

Annual Report
Privacy Commissioner
1985-86



**Annual Report
Privacy Commissioner
1985-86**



The Privacy Commissioner of Canada
112 Kent Street, 14th Floor
Ottawa, Ontario
K1A 1H3
(613) 995-2410

1-800-267-0441 The switchboard is open from 7:30 a.m. to 6:00 p.m., Ottawa time.

© Minister of Supply and Services Canada 1986

Cat. No. IP 30-1/1986

ISBN O-662-53847-1

"No personal information shall be collected . . . unless it relates directly to an operating program or activity . . .".

"A government institution shall, wherever possible, collect personal information . . . directly from the individual to whom it relates . . .

". . . shall inform any individual . . . of the purpose for which the information is being collected.

". . . shall take all reasonable steps to ensure that personal information . . . is as accurate, up-to-date and complete as possible.

"Personal information . . . shall not, without the consent of the individual to whom it relates, be used . . . except

(a) for the purpose for which the information was obtained or compiled . . ."

(or in accordance with specific exceptions set out in section 8)

The *Privacy Act*

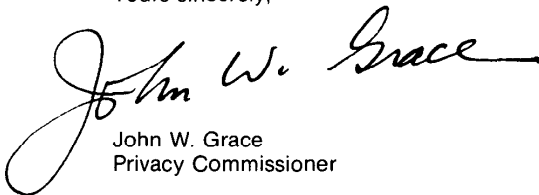
The Honourable Guy Charbonneau
The Speaker
The Senate
Ottawa

June 30, 1986

Dear Mr. Charbonneau:

I have the honour to submit to Parliament my annual report. This report covers the period from April 1, 1985, to March 31, 1986.

Yours sincerely,



John W. Grace
Privacy Commissioner

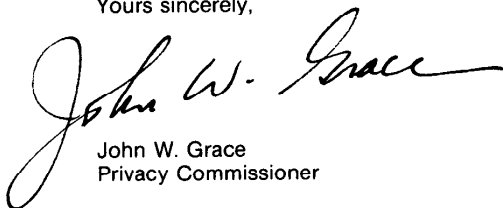
The Honourable J. Bosley
The Speaker
The House of Commons
Ottawa

June 30, 1986

Dear Mr. Bosley:

I have the honour to submit to Parliament my annual report. This report covers the period from April 1, 1985, to March 31, 1986.

Yours sincerely,

A handwritten signature in cursive script that reads "John W. Grace". The signature is written in black ink and is positioned above the printed name and title.

John W. Grace
Privacy Commissioner

Contents

Mandate	1
A Special Time	2
A Little History	4
Yet Criticism was Heard	5
Unforeseen Challenges	6
Privacy Issues.....	7
Impact of micro computers	7
Privacy Act and computer-matching	7
Social insurance numbers	8
Electronic surveillance	9
Extending privacy protection	10
Transborder data flow	12
The private sector and the OECD guidelines	13
Section 19	13
Role of the Privacy Commissioner	16
Consulting the Commissioner	16
The audit function	20
Exempt information banks	21
Opening Up Access	24
The Role of the Coordinator	25
Complaints Branch	26
Access	28
Misuse	34
Delay	38
Correction	39
Collection, Retention and Disposal	40
Language	41
Index	42
On the Commissioner's Initiative	43
Inquiries	44
Notifying the Commissioner	46
Compliance Branch	50
The Privacy Act in Court	54
Corporate Management	57
The Privacy Act and You	59
Appendices	
I Organization Chart	62
II Information Request Form	63
III Government Institutions Covered by the Act	64

Mandate

The *Privacy Act* provides individuals with access to their personal information held by the federal government; it protects individuals' privacy by limiting those who may see the information; and it gives individuals some control over the government's collection and use of the information.

The Act sets out the principles of fair information practices, requiring government to:

- collect only the information needed to operate its programs;
- collect the information directly from the individual concerned, whenever possible; and
- tell the individual how it will be used;
- keep the information long enough to ensure an individual access; and
- "take all reasonable steps" to ensure its accuracy and completeness.

Canadian citizens or permanent residents may complain to the Privacy Commissioner if:

- they are denied any part of the information;
- they are denied their request to correct some of the information on the file — or their right to annotate it;
- the department takes longer than the initial 30 days or maximum 60 days to provide the information;
- the Personal Information Index description of the contents of the information bank is deficient in some way;
- the department's listing in the Index does not describe all the uses it makes of personal information;
- an institution is collecting, keeping or disposing of personal information in a way which contravenes the *Privacy Act*.

Such complaints are investigated by the Privacy Commissioner by having his investigators examine any file (including those in closed banks) except confidences of the Queen's Privy Council to ensure that government institutions are complying with the Act.

The Act also gives the Privacy Commissioner the power to audit the way government institutions are collecting, using and disposing of personal information, without having to wait for a complaint.

A Special Time

"The committee designated or established by Parliament . . . shall, within three years after the coming into force of this Act, undertake a comprehensive review of the provisions and operations of this Act . . ."

The Standing Committee on Justice and Solicitor General this year carries out the assignment which Parliament built into the *Privacy Act*: an examination of how the legislation is working.

This is provided in Section 75(2) which contains the unusual and admirable instruction to undertake, within three years of the Act coming into force, "a comprehensive review" of its "provisions and operation" and to submit to Parliament a report "including a statement of any changes the committee would recommend."

The *Privacy Act* became effective July 1, 1983. Thus 1986, the year of the Parliamentary review, is a special time in the life of the legislation.

The Standing Committee on Justice and Solicitor General asked the Privacy Commissioner to participate in its review. The first stage of this participation was to provide the committee with an evaluation of the strengths and weaknesses of the Act, a response to privacy issues identified as of particular interest to the committee and an account of the operations of the Privacy Commissioner's Office, including case summaries and compliance reports.

The Privacy Commissioner does not have one message for the Parliamentary committee and another for Parliament and the public. Therefore, this annual report appropriates the main body of the Privacy Commissioner's

brief to the committee. In addition, it provides yearly statistics, descriptions of significant complaints and auditing activities — all the kinds of information offered in the previous two annual reports.

But the perspective is broader than usual — perhaps the more useful for that — and the organization of topics is a response to the committee's catalogue of special interests. Since these interests cover the major privacy issues of the day, they are gathered comfortably with this report.

First, a few generalizations about the year in privacy.

The causes for concern and for vigilance in protecting personal information do not recede. Computer networking, the cross-matching of computer-held information, lax security and electronic information exchange challenge the cherished value that individuals should retain a residual control over the personal information that others, including governments (perhaps, especially governments) know about them. Human dignity demands nothing less.

The *Privacy Act* is an important instrument of control over the vast amount of personal information collected, held and disposed of by the federal government. It sets a brave example and it is encouraging to note that one by one the provinces are proceeding with their own privacy legislation.

Yet the technology is relentless. The *Privacy Act's* principles of data protection seem to be flexible enough — simply because they are principles — to combat the new wizardry. But are the prohibitions specific enough to handle each fresh challenge in information technology? Has policy been overtaken by technology which was not known when the *Privacy Act* was passed? Are the custodians of personal information sufficiently supportive of privacy values and alert to the dangers?

These are among the questions which the three-year review must address. But there is no need — or justification — to await the results of any review before defending personal information from abuse, be the information in computers or still in that primitive vestige of an ancient time, a paper file.

The results of a recent American study compel attention in Canada. The Office of Technology Assessment (OTA) found that about 80 per cent of the records covered by the American *Privacy Act* are now maintained in fully or partially computerized systems. No great surprise there. Nor was it much of a revelation to have the study conclude that the impact of the growing use of these systems and of electronic data linkages increases the difficulty and complexity of protecting government institutions.

What is shocking in the OTA's report are these statistics: first, 40 per cent of the agencies examined had not even conducted a risk analysis during the past five years of exponential growth of computer systems; second, 75 per cent of the agencies have no explicit policy to protect the security of information in federal government microcomputers; third, 60 per cent have no, and are not developing, contingency plans for use if mainframe computers are disrupted.

Comparable Canadian statistics need not be produced before federal government managers look to put their own houses in order.

If there is continuing reason for vigilance, there is also reason for some encouragement. Sensitivity to privacy concerns inside of the federal government is increasing, though this is a subjective, not a quantifiable, judgment.

The most significant piece of evidence for optimism is that some — still only a few — federal institutions are conducting their own *Privacy Act* compliance audits.

This means that public service managers have come to believe that meeting their responsibilities for fair information practices under the Act cannot be discharged without systematic auditing. The decision to make privacy audits as routine as financial or management audits will depend upon individual managers, upon the amount and sensitivity of personal information under their control and their audit resources.

But the precedent of internal privacy audits represents an historic breakthrough. The onus now shifts to others to demonstrate how they can be comfortable about compliance without such audits.

A Little History

"I do not believe there are any real fundamental objections to the privacy aspects of the bill."

The words were those of the late Walter Baker, MP for Ottawa-Carleton. He was speaking to Bill C-43 — the legislation combining both the *Access to Information Act* and the *Privacy Act* — when it was brought before the Justice and Legal Affairs Committee in 1981.

It was a significant comment, coming as it did from a senior opposition member of the Committee who, not long before, had appeared as a minister to pilot similar legislation through the same Committee.

Mr. Baker's general approval set the tone for the Committee's examination of the *Privacy Act*.

Privacy legislation was not new, though, as Part IV of the *Canadian Human Rights Act* of 1977, it may have seemed a mere appendage of a much broader act, as if not deserving a status of its own. Yet perhaps it was a prudent way to start, allowing experience and expertise to accumulate before bringing forth what was, by North American standards at least, comprehensive data protection legislation.

