn, David, Ottawa, Ontario

National Union of Provincial Government Employees

Ontario Press Council

Petro-Canada

Pollard, Arthur, Victoria, B.C.

Prisoners' Rights Committee

Privacy Commissioner

Public Archives of Canada

Public Interest Advocacy Centre

Public Service Alliance of Canada

Public Service Commission

Ray, Dr. A.K., Gloucester, Ontario

Riley, Thomas, Toronto, Ontario

Rosen, Leonard, Montreal, Quebec

Royal Bank of Canada

Rubin, Ken, Ottawa, Ontario

Sewell, Victor, Mission, B.C.

Social Science Federation of Canada

Statistics Canada

Sterling, Theodore, Burnaby, B.C.

Treasury Board Secretariat

Uniroyal Chemicals

MINUTES OF PROCEEDINGS

TUESDAY, January 27, 1987
(14)

The Standing Committee on Justice and Solicitor General met *in camera* in Room 307 West Block at 9:45 o'clock a.m., this day, the Chairman, Blaine A. Thacker presiding.

Members of the Committee present: Robert Horner, Jim Jepson, Alex Kindy, Rob Nicholson, Svend J. Robinson and Blaine A. Thacker.

Acting Members present: Warren Allmand for Robert Kaplan and Joe Reid for Allan Lawrence.

In attendance: *From the Library of Parliament*: Philip Rosen, Research Officer. *Expert Consultants*: Professor David H. Flaherty, University of Western Ontario and Professor Murray Rankin, University of Victoria.

The Committee resumed consideration of its draft Report on the Access to Information and Privacy Acts.

At 12:20 o'clock p.m. the Committee adjourned until 3:30 o'clock p.m. this day.

AFTERNOON SITTING
(15)

The Standing Committee on Justice and Solicitor General met *in camera* in Room 307 West Block at 3:40 o'clock p.m., this day, the Chairman, Blaine A. Thacker presiding.

Members of the Committee present: Robert Horner, Alex Kindy, Rob Nicholson, Svend J. Robinson and Blaine A. Thacker.

Acting Member present: Warren Allmand for Robert Kaplan.

In attendance: *From the Library of Parliament*: Philip Rosen, Research Officer. *Expert Consultants*: Professor David H. Flaherty, University of Western Ontario and Professor Murray Rankin, University of Victoria.

The Committee resumed consideration of its draft Report on the Access to Information and Privacy Acts.

It was agreed, - That the services of Professor Murray Rankin, University of Victoria, B.C. and Professor David H. Flaherty, University of Western Ontario, London, Ontario be retained from December 1, 1986 to March 31, 1987 to complete the work on the Committee's review of the Access to Information and Privacy Acts.

It was agreed, - That the Committee will print 5,000 copies of its First Report to the House in tumble bilingual format with a distinctive cover.

At 4:30 o'clock p.m. the sitting was suspended.

At 5:15 o'clock p.m. the sitting resumed.

At 5:55 o'clock p.m. the Committee adjourned to the call of the Chair.

THURSDAY, February 19, 1987
(17)

The Standing Committee on Justice and Solicitor General met *in camera* in Room 307 West Block at 3:45 o'clock p.m., this day, the Chairman, Blaine A. Thacker presiding.

Members of the Committee present: Svend J. Robinson and Blaine A. Thacker.

Acting Members present: Allan Pietz for Rob Nicholson and Warren Allmand for Robert Kaplan.

In attendance: *From the Library of Parliament*: Philip Rosen, Research Officer.

The Committee resumed consideration of its draft Report on the Access to Information and Privacy Acts.

At 4:20 o'clock p.m. the Committee adjourned to the call of the Chair.

TUESDAY, March 3, 1987
(18)

The Standing Committee on Justice and Solicitor General met *in camera* in Room 308 West Block at 11:15 o'clock a.m., this day, the Chairman, Blaine A. Thacker presiding.

Members of the Committee present: Robert Horner, Jim Jepson, Robert Kaplan, Alex Kindy, Allan Lawrence, Rob Nicholson, John V. Nunziata, Svend J. Robinson and Blaine A. Thacker.

In attendance: *From the Library of Parliament*: Philip Rosen and Don MacDonald, Research Officers.

The Committee resumed consideration of its draft Report on the Access to Information and Privacy Acts.

It was agreed, - That the draft report, as amended, be adopted as the Committee's First Report to the House and that the Chairman be authorized to make such typographical and editorial changes as may be necessary without changing the substance of the draft report and that the Chairman be instructed to present the said report to the House.

It was agreed, - That pursuant to Standing Order 99(2), the Committee request that the Government table a comprehensive response to its First Report.

The Committee proceeded to the consideration of future business.

At 12:10 o'clock p.m., the Committee adjourned to the call of the Chair.

Luke Morton,
Clerk of the Committee.