Thus the drafters of the privacy portion of Bill C-43 had the advantage of drawing upon the first generation of data protection legislation in Canada.

The Parliamentary passage of Bill C-43 provided the first opportunity to review the privacy legislation which had been broadened and strengthened in important ways. But the access to information part of Bill-C43 received by far the greater attention throughout the Committee hearings. It was more controversial and it broke new ground; privacy laws were not only already in place, but they seemed less threatening.

Yet Criticism was Heard

Of course, concerns about some provisions of the *Privacy Act* were heard. That is why a three-year review was put in place.

The most serious concerns were raised not by members of the Justice and Legal Affairs Committee but by such as the Canadian Association of Chiefs of Police, archivists and civil libertarians.

The Police Chiefs spoke of their "very real fear that one of the ancillary effects of access and privacy legislation would be the erosion and emasculation of law enforcement functions across Canada." The chiefs had been told that, as a result of similar legislation, "sources of information both private and public in the United States . . . have to a great extent dried up."

Speaking for his colleagues, Chief John W. Ackroyd of the Metropolitan Toronto Police Force said:

"Informants refuse to supply crucial investigating information. Government departments refuse to share data, not only with themselves, but with law enforcement agencies."

Others, such as representatives of the Civil Liberties Association, National Capital Region, said that the exemptions in the *Privacy Act* are "not well-defined or restrictive enough," and condemned "a wide opening of the door (to personal information) to a host of authorized third parties that includes debt collectors, something called consistent uses, members of Parliament, and something as loose as the public interest."

Academics appearing before the Committee had no complaints but archivists felt that privacy protection provisions were "too sweeping" and that they threatened "to hinder legitimate historical and social science research in Canada."

Representatives of the Canadian Bar Association argued in favor of basing exemptions on a harms or injury test rather than providing class exclusions.

A member of the Committee wanted the onus to be put on Crown corporations to demonstrate why they should not be covered by the *Privacy Act*.

Did the *Privacy Act* tip the balance too far on one side? Has law enforcement or research been hindered? Have the exemptions sometimes made a mockery of the privacy rights which the law was intended to provide? Should the *Privacy Act* cover more institutions?

These will be among the questions which a review must address.

Yet they are in many ways the easy questions to answer. The main parts of the Act are functioning effectively. Some fine tuning needs to be performed, as some following recommendations suggest. But from the vantage point of the Privacy Commissioner's Office, there appears to be little substance to the fears of three years ago. Most of the weaknesses anticipated and feared have not been realized.

In fact the problems which have arisen with the legislation and are addressed in this report were largely unforeseen.

Unforeseen Challenges

The most important issues facing the new Justice and Solicitor General Committee arise out of the new threats which technology poses to personal privacy. These concerns have been identified already in the catalogue of "general issues" set out by the Committee.

Each of these issues could justify a full-blown study. For example, about two years ago, the United States Congress instructed its Office of Technology Assessment (OTA) to conduct research into the implications of new information technology upon civil liberties, and, even, upon the balance of power among branches and levels of government.

The OTA was not sure about the dimensions of the problem, having estimated that the number of computer systems put into use by the U.S. government could increase from about 18,000 in 1983 to anywhere from 300,000 to one million in 1990. The spread itself reveals how much everyone is travelling into the unknown.

The study is not yet completed.

In Canada, the numbers are much smaller but the growth of computers is also 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 and it was estimated that the 1985-86 expenditure would be some \$25 million.

Large computers (equivalent to or more powerful than an IBM 370/158) totalled 57 in 1983, an increase of 11 over the previous year. Later figures on larger computers were unreported.

The growth speaks for itself. The unanswered question is this: how far behind has technology left privacy or data protection policies?

The following responses to the general issues about which the Committee has expressed its interest are sometimes merely suggestive, certainly not exhaustive. The responses are not based on original or systematic research, but on the knowledge, perceptions and intuitions growing out of the office's professional responsibility and commitment to fair information practices.

Privacy Issues

Impact of microcomputers

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 is that micro or personal computers confer this power upon ever-increasing numbers of individuals. Control over personal data becomes much more difficult to achieve. Anyone with a personal computer 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, able to access centralized record systems.

It is little comfort to be told that personal computers have no access to mainframe data bases. The personal computer's ability to develop its own record systems and share information without leaving an audit trail raises new and far-reaching threats to privacy protection. The supervision of the uses of personal information in large, formally-constituted and publicly catalogued systems is daunting enough. Vastly increased numbers of decentralized (even portable) and undeclared collections of personal information constitute a profound new threat to principles of fair information practice enunciated in the *Privacy Act*.

Privacy Act and computer-matching

Subsection 7(a) of the *Privacy Act* prescribes 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 com-

parison 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 attempt to justify computer-matching as now understood.

Yet, one must be aware of the American experience. Subsection 3(b) of the U.S. *Privacy Act* establishes the conditions under which a government institution may disclose personal information without the consent of the individual. One such condition is "for a routine use", that is, a use consistent with the purpose for which it was collected. Under this provision, computer-matching to detect fraud has become a common practice in some agencies. It has been estimated that some 500 computer-matching programs are regularly carried on in American jurisdictions.

The terminology of the U.S. act is close enough to that of the Canadian legislation to leave privacy protectors uneasy lest the words "routine use" be invoked to justify computer-matching in this country.

Computer-matching turns the traditional presumption of innocence into a presumption of guilt. In matching, even when there is no indication of wrongdoing, 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.

In the Richardson decision, the Supreme Court of Canada held that Revenue Canada, in pursuit of tax information, should not have complete access to a brokerage house's list of customer transactions. The examination

of such a list under the presumption that anyone involved in certain transactions could be guilty was characterized by the court as a "fishing expedition". Though this decision reinforces the protection against cross-matching now implicit in the *Privacy Act*, growing pressure to use the technique in pursuit of some admirable causes may make it prudent to make the prohibition specific and explicit.

Indeed, the *Income Tax Act* has already been amended to allow Revenue Canada to carry out legally precisely the kind of fishing expeditions which the Supreme Court held to be illegal. It must be asked if Parliament was sufficiently aware that it was over-ruling the Supreme Court and giving legal sanction to a practice which turns the presumption of innocence upside down.

Social insurance numbers

The Office of the Privacy Commissioner continues to receive many inquiries about social insurance numbers (SIN). For many persons a SIN is the focus and, unfortunately, the limit of privacy protection concerns. As such, it is important. The danger of singling out SINs for special treatment is that the protection of other personal information may seem less important and be neglected. SINs should be protected from indiscriminate and trivializing uses. But so should all personal information.

A social insurance number is personal information as defined in the *Privacy Act*. It receives the same protection, no more or no less, than does any other identifier or item of personal information. The issue is whether this number is so important, so special, that it requires controls over its use beyond that already offered.

At present, no legislation restricts the use of social insurance numbers. There are, however, 11 laws or regulations giving federal agencies the authority to request a social insurance number. These are:

Unemployment Insurance Act, 1971
and Unemployment Insurance
Regulations
Immigration Act, 1976
Income Tax Act
Canada Pension Plan Act
Old Age Security Act
Canada Elections Act
Canadian Wheat Board Act
Race Track Supervision Regulations
(Criminal Code)
Gasoline Excise Tax Refund
Regulations
(Excise Tax Act)
Canada Student Loans Regulations
(Canada Student Loans Act)
Family Allowances Regulations
(Family Allowances Act, 1973)

If a number is requested for any other purpose, an individual is simply not obliged to meet the request. Of course, by not providing the number, he or she may be denied the goods or services which are desired.

The arguments for special status deserve respect. Unwanted information linkage through a SIN may still be easier than through any other single piece of personal information. However, with new computers, that may not be true much longer.

Uncontrolled and general use of the SIN establishes a de facto national identifier with all its ominous and de-humanizing implications. But after a thorough study of the issue, the former Privacy Commissioner, Inger Hansen, opposed placing any legal restriction upon using social insurance numbers. She argued that such would be a band-aid solution, and a dangerous one, for it would convey a false sense of privacy security. She felt that private identifiers would take the place of SINs, though persons might think that their privacy was effectively protected because the law controlled the uses of the SIN.

Ms. Hansen's recommendations went beyond the narrow issue of SIN usage. She proposed that anyone collecting personal information of any kind be forced by law to disclose its intended uses. Uses not disclosed in advance, not consented to or authorized by law would be illegal.

Another proposed approach is legislation to limit the legal use of SINs to the federal government and within the federal government.

SINs are not collected to be exchanged with other federal agencies: that would contradict the *Privacy Act*. Nor are the SINs, which government institutions are authorized by statute to collect, available to institutions or individuals outside government. Therefore, possession of another person's SIN should no more unlock personal information from government than using another person's name.

Electronic surveillance

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*.

It is easy enough to say that such protection should be part of the bargain between employee and employer. That should be the first line of defence. But it can be a one-sided combat when an employer installs, for example, telephone monitoring. The legitimate goal of preventing abuse of the long-distance network means that all calls are recorded and new significantly closer supervision is introduced. Personal privacy is inevitably the loser.

But monitoring telephone calls is almost benign compared to surveillance by either video cameras or other security and locator systems which can record the movement of employees at or outside of their workplace — with or without their knowledge. Such surveillance is benign as well when compared to measuring the productivity of cashiers, airline personnel or telephone operators who are using computer terminals that tabulate the number of keystroke entries.

Eavesdropping, more insidious and effective than wiretapping, may now be carried out by using optical systems, parabolic microphones, beepers and tonal pagers for electronic tracking, by magnetic cords and by telephone, cable TV and VDT monitoring. These new devices so enhance the capabilities for surveillance anywhere that the illegal older methods of wiretapping or "bugging" are almost obsolete.

The "natural" home for legislative protection against attacks on privacy through electronic devices would be the *Protection of Privacy Act* (Part IV.1, Invasion of Privacy, Criminal Code). The main purposes of this Act are to prohibit unauthorized wiretapping of telephone conversations and to establish ground rules for legal telephone eavesdropping by police. Since the *Protection of Privacy Act* now prohibits physical surveillance, broadening its provisions to cover the new kinds of eavesdropping would have a certain logic.

Unfortunately, the act evokes little confidence. According to critics, it too successfully eases the way for police wiretapping and its name is a perverse irony. A recent working paper of the Law Reform Commission found it "astounding" that the number of court-authorized interceptions in Canada is 20 times, per capita, greater than in the United States.

Thus, the *Protection of Privacy Act* would be a weak and suspect base upon which to build protection against new kinds of electronic surveillance. It is so suspect and made so obsolete by new surveillance technology that a fresh start is required rather than tinkering amendments.

Is the answer in broadening the *Privacy Act* to cover electronic surveillance of all kinds? Should the *Criminal Code* or the *Canada Labor Code* deal with the issue in their separate ways?

The answers do not come easily and the questions go much beyond a review of the *Privacy Act*. But the present relationship between the *Protection of Privacy Act* and the *Privacy Act* is untidy and unsatisfactory. The division is based on distinctions which are hard to maintain because the old divisions have broken down.

The use of computers to link information or to draw up personal profiles is no less electronic surveillance than listening to telephone conversations. The new technologies and the threat do not respect separate statutory compartments. 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.

Extending privacy protection

Inside government:

When the *Privacy Act* was introduced, Parliament was told that the legislation was the first phase of federal privacy protection. The Act covered only the federal institutions set forth in the schedule to the legislation. The next phase, the government said, would be to bring federally-regulated institutions under the Act. Time was unspecified. Such an extension would include, presumably, banks, some telephone companies and broadcasting entities.

Federal institutions which competed in the market place, such as Air Canada, CN and the CBC, were not included from the beginning because of perceived disadvantages to their competitive position.

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.

Federal institutions competing in the market place should be asked to demonstrate why compliance with the *Privacy Act* would put them at a disadvantage. Privacy protection does not, in fact, impose significant costs. Some private sector institutions are themselves accepting voluntary data protection codes. Why should Canada Post be covered by the *Privacy Act* and not, say, CN? Why National Film Board and not the CBC?

Outside government:

The next logical extension of the legislation — the second phase which was anticipated in 1982 — would take the *Privacy Act* beyond the confines of federal institutions to include federally-regulated institutions.

Such an extension would cover Canadian chartered banks, telephone companies regulated by the Canadian Radio-Television and Telecommunications Commission and cable television companies, also regulated by the CRTC.

Today's fashion is said to be for deregulation. If that is so, and government is reluctant to extend its authority, broadening the *Privacy Act* would have to be justified by demonstrable abuses of privacy. Moreover, to push privacy legislation where it is neither necessary nor wanted would cause it to be held cheap or to make it a burden rather than an asset.

No endemic abuses have been brought to the attention of the Privacy Commissioner's Office, though there have been many inquiries as to whether banks, telephone or television companies are covered by the *Privacy Act*. The inquiries suggest a general unease over the potential impact of computer technology upon personal privacy. Public apprehension often focuses upon the adequacy of protection for the privacy of credit card transactions. Inter-active cable television, though still in a formative stage, sometimes raises privacy concerns.

Such apprehensions are entirely healthy. The possibility of violations of privacy are enormous.

But banks appear to recognize their strong vested interest, as well as the legal requirement, of maintaining high standards of confidentiality. The banking industry has developed a statement of privacy principles to which it pledges adherence. Individual banks are presenting their own privacy codes to give substance and rigor to the principles. A large credit bureau has recently adopted a code of operating standards which incorporates important privacy protection principles. The association of cable television operators was among the first such private sector organizations to develop a code of fair information practices. At the initiative of the CRTC, stricter data protection provisions have been put into telephone company regulations.

In the face of this, 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.

It should also be remembered that the regulators of federal institutions do not need new privacy legislation for them to press privacy codes upon the institutions under their jurisdiction. What is needed, very simply, is their commitment to privacy principles outside the walls of government.

Transborder data flow

Concern over vast amounts of information crossing international boundaries by the marvel of electronic data processing and transmission quickly transcended the privacy issue. Even the pioneering study of the departments of Communications and Justice, "Privacy and Computers" observed that the principal problem with the flow of Canadian data into the United States

"... is not one of the privacy of Canadian data subjects being invaded by data about them being stored in the United States. It is rather that data processing and communications business may be lost to Canadians as a result of this foreign flow; that data in United States databanks might be peremptorily withheld abroad for a variety of reasons. . . . that United States laws might change and leave Canadians less well-protected; and that, as a sovereign state, Canada feels some national embarrassment and resentment over increasing quantities of often sensitive data about Canadians being stored in a foreign country."

Thus, economic protectionism and sovereignty were intertwined with privacy from the beginning; the non-privacy issues in fact often dominated the discussions. International organizations, notably the Organization for

Economic Co-operation and Development (OECD) and the Council of Europe, rather than individual nations have worked to keep privacy an integral part of all transborder data flow considerations.

If there are no, or limited, privacy protection laws within a country, no convincing claim can be made that a loss of protection is suffered when personal information crosses an international boundary line.

Like charity, the protection of transborder data begins at home. Before countries earn the right to preach about protecting privacy values in the flow of personal information crossing borders, they need to have adequate data protection laws within their own jurisdictions.

Non-government institutions also earn the same right only by having established and honored their own effective codes for the protection of the privacy of their employees and customers. Such codes should be consistent with the *Privacy Act* principles of fair information practices.

Therefore, for starters the Canadian government should demonstrate the seriousness of its desire to protect the personal information of its citizens from abuse either inside or outside the country by extending the *Privacy Act* to include all its own institutions and to encourage others to adopt fair information practices.

It is at least premature to raise alarms about transborder data flow and privacy when this country has done so little about implementing the OECD guidelines.

The private sector and the OECD guidelines

The "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" are an admirable OECD initiative which set minimum standards for the treatment of personal data among member countries. As a country which in June, 1984, formally committed itself to adherence to the guidelines, Canada accepted the obligation, among others, "to encourage private sector corporations to develop and implement voluntary privacy protection codes."

Yet there is no evidence of even minimum encouragement by the government; no visible effort to discharge this obligation.

The last report of the Privacy Commissioner asked that the important commitment to foster voluntary privacy codes "be discharged with conviction and vigor and without further delay." The recommendation still applies.

Some industry associations and private Canadian companies, as has been noted, have not waited for their governments to urge them to put the OECD's data protection principles in place. But such initiatives are still exceptional in the private sector and, without any push from government, they will probably remain so.

Canada played an admirable leadership role in formulation of the OECD guidelines. It is difficult to understand the reluctance not to continue this role by having the guidelines implemented. Unless there is a sign that Canada takes its commitment more seriously, agreeing to the guidelines will seem like mere posturing, if not bad faith.

Section 19 - other governments' information

Subsection 19(1) of the *Privacy Act* reads:

"Subject to subsection (2), the head of a government institution shall refuse to disclose any personal information requested under subsection 12(1) that was obtained in confidence from

(a) the government of a foreign state or an institution thereof;

(b) an international organization of states or an institution thereof;

(c) the government of a province or an institution thereof; or

(d) a municipal or regional government established by or pursuant to an Act of the legislature of a province or an institution of such a government."

The purpose of such exemptions is clear enough: the exchange of information is part of the life-blood of modern governments. Without some assurance that information being given out will be protected by the receiving government, the most useful sources of supply could dry up. Governments also want to control their own information. They do not want sensitive data, held secure in their jurisdiction, to be released under the access laws of another jurisdiction. It is a matter of informational sovereignty and, in principle, that is entirely defensible.

What is not defensible are the blanket claims of confidentiality which have been declared 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, one level of government to another. When a province unilaterally imposes confidentiality upon all information it shares with the federal government, 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."

The point has been made in the first two annual reports of the Privacy Commissioner: the *Privacy Act* may now be used to prevent an individual from receiving personal information which he or she might have received before the legislation was in effect. It is, of course, profoundly damaging to the credibility of the *Privacy Act* if confidentiality claims are not made for good and sufficient reasons.

On two occasions, the Privacy Commissioner made the following recommendation:

"The matter should not wait to be addressed until the parliamentary review. The Minister of Justice should draw the problem to the attention of his provincial colleagues, requesting their cooperation in protecting the integrity of the federal legislation. Without that cooperation, we face the paradox of an expanded *Privacy Act* reducing individuals' rights."

The Minister of Justice may indeed have raised this issue with the provincial attorneys' general. Unfortunately, section 19 and confidentiality blankets still prevent a significant number of individuals from receiving personal information to which they would be otherwise entitled.

Investigators from the Privacy Commissioner's Office have been instructed to ask federal custodians of provincially-originated information to seek release of personal information by provincial authorities on a case-by-case basis. This approach was taken when provincial authorities, in response to the Privacy Commissioner's complaint, said that they wanted the opportunity to review each request and that they would be disposed to authorize releases in the spirit of the *Privacy Act*.

Unfortunately, the formal claim of confidentiality is usually given more respect than statements of goodwill. Most federal institutions play it safe — and easy. They remain reluctant to get behind the general prohibition and unresolved complaints pile up in the Privacy Commissioner's Office.

Section 19 remains a major source of frustration to applicants for personal information and to the administration of the *Privacy Act*.

There are two possible solutions:

- 1) remove the absolute protection which the *Privacy Act* now gives all information coming from sources outside the federal government;

2) convince provinces to withdraw claims of total confidentiality.

When provinces adopt privacy legislation of their own, individuals will be able to apply directly for personal information under provincial control. As this happens, section 19 should become a less significant problem. In addition, provinces committed to the fair information practices represented by privacy laws are not as likely to make excessive confidentiality demands. But these hopes are of no help at all to those whose personal information is now captive of section 19.

Role of the Privacy Commissioner

The basic utility of the Privacy Commissioner's Office is that it exists. Government ministers and government managers know that the way they handle personal information under their control is subject to review. It will not be limited, remote or unlikely as a review resulting from an appeal to the Federal Court. But it will be a review made systematically by an office reporting directly to Parliament, an office with broad investigatory powers, with statutory responsibilities to see that personal information is handled according to the specific data protection principles set forth in the *Privacy Act*.

The Office also provides a special place for persons to turn when they feel deprived of a privacy right: a place less awesome, less formidable, less expensive and less cumbersome than a court; a place with more specific privacy expertise; a more useful place. Yet the Office is as rigorously independent of government as any court. The Commissioner can be removed only after a resolution passed by both the Senate and the House of Commons; he has the security of a long term.

Of course, the Commissioner cannot issue enforceable orders. Ministers may reject his recommendations, if at the peril of being cited in his annual report to Parliament or being over-ruled by the Federal Court to which the Commissioner, as well as a complainant, may appeal.

Should the Privacy Commissioner be able to make decisions binding on government? The test is whether such authority would make the Office any more effective on behalf of its clients and privacy protection. It is doubtful that it would. The ombudsman's role is preserved. Negotiation and persuasion

now often achieve what an adversarial position would not. It can be an advantage not to have the power to issue orders.

A Privacy Commissioner with authority to compel compliance would be cast instantly in such an adversarial role. Positions would harden, putting the Privacy Commissioner's Office in a chronic state of war with government institutions. Investigations in such an atmosphere would be more difficult and not be in the best interest of anyone. Cooperation, not confrontation, is the goal.

The direct access the Privacy Commissioner has to Parliament, either by an annual or special report, sustains the Office with all the authority it requires.

Consulting the Commissioner

If the Office does not seem to require new powers, its consultative role should be examined, better defined and strengthened. The context in which the Privacy Commissioner sees this role was put as follows in his first annual report:

"... he is not called 'Privacy' Commissioner to be a non-combattant in the endless war between the individual's claim to privacy and the state's need to regulate. Both are legitimate claims. But the balance should be struck and priorities established by legislators and not by the Privacy Commissioner.

"Privacy gives way to competing social values, for example, to the claims of national security and justice, when the legitimacy of such claims has been established. But the contest is often even and the choice difficult.

"The Privacy Commissioner will assert the privacy claim and only this claim. That does not mean the Commissioner is unmindful of or insensitive to other values and interests. But they will be for others to assert."

The question is how best should the consultative function be discharged? The Commissioner's Office maintains a watching brief on new legislation for possible conflicts with the *Privacy Act*. On two occasions the Commissioner's Office has been asked about the privacy implication of contemplated legislation. These initiatives showed an encouraging sign of sensitivity to privacy issues by the legislative planners.

But at other times the *Privacy Act* appears not to have been taken into serious consideration nor is the Privacy Commissioner consulted routinely in advance of some legislation or policies impinging upon the *Privacy Act*.

Item:

Bill C-48, the *Family Orders Enforcement Assistance Act*, was passed by the House of Commons on January 23, 1986. When the Bill was being reviewed by House and Senate committees, the Privacy Commissioner advised that the legislation would make an important exception to privacy protection principles contained in the *Privacy Act*.

Question: Should the Privacy Commissioner appear before such committees to address his privacy concerns?

Item:

Amendments passed in 1985 to the *Aeronautics Act* dealt with the reporting of medical and optometric examinations of flight crew members, air traffic controllers and other holders of Canadian aviation documents which impose fitness standards. The act deems that consent has been given by the patient to have his or her medical information transmitted from the examining physicians to medical advisors to the Department of Transport.

Medical records coming from outside doctors and optometrists become the property of the Department of Transport and, as such, subject to complaints and audit under the *Privacy Act*. The *Aeronautics Act* does not provide for the proper control of such information nor is the location of the information indicated.

Clearly, no thought was given to privacy principles when this act was being drafted.

Question: Why was the Privacy Commissioner not consulted?

Item:

In 1982, the *National Harbours Board Act* was amended by the *Canada Ports Corporation Act*. The effect of this new act was to allow the government to establish various ports in Canada as separate corporations. Before this amendment, the ports were all part of the National Harbours Board.

The National Harbours Board was a government institution under the jurisdiction of the *Privacy Act*. Subsequent to the passage of the amendment, some

harbours were set up as separate legal entities. No amendment was made to the schedule of the *Privacy Act*, effectively removing personal information from the control of the Canada Ports Corporation and putting it under the control of the newly-created ports. Canadians were therefore deprived of access to personal information which was formerly accessible when in the possession of the Canada Ports Corporation.

As a result, the Privacy Commissioner had to dismiss a complaint because of lack of jurisdiction. Authorities of the port in question did not know that it no longer came under the jurisdiction of the *Privacy Act*. Yet they refused to release some information.

The matter has been brought to the attention of lawyers for Canada Ports Corporation and the Department of Justice. No action has been taken to date to restore rights lost as new ports corporations are created and not added to the schedule of government institutions.

Question: Why wasn't there some awareness of the impact of the changes upon privacy rights?

Item:

In 1985, a "Conflict of Interest and Post-Employment Code for the Public Service" was announced and implemented. The Privacy Commissioner had serious privacy protection concerns about the code, concerns he expressed in a letter to the Secretary of the Treasury Board. The letter raised questions about the employer's mandate to demand "sweeping disclosures which go far beyond those supplied on a curriculum vitae or those required on an

employee's routine personnel information form." The letter noted that the collection process itself poses a threat to personal privacy and that the protection offered by the *Privacy Act* may be insufficient.

The letter also pointed out that by demanding the personal information required by the code as a condition of employment, the government makes that information integral to an employee's position. If this is so, the information may not be exempted as being personal and the government as employer would be left, as the letter stated, "in the invidious position of not offering its employees any expectation of confidentiality for highly personal information which might be sought under the *Access to Information Act*."

The government may have a reassuring reply to these arguments, though none has yet been received.

Question: Why was there no advance consultation with, or advice sought, from an office which has special responsibilities for and sensitivity to privacy protection?

Item:

In November 1985 a fundamental change was made in the Regulations without any notification, before or after, to the Privacy Commissioner.

Originally, when a government department refused to make a requested correction to personal information in its files, applicants were to be informed that they had the right to "require a notation of the correction requested be attached to the information". Section 11 of the Regulations read as follows:

"11.(2) Within 30 days after the receipt of a Correction Request Form the head of the government institution that has control of the personal information shall

(a) where the request is complied with, notify the individual that the correction requested has been made; or

(b) where the request is refused, notify the individual

(i) that the request has been refused and set out the reason for the refusal,

(ii) that the individual has the right to require that a notation of the correction requested be attached to the information, and

(iii) that the individual has the right under the Act to make a complaint to the Privacy Commissioner."

The new version requires the department only to tell the individual that a notation, which says that the request for correction has been refused in whole or in part, has been attached to the personal information. Even if the applicant has said that the information is entirely wrong, the only notation to be appended now is that the department refused the request.

Under the former section, if applicants said the information was wrong, they would have been notified that the government refused its correction. Then a notation could have been put on file explaining what the applicant believed to be the correct information. The Regulations now state in section 11:

"(4) Where a request by an individual under paragraph (1)(a) to correct personal information is refused in whole or in part, the head of the government institution that has control of the personal information shall, within thirty days after the receipt by the appropriate officer of the Correctional Request Form forwarded by the individual,

(a) attach a notation to the personal information reflecting that a correction was requested but was refused in whole or in part;

(b) notify the individual that

(i) the request for correction has been refused in whole or in part and set out the reasons for the refusal,

(ii) the notation under paragraph (a) has been attached to the personal information, and

(iii) the individual has the right to make a complaint to the Privacy Commissioner;

(c) notify any person or body referred to in paragraph (1)(b) that the notation under paragraph (a) has been attached to the personal information;"

The former version afforded persons seeking redress under the Act much better protection.

Question: Why is the consultative role of the Privacy Commissioner's Office not better defined and strengthened?

The audit function

The most important single change between Part IV of the *Canadian Human Rights Act* and the *Privacy Act* is the added authority given to the Privacy Commissioner to "carry out investigations in respect of personal information under the control of government institutions to ensure compliance with sections 4 to 8."

Without this authority, the role of the Privacy Commissioner would be essentially passive, an ombudsman waiting, if not for Godot, for complaints of greater or lesser significance to investigate. Section 37 gives the Privacy Commissioner the mandate, and surely the obligation, to initiate continuing, comprehensive and systematic investigations into the way personal information is collected, protected, used and disposed of by every federal government institution covered by the *Privacy Act*. Thus, he can become a vital player in data protection.

The Canadian Privacy Commissioner does not play the central role of European Data Commissioners in data protection; government in Canada retains basic control. But the audit function enormously enhances his role from that of pure ombudsman. In the long term, his auditing authority will have, if it does not already, a much greater impact on data protection than his complaint-handling responsibilities.

None of this is to downgrade the importance of effective responses to individual complaints. They have received priority from the start; more investigators are still assigned to complaints (six) than to compliance (four), though those figures may soon be reversed.

The Privacy Commissioner should become, if he is not already, to personal information auditing what the Auditor General is to financial control.

This should not require anything like the staff resources of the Auditor General. In fact, the Privacy Commissioner's compliance operation should be conducted by a small number of investigators possessing specialized auditing skills. It is neither acceptable nor necessary to create a large new compliance auditing bureaucracy. The public service cannot support an ever-expanding number of oversight authorities with ever-expanding staffs; the system becomes overloaded.

The front line in the battle for effective data protection is within government institutions themselves. Their heads, after all, have the responsibility to implement the principles of fair information practice set forth in the *Privacy Act*. Knowing that the Privacy Commissioner can, at any time, initiate an investigation into a government institution's handling of personal information should have a salutary effect upon standards of record-keeping.

Auditing for compliance with the Act should be as much a part of internal audits as routine financial or management audits. That has not yet happened, though a start is being made. It is the Privacy Commissioner's responsibility

and intention to determine that the heads of government institutions take their *Privacy Act* responsibility as seriously as any other of their statutory obligations.

Compliance investigators have carried out an audit of all the personal information banks of a large department (Fisheries and Oceans). As noted previously, investigation of information banks designated as exempt from access has also begun. The Privacy Commissioner accepts a special responsibility toward these banks because of their intrinsic sensitivity, because they are closed and because he is the only outside agent authorized to give them independent scrutiny.

It would seem that Parliament would expect compliance investigations of these above all other information banks.

In addition to their examination of both open and closed personal information banks, compliance investigators are auditing the manner in which government institutions respond to requests from investigative bodies to disclose personal information under the authority of section 8(2)(e) of the *Privacy Act*. This section sets forth certain procedures to be followed: that each request should be in writing; that the request specify the information being sought. Subsection 8(4) provides that a copy of every request from an investigative body be retained along with a record of any information disclosed. These records are to be kept for examination by the Privacy Commissioner.

An audit of the handling of 8(2)(e) requests became especially timely after section 9 was amended, ending the requirement for a notation on an individual's file indicating that it had been

seen by an investigative body. Since individuals now no longer know that outsiders have been looking at their files, it seemed important for the Privacy Commissioner's Office to determine if third party access was in accordance with the requirements of the *Privacy Act*.

That specific audit is well advanced and soon every institution covered by the *Privacy Act* will have been covered. The exercise has itself been important. Neither serious nor endemic compliance failures were discovered. It was also useful because within a short time it raised the privacy flag in a great many places. Departments suddenly knew that there was such a thing as compliance auditing. The audit introduced many departments to the Privacy Commissioner's officers for the first time. The investigators met privacy co-ordinators and others to test knowledge of, and interest in, the *Privacy Act* and to discuss matters of concern raised by those being visited.

A credible audit demands an intellectually defensible methodology. Four auditors, confronting hundreds of thousands of files, face the daunting challenge of being able to make valid findings without spending a working lifetime examining each one. Assistance in devising sampling methods has been received from statisticians.

Exempt information banks

One of the most sensitive and vexed issues arising during the first years of the *Privacy Act* is the status of and necessity for what are called, in the jargon of the privacy trade, exempt banks. Some history is indispensable.

Little concern was expressed about exempt banks during the legislative passage of the *Privacy Act*. It seemed straightforward enough: section 18 gave the Governor-in-Council the right to "designate as exempt banks certain personal information banks" containing files all of which consisted "pre-dominantly" of personal information of a particularly sensitive nature. Information qualifying a bank as exempt would be that which, for example, "could reasonably be expected to be injurious to the conduct of international affairs, the defence of Canada" or personal information obtained or prepared in the course of criminal investigations.

When the Act came into effect, 19 (of some 2,200) banks were designated as closed; following a complaint to the Privacy Commissioner, an additional bank was closed. Individuals who applied for personal information which might be contained in the closed banks were denied access, being given neither denial nor confirmation of the existence of information about them.

The Privacy Commissioner has the responsibility for the oversight of these closed banks. He may examine all personal records (except confidences of the Queen's Privy Council) in any bank in which personal information is kept. The Commissioner may recommend that files be removed from a bank, or material be removed from files and transferred to other banks, or that files be destroyed. He can do this while neither confirming nor denying the existence of a particular file, if that has been the position of the department. He does, however, assure a complainant that he, an independent officer, has looked at the files in these banks and that the complainant's privacy rights have been respected.

The status of these exempt banks was challenged following the application of Nick Ternette for personal information from RCMP bank P-130, Security Service Records (now SIS-P-PU-010). The RCMP would neither confirm nor deny the existence in the bank of any personal information about the applicant. Mr. Ternette complained to the Privacy Commissioner who investigated and found that he too could neither confirm nor deny the existence of any record. He told Mr. Ternette his rights had been respected and advised him of his right to appeal to the Federal Court of Canada for a review of the RCMP's refusal of his application.

Mr. Ternette appealed. His lawyer asked the Department of Justice to confirm that all the files in the bank had been examined before it was closed to determine if the bank met the criteria for exemption. The Department of Justice responded that the files had not been individually reviewed and that the bank should now be treated as an open bank.

Such new treatment does not mean that the power to exempt sensitive files has been diminished in any essential way. Personal information in this or any bank may not be released if exemptions provided in the *Privacy Act* can be applied. But losing exempt status does mean that a file can be exempted only after a specific, new examination, and not merely because it is found in a special bank.

The Department of Justice's inability to defend the validity of the RCMP's exempt bank forced the Privacy Commissioner to abandon an original working assumption that exempt banks were properly closed.

The Privacy Commissioner has a special responsibility, because of the uniqueness of his access, to examine closed banks for compliance with the *Privacy Act*. When the office first opened for business, he had to assume the validity of the exemption of each of the 19 banks from the general right of access. Without making such an assumption, it would have been impossible to carry out the immediate and pressing duty of investigating all complaints. In fact, had the original investigation staff of four persons been set to work on examining closed banks, complaint-answering would have been indefinitely delayed, effectively denying many applicants their privacy rights.

In January 1985 the compliance branch of the Privacy Commissioner's Office began a systematic examination of all closed banks. The first to be investigated were two banks of Employment and Immigration Canada, EIC/P-PU-260 (Immigration Security and Intelligence Data Bank) and EIC/P-PU-265 (Enforcement Information Index System). These banks were chosen for the administrative convenience of the Privacy Commissioner's Office, not because of any special concern. The Commissioner was 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. However, the investigation found evidence that individual files had not been examined prior to the application for exempt status.

The Privacy Commissioner informed the deputy minister that since the banks did not meet the criteria of the *Privacy Act*, he would treat any complaints relating to these banks in the same manner as those against open banks.

The Privacy Commissioner also asked deputy ministers responsible for all other closed banks to advise him whether files in these banks were properly examined before a submission for exemption was made to the Governor-in-Council. On the basis of the replies and planned systematic audits, findings will be made as to compliance of the exempt banks with the provisions of the *Privacy Act*.

Any banks which, in the opinion of the Privacy Commissioner, were improperly constituted will be treated as open. Though this involves a fundamental change in the handling of the personal information in such banks, the change is not sweeping so far as the ability to exempt information is concerned.

Yet there is some gain from the data protection standpoint. 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.

From the Privacy Commissioner's point of view, there is another advantage in the loss of exempt status. The very fact that whole banks of personal information are excluded from access discourages persons from using the *Privacy Act* and fosters skepticism about the usefulness of the legislation. Opening up these closed banks should enhance the credibility of the *Privacy Act*.

In summary: The concept of exempt banks remains defensible. Their disadvantages perhaps make them dispensable.

Opening up Access

The right of access to personal information under the *Privacy Act* is now given to, in the words of subsection 12(1), "every individual who is a Canadian citizen or a permanent resident within the meaning of the *Immigration Act*, 1976."

Privacy Act Extension Order No. 1 was made on July 24, 1983, only a few weeks after the *Privacy Act* became effective. The order extended the right of access to include an inmate within the meaning of the *Penitentiary Act* who is not a Canadian citizen or a permanent resident within the meaning of the *Immigration Act*, 1976.

Thus non-Canadians and non-permanent residents who are incarcerated in Canadian prisons qualify for all the rights of the *Privacy Act* while non-Canadians and non-permanent residents who are outside of prisons do not.

If there were good reasons for allowing anyone in a Canadian prison to use the *Privacy Act* (and there were: to fulfill Canada's international obligations), there are stronger reasons for giving access rights to those persons in the country who are not in prison.

The anomaly is unfair and unsustainable. It should be ended quickly by extending the right of access to any person applying for access from within Canada. The lesser additional anomaly is that the personal information of such persons is now protected (along with everyone else's), though they have no right to receive such personal information.

Persons with non-resident status are often affected profoundly by administrative decisions of federal government institutions. They may be entitled, under some legislation, to their personal information upon which a decision may have been based. But that entitlement may come too late to be useful; sometimes there is no entitlement at all.

Opening the *Privacy Act* to anyone in this country would end a mean discrimination contrary to the very spirit of the Act.

The Role of the Coordinator

From his first report, the Privacy Commissioner has emphasized the importance of the "privacy professionals" — the privacy coordinators — in each government department who are given specific and special responsibilities in the administration of the *Privacy Act*.

There 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 coordinators by their superiors. Some coordinators 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 coordinator is not yet generally seen as desirable for career progress.

In departments and agencies with few privacy requests, a lesser role may seem understandable enough. Yet the function of the privacy coordinators should be much more than handling specific applications. It should, for example, be also a teaching role with coordinators training departmental staff, sharing their knowledge of, and sensitivity to, data protection both with their colleagues and those outside of the public service.

Given greater encouragement to act as privacy advocates and animators, coordinators could reduce the still widespread invincible ignorance about the *Privacy Act* and play their legitimate role of true privacy professionals.

Complaints Branch

Investigating complaints is the heart of the office's day-to-day business. Investigators completed work on 401 such complaints during the reporting year. The Commissioner found 221 justified while dismissing 173. The remaining seven were abandoned.

More than 46 per cent of the complainants believed they had been denied some or all of the material improperly; 44 per cent complained that departments had taken longer to respond to requests than the initial 30 days or maximum 60 days the Act permits; a little more than three per cent complained that personal information was misused; just under three per cent complained that they were denied a correction or notation to their files; two per cent disagreed with departments' collection, retention or disposal of personal documents; less than one per cent complained about the language of the documents or deficiencies in the Personal Information Index.

While 401 complaints may appear to be a large number, the figure should be balanced against approximately 36,000 applications which government agencies received during the same period.

During the October 1 to December 31, 1985 quarter (the latest for which Treasury Board statistics were available at press time), National Defence alone received 4,708 new applications, Correctional Service Canada, 1,376, and Public Archives, 1,307. Delays accounted for 101 of the 173 complaints against Correctional Service Canada and 43 of the 48 against National Defence.

A few departments are the focus of the most complaints because, for example, the information handled has considerable impact on the individuals (Correctional Service Canada — 173 complaints), because of the sheer volume of their clients (Employment and Immigration Canada — 41), or the size of their workforce (National Defence — 48), or the nature of their files (RCMP — 40).

In choosing cases for this report, an effort was made to balance the departments selected, given the focussed nature of the complaints.

Conducting an investigation

Once an individual complains to the Commissioner (usually — but not necessarily — in writing), the Commissioner advises the government department that there will be an investigation.

Although the Act give the Commissioner authority to enter government premises, subpoena documents and compel testimony, he has not yet been required to use it. Informal methods are preferred and they have sufficed. Nevertheless, the powers are there if needed.

At the conclusion of the investigation (which must be conducted in private), the Commissioner tells the complainant what he has found and whether he considers the complaint justified. If the complaint is justified, the Commissioner notifies the department and makes appropriate recommendations. He may also ask the department to advise him, within a specified time, as to how it proposes to deal with his recommendations.

When the Commissioner puts a limit on the department's time to respond he must delay his report to the complainant until the time has expired. If the department does not meet the deadline, or if the Commissioner considers the response inadequate, he may report with any comments he finds appropriate to the complainant.

The Commissioner may, with the complainant's consent, ask the Federal Court to review a complaint that access was denied. There is no court review of complaints about delay, misuse, correction/notation, collection/retention/disposal, language, or the Index.

Access

This category includes complaints from applicants who have been denied some, or all, of the information in their files. The *Privacy Act* permits departments to withhold personal information if, for example, it concerns someone else, if it was received in confidence from another level of government, if its release could endanger another person or Canada's defence or the conduct of its affairs. (For a complete list of exemptions, see The *Privacy Act* and You on page 59.)

"Secret" files released

An employee of Treasury Board complained to the Privacy Commissioner that her employer had kept secret files about her. She alleged that the information was collected without her knowledge, that it was defamatory, improperly used and disclosed, and withheld from her when she applied to see it under the *Privacy Act*.

The department's privacy coordinator had asked the Staff Relations Branch, where her documents were held during a grievance procedure, to respond to the woman's request. The branch, in turn, had asked the unit, where the complainant worked, to send it all relevant documents. The branch assembled material and returned it to the coordinator to pass on to the woman.

The investigation disclosed that the branch omitted documents from the package of material sent to the coordinator. Among the missing documents were three briefing files for senior staff about the complainant's grievance and five sealed envelopes containing material from her work unit. The briefing material was withheld as the branch believed it was not accessible under the *Privacy Act*.

The investigator examined all the documents and recommended that they be released and Treasury Board agreed.

The complainant asked that the documents be destroyed. When the investigator explained her right to correct factual errors or to note the files, the woman dropped her other privacy complaints and chose to pursue the matter through the Public Service Commission and the Canadian Human Rights Commission.

The Commissioner found the complaint justified.

Informant's Name Is Private

A New Brunswick woman complained to the Commissioner that Employment and Immigration Canada had removed identifying details from the copy of a letter she received in response to a privacy request.

The letter alleged that the woman was not entitled to receive unemployment insurance because her fisherman husband was selling the catch in her name to qualify her for unemployment insurance. EIC sent the woman a typed copy of the hand-written letter, omitting the name, address and any details which would identify the letter writer.

EIC withheld the information because its release could impair a lawful investigation and identify a confidential source of information. EIC uses these sources to retrieve hundreds of thousands of dollars of fraudulent claims annually. The department also worried that there could be reprisals against the informant.

The Commissioner concluded that the concern about reprisals was real and that the department had properly invoked the relevant section of the *Privacy Act*. He dismissed the complaint.

Copy Not Needed For Access

A public servant complained to the Commissioner that the Public Service Commission (PSC) had denied a copy of the tape of the oral part of his French language test. PSC had offered to let him hear the tape in the company of one of its language assessment officers but the complainant maintained that the Act gave him the right to his own copy.

The Commissioner examined the complaint and concluded that the Act quite clearly gives the department its choice, whether to "permit the individual to examine the information ...or provide the individual with a copy...".

He dismissed the complaint.

Form Found In Regional Office

An RCMP employee asked to see his files so he could learn why he was denied a promotion. After examining the file, he complained to the Commissioner because a form was not included which illustrates the scores of members being considered for promotion.

When he was told that the applicant had received everything in the file, the Privacy Commissioner's investigator discussed the problem with RCMP staff. As a result, "B" division in St. John's was consulted and the form was eventually found. It had been missed in the first search because it was not placed in the proper files. As a result of the complaint, "B" division now holds the form in the appropriate place.

The Commissioner found the complaint justified and the file was referred to the Compliance Branch for follow-up.

Complaint Brings Pension

A man denied a disability pension under the Canada Pension Plan applied to see the information on which his application was dismissed. When he examined the material from Health and Welfare Canada, he found three medical reports missing and complained to the Commissioner that they had been improperly withheld.

The investigator's examination found that the man had received everything in the file. The medical reports, which Health and Welfare needed to make an informed decision about the man's pension entitlement, were not on file.

Health and Welfare said that, despite repeated requests, the doctor and two hospitals had not supplied the reports. The investigator reminded the staff that the *Privacy Act* requires departments to "take all reasonable steps to ensure that personal information that is used for an administrative purpose...is as accurate, up-to-date and complete as possible."

Health and Welfare agreed to try again and, within a few days, it was evident that headway was being made. The Commissioner advised the applicant that his office was "stepping back to allow Health and Welfare to do its job." Later phone calls to the complainant and department confirmed that the information was being obtained. The complainant reported finally that his disability pension was granted.

Although technically the complaint was not justified because all the information in the file was released, the Commissioner considered his intervention within his mandate to ensure that the information was accurate and complete.

Applicant Need Not Reapply

Correctional Service Canada (CSC) returned a former inmate's application to see his personal information in four banks because all the banks had been reorganized. CSC enclosed a list of the new banks and asked him to re-apply.

The man complained to the Commissioner that he had been denied access.

In a letter to CSC, the Privacy Commissioner observed that he had no difficulty with CSC's reorganization as such, but that an applicant who had cited bank numbers from a current edition of the Personal Information Index should receive access. "The onus is on the government institution to find the information", the Commissioner wrote.

"Since Mr. ——— inquired of all the information banks listed in the Personal Information Index, it seems to me that it is the duty of any department to see that he gets all the information as listed in the 1984 Index to these information banks. It is not the applicant's fault that the records' system has been changed," the Commissioner concluded. CSC searched the banks and provided the material.

The Commissioner recommended that any department reorganizing its personal information banks make the adjustments on an applicant's behalf during the interim period before the publication of the amended Index.

He found the complaint justified.

Negotiations Prompt Release

A Manitoba man lodged complaints with the Commissioner after several departments delayed providing, denied they had, or deleted requested material about him. The man, a government employee, was looking for any material about his political activities.

The investigation confirmed that Transport Canada had nothing about him in its files. The Commissioner also agreed that the Department of Justice's 30-day extension to review the material was reasonable and confirmed that material was properly withheld because it was subject to solicitor-client privilege. The Commissioner also dismissed the complaint that Employment and Immigration's (EIC) extension of time to respond was unreasonable.

However, the Commissioner disagreed with some of the exemptions applied by both EIC and the Privy Council Office (PCO). The investigator negotiated release of portions of several documents which had been totally exempted because they were privileged, were personal information about others, or were confidences of the Queen's Privy Council (the latter are outside the Act altogether).

The applicant was also sent sections of a document that PCO had considered "not relevant to the request".

The Commissioner found justified the access complaints against EIC and PCO.

Expense Claims Not "Personal"

An RCMP member grieved when the force denied him \$600 of expenses incurred during a transfer. He applied to see the various documents from the grievance but three pages were withheld because they concerned a third party.

The investigation revealed that the information withheld were travel claims of two other members, exempted by the RCMP on the grounds that this was personal information about other individuals. The investigator pointed out that information about the position or functions of federal employees is not "personal information" and may be released.

The RCMP agreed that the information was not personal and it was released.

The Commissioner found the complaint justified.

Applicant Supplies More Detail

A former inmate complained to the Commissioner that Correctional Service Canada (CSC) denied him access to personal information in eight of its banks.

The investigator confirmed that CSC could find no information and the Commissioner invited the complainant to provide more data.

Subsequently, the inmate supplied more details. CSC found the documents the man was seeking and mailed them to him. The Commissioner dismissed the complaint because the applicant had not supplied sufficient information to locate the desired documents.

Names Not Privacy Request

A representative of an employees' association, denied access to a list of Canada Post employees in the management, professional and scientific groups, complained to the Commissioner.

Canada Post maintained that the employees' names were personal information and could not be released.

In fact, both parties were wrong. The association representative may not apply under the *Privacy Act* for information about other individuals, because the *Privacy Act* gives access rights only to the individual who is the subject of the information. Since the names of federal employees are not personal information, contrary to the position of Canada Post, the list would normally be obtainable under the *Access to Information Act*.

However, since Canada Post is not subject to the *Access to Information Act*, the Commissioner could not refer the complainant to the Information Commissioner and he dismissed the complaint.

Application Can be a Problem

During an inquiry at the Laval maximum security institution in Montreal, an investigator's attention was drawn to a problem with which Correctional Service Canada has had to cope since the *Privacy Act* came into force.

The problem occurs when inmates coerce others into applying for personal information and then force them to turn over the material so other inmates can examine the inmate's record. A refusal to apply for the information can have serious consequences, but the consequences can be equally serious when other inmates find out the details of someone's record or evaluation.

Correctional Service's managers claim that penitentiary directors are free to require inmates to examine the documents in an office and not take them to their cells, thus protecting both the inmate's and the institution's security.

The problem is being monitored by Correctional authorities and the Privacy Commissioner.

Woman's Drawings Not Found

A Montreal woman sought the Commissioner's assistance in tracking down a collection of her drawings and paintings which helped her gain entry to Canada in the early 1930s.

The woman's father, after arriving in Canada from Poland, applied to bring the rest of his family. The Department of Immigration and Colonization (as Employment and Immigration was called) refused permission to bring his 12-year-old daughter because polio had left her physically disabled.

Following a lengthy exchange of letters and rejections, the applicant submitted his daughter's school marks and a portfolio of her art work. Eventually, the department relented and she was allowed to join her family but the art was never returned.

She applied to Public Archives but nothing was found in its large collection of documents concerning immigration from Europe during the period. A formal privacy application to Employment and Immigration also turned up no records and she complained to the Commissioner.

The investigation confirmed that neither Public Archives nor Employment and Immigration had the material in their files. It is likely that the woman's documents were in her father's immigration file and were thus destroyed as part of the regular procedure.

The Commissioner dismissed the complaint.

RCMP as Provincial Police

A school administrator complained to the Commissioner when the RCMP refused to disclose the names of members of a "Committee of Concerned Parents" who alleged wrongdoing between himself and a local businessman.

The RCMP refused the information because it was obtained in its role as provincial police. The *Privacy Act* requires that the RCMP "shall refuse to disclose any personal information . . . obtained or prepared . . . while performing policing services for a province . . .".

The investigation revealed that the provincial Ministry of Education had investigated and dismissed the charges of wrongdoing as unfounded. The complainants were told but committee members made subsequent complaints to the local RCMP detachment and the administrator considered it harassment.

The Commissioner explained in his letter dismissing the complaint that this information must be withheld under an agreement between the provincial government and the RCMP. He suggested the man call the provincial ombudsman.

Release Could Endanger Writer

A government supervisor complained to the Commissioner that the department had refused him a copy of a letter accusing him of sexual harassment in his office.

The department withheld the letter because the writer was afraid of the supervisor. Based on previous incidents, it was concerned that the supervisor might threaten the employee's safety.

Investigation revealed there was a history of violence.

The Commissioner concluded that the department's fear of reprisals was a "reasonable expectation" and dismissed the supervisor's complaint.

Woman Seeks Husband's Files

A woman asked the RCMP for documents about herself in six RCMP banks, including two containing records on members of the force. Her husband, a force member, and she, an RCMP civilian employee, were in the midst of a marriage breakup. She was seeking information in which her name appeared or, in which reference was made to an event concerning custody of their child. The material she received had several passages blacked out and as a result she complained to the Privacy Commissioner.

The investigator found that the RCMP had no information about her in two banks and had properly withheld a small amount of material because it concerned someone else and was obtained during a lawful investigation or an inquiry into a security clearance.

The investigator persuaded the force to release three more small items of information but there was nothing on any file about the child custody incident.

The Commissioner dismissed the complaint.

Misuse

Complaints in this category allege that the government is using or disclosing personal information without the individual's consent or for a purpose unrelated to the original use.

SIN Not For Public Display

A senior officer in a Correctional Service maximum security penitentiary complained to the Commissioner that a supervisor had posted a memo about him, complete with his social insurance number, in a central meeting room where it could be seen by other employees and inmates.

The memo contained his name and a directive about his work area. The *Privacy Act* does not consider information about a federal public servant's job, salary range and duties as "personal" and these details may be made public. However, an employee's SIN has nothing to do with the job or its duties, and therefore, is personal information and cannot be released.

The Commissioner concluded that the SIN was improperly displayed and considered the complaint justified.

... Nor are Grievance Procedures

A woman complained that her supervisor breached the *Privacy Act* by posting a grievance notice on an office wall where it could be seen by other employees and the public. (Grievance notices are formal documents in which employees allege that the employer has violated the collective agreement. They contain detailed allegations and can contain other individuals' names.)

The investigation found that the Employment and Immigration Canada supervisor had posted the notice and two other employees had seen it. The supervisor said that he had posted it only to remind himself of the deadline. EIC management had told the supervisor of his error and the notice was removed.

Following the investigation, EIC amended its personnel manual to require officers responsible for the administration of discipline to become fully conversant with the requirements of the *Privacy Act*.

The Commissioner found the complaint justified.

Only Doctors See Medical Reports

During a disciplinary procedure an RCMP officer was examined by a civilian medical specialist. When the doctor's report was seen by management, the officer complained to the Commissioner that the information had been misused.

The investigation revealed that the RCMP's own policy restricts members' medical files to health service officers (RCMP doctors). Once the force was aware of the incident it took steps to prevent its recurrence, including publishing a Medical Confidentiality Policy Statement as an annex to the RCMP Manual of Administration.

Evidence indicated that this was an isolated incident. Nevertheless, the Commissioner found the complaint justified.

Information Released in Error

An RCMP member complained to the Commissioner that documents he received from a privacy request contained personal information about other members. The documents concerned his promotion and transfer which had been grieved by another member.

The material he received highlighted others' personal information. He observed, "this made interesting reading" but he was concerned that the error had happened and that personal information about himself or any other member could be released.

It was apparent from the investigation that the material had been highlighted in preparation for its removal, but it was never erased.

The Commissioner considered the complaint justified and the RCMP took steps to ensure it does not improperly disclose personal information again.

GROUND OF COMPLAINTS AND INVESTIGATION RESULTS

Grounds	Abandoned	Justified	Dismissed	Total
Misuse	—	7	7	14
Access	5	60	120	185
Correction	—	—	12	12
Language	—	1	1	2
Index	—	1	—	1
Collection/ retention/disposal	—	2	8	10
Delay	2	150	25	177
Totals	7	221	173	401

Completed complaints by department, type, and result

Department	Complaint Type	Number (Total)	Justified (Total)	Dismissed (Total)	Abandoned (Total)
Agriculture Canada	Access Col/Ret/Dis	4 1 (5)	— 1 (1)	4 — (4)	— —
Atomic Energy Control Board	Access	1 (1)	—	1 (1)	—
Canada Post	Access Misuse	3 1 (4)	— —	3 1 (4)	— —
Canada Ports	Delay	1 (1)	—	1 (1)	—
Canadian Human Rights Commission	Access	1 (1)	1 (1)	—	—
Canadian Security Intelligence Service	Access	4 (4)	—	4 (4)	—
Communications	Access	1 (1)	—	1 (1)	—
Consumer and Corporate Affairs Canada	Access	1 (1)	—	1 (1)	—
Correctional Service Canada	Access Misuse Correction Delay Language Index Col/Ret/Dis	57 7 3 101 2 1 2 (173)	26 4 — 100 1 1 1 (133)	28 3 3 — 1 — 1 (36)	3 — — 1 — — — (4)
Employment and Immigration Canada	Access Delay Col/Ret/Dis	21 17 3 (41)	8 8 — (16)	13 9 3 (25)	— — —
Energy, Mines and Resources	Misuse	1 (1)	1 (1)	—	—
Finance	Access	1 (1)	—	1 (1)	—
Fisheries and Oceans	Delay	1 (1)	1 (1)	—	—
Health and Welfare Canada	Access Delay Correction	4 2 1 (7)	1 — — (1)	2 2 1 (5)	1 — — (1)
Indian and Northern Affairs	Access	2 (2)	—	2 (2)	—
Justice	Access Delay	6 1 (7)	2 — (2)	4 1 (5)	— —
Labour Canada	Access	1 (1)	—	1 (1)	—

Department	Complaint Type	Number (Total)	Justified (Total)	Dismissed (Total)	Abandoned (Total)
National Defence	Access	6	—	6	—
	Correction	1	—	1	—
	Delay	41 (48)	36 (36)	5 (12)	—
National Parole Board	Access	5	2	3	—
	Misuse	1	—	1	—
	Correction	1	—	1	—
	Delay	3 (10)	2 (4)	1 (6)	—
Privy Council Office	Access	1	1	—	—
	Delay	1 (2)	— (1)	1 (1)	—
Public Archives Canada	Access	3	—	3	—
	Correction	1 (4)	—	1 (4)	—
Public Service Commission	Access	11	6	5	—
	Misuse	1	—	1	—
	Correction	3	—	3	—
	Col/Ret/Dis	2 (17)	— (6)	2 (11)	—
RCMP	Access	30	4	26	—
	Misuse	2	2	—	—
	Correction	2	—	2	—
	Delay	5	—	4	1
	Col/Ret/Dis	1 (40)	— (6)	1 (33)	— (1)
Revenue Canada Customs and Excise	Access	1	1	—	—
	Misuse	1	—	1	—
	Col/Ret/Dis	1 (3)	— (1)	1 (2)	—
Revenue Canada Taxation	Access	5	1	4	—
	Delay	2 (7)	2 (3)	— (4)	—
Social Sciences and Humanities Research Council	Access	2 (2)	1 (1)	1 (1)	—
Solicitor General Canada	Access	3	12	2	—
	Delay	1 (4)	1 (2)	— (2)	—
Statistics Canada	Access	1 (1)	—	1 (1)	—
Supply and Services Canada	Access	1 (1)	1 (1)	—	—
Transport Canada	Access	2 (2)	—	1 (1)	1 (1)
Treasury Board	Access	2 (2)	1 (1)	1 (1)	—
Veterans Affairs Canada	Access	5	3	2	—
	Delay	1 (6)	— (3)	1 (3)	—
TOTAL		401	221	173	7

Delay

Departments have a 30-day period in which to respond to requests, and may have up to 30 days more if responding within that time "would unreasonably interfere with" the department's operations, or if more time is needed to consult with other departments. Translations must be completed in "such period of time as is reasonable".

Jurisdiction Lost

Following dismissal from his Vancouver harbour job, a man complained to the Commissioner about Canada Ports Corporation's delay in responding to his application for access to his file.

The investigation found that a 1982 amendment to the *National Harbours Board Act* (creating Canada Ports Corporation) enabled the government to establish various Canadian ports as independent corporations. Although the schedule listing all the government institutions subject to the new *Privacy Act* lists Canada Ports Corporation, not all the individual ports were included. The Privacy Commissioner was never advised.

Employees of the ports of St. John's, Halifax, Quebec, Montreal, Prince Rupert, and Vancouver had, in effect, lost their rights under the *Privacy Act*. As a result, the Commissioner had to dismiss the complaint.

The Commissioner discusses the need to advise him about legislative changes on page 16 of this report.

ORIGIN OF COMPLETED COMPLAINTS BY PROVINCE AND TERRITORY

Newfoundland	1
Prince Edward Island	3
Nova Scotia	13
New Brunswick	13
Quebec	117
National Capital Region Quebec	7
National Capital Region Ontario	28
Ontario	85
Manitoba	24
Saskatchewan	28
Alberta	18
British Columbia	60
Northwest Territories	1
Yukon	0
Outside Canada	3
Total	401

Correction

The Act provides that a complaint can be launched if a department refuses to place a note on a file to correct what an individual believes is erroneous. This right has encouraged applicants to try and have subjective judgments with which they do not agree removed from their record. While the *Privacy Act* does not allow applicants to change history, it does ensure that their version of a situation is on file and that all users of the information are told that the file has been annotated.

War Medical Can't Be Changed

When the Public Archives refused to change a man's Second World War medical assessment he complained to the Commissioner.

Archives had explained to the applicant that there was nothing on his medical files to indicate that the assessment was not an honest opinion of the examining doctor, and that it could not change history.

During the investigation the complainant said that some details were missing and a meticulous search on the Archives computer located more information on the applicant in collective medical records from a military district. These were sent to him.

Since the Commissioner could find no reason to call the medical examiner's opinion into question, he dismissed the complaint but advised the man that he could place his version of the facts on file.

Collection, Retention and Disposal

Applicants may complain to the Commissioner if government is collecting more personal information than it needs for a program or has no program at all; if the material is not being properly kept, kept too long, disposed of too soon or in a manner which does not maintain the privacy of the individual it concerns.

Can Investigate Leave Claims

A Revenue Canada (Customs) employee complained that the department collected personal information during an inquiry into allegations that he had submitted fraudulent sick leave claims while working elsewhere. He also complained that the department was releasing personal information about him during its interviews with his friends and associates, damaging his credibility and invading his privacy.

Revenue Canada cited the collective agreement with the complainant's occupational group, the department's policy on paid sick leave and a section of the *Financial Administration Act* (FAA) as the legal authority for its investigation.

The Commissioner did not agree that the collective agreement or internal departmental policy constituted legal authority. However, after investigation, he concluded that the FAA gives departments clear responsibility for personnel management.

"I accept that the very nature of management implies a right, and in fact a duty, to inquire into matters which touch upon the operations, resources, or activities within the management area. This right to conduct an investigation is therefore, in my view, integral to those in whom management responsibility has been vested", the Commissioner said.

He also referred the complainant to a Federal Court ruling that the power to conduct such investigations is incidental to the provisions of the FAA.

The Commissioner dismissed the allegation that the department had improperly revealed personal information. Since the investigation itself was proper and inquiries necessitated revealing the man's name and where he worked in order to obtain further information, the Commissioner concluded that the release was proper.

Collecting additional information about an employee from other sources does not breach the *Privacy Act* when collecting directly from the individual could result in inaccurate data or defeat the purpose of the collection.

Language

Applicants are entitled to receive material in the official language of their choice providing the material exists in that language. If it does not exist the head of the department must have it interpreted or translated for the applicant.

Must Offer to Translate

The office received only two language complaints during the year.

A former inmate received documents from Correctional Service Canada in French only rather than the requested English version. The department had advised the applicant that translation would take three to six months and that it was forwarding the French versions. It invited him to inform the department if he wanted translations. He complained to the Commissioner.

The Commissioner dismissed the complaint because the department had offered to translate.

The second complaint was similar, involving an inmate in the same penitentiary. However, this inmate was sent French documents without any offer to translate them.

The Commissioner found his complaint justified.

Index

Applicants may complain to the Privacy Commissioner if they believe that the Personal Information Index, the directory of the government's personal information banks, is in some way deficient. There was one such complaint this year.

Banks Not as Described

An inmate found several improperly described Correctional Service banks in the Index. A new list of personal information banks had been posted in the penitentiary and the department conceded that the Index listing was out-of-date.

The institution's reorganization of its banks, described in the complaint "Applicant Need Not Reapply" on page 30, prompted this complaint also.

The November 1985 edition of the Index correctly describes all the banks but the Commissioner considered the complaint justified.

On the Commissioner's Initiative

The *Privacy Act* gives the Commissioner the power either to initiate his own formal complaint, or to investigate the government's compliance with the fair information practices set out in the Act. The latter is a less formal procedure which does not put the Commissioner in the position of making accusations, but allows him more flexibility to inquire when circumstances cause concern.

Files blowin' in the wind

There were two occasions during the past year when the Commissioner exercised his discretion to investigate without a filed complaint.

The first was prompted by an article in the November 27, 1985, edition of the *Winnipeg Free Press* in which a reporter described bags of personal documents scattered in a snow-filled alley behind the local Employment and Immigration office.

The documents, found by two *Free Press* photographers, contained, among other things, personal data on individuals participating in the now-defunct Local Employment Assistance Program or being trained under the National Industrial Training Program. The Commissioner considered the matter serious enough to warrant an inquiry and sent two investigators to Winnipeg.

The investigators found that the files were dormant records which staff had cleared out of a file cabinet and put into cardboard boxes for disposal. The boxes were on (or beside) the waste-paper basket and, that night, the cleaner — believing the material was garbage — placed it all in garbage bags and put the bags in the alley. By next morning some of the bags had been broken, probably by a vehicle, and the contents were scattered.

An employee arriving that morning found and retrieved some of the docu-

ments and notified a supervisor. A lot of the material remained in the alley for several hours to be found by the newspeople.

The Commissioner concluded that the EIC office was negligent in handling the out-of-date files by not properly supervising or instructing the cleaner about disposal. In addition, the office was not limiting access to personal documents and even current material was not locked up.

The Commissioner recommended placing all the current personal files in locked containers. He also observed that had the supervisor taken immediate action to retrieve the blowing papers only the employees would have found the material and the damage would have been contained. He asked Employment and Immigration to make all personnel aware "without delay" about the provisions of the *Privacy Act* and of its impact on internal procedures and employees who handle clients' personal files.

The Unemployment Insurance survey

In the second case, a reporter called the Commissioner after being told that EIC engaged Peat Marwick & Associates to survey unemployment insurance recipients. Her source alleged that EIC had improperly released personal information to the company. The Commissioner sent investigators to both the department and the company to determine the facts.

During the investigation there were allegations in Parliament that the responsible Minister had ordered destroyed the files which related to the case. The investigation was not completed during this reporting year but the Commissioner will report to the Minister.

Inquiries

Many individuals continue to confuse the application process under the *Privacy Act*, viewing the Privacy Commissioner's Office as the place where all the files are kept. Much investigators' time is spent explaining how to apply for personal information and re-directing application forms for personal information to the department holding the files.

Staff handled 1086 inquiries during the year. Of these, 69 per cent wanted information about the Act and how to use it, or had misunderstood how to apply. Ten per cent either wanted to complain about an organization's use of social insurance numbers or sought clarification about the requirement to provide a SIN. About 15 per cent sought access to personal documents controlled by Crown corporations, private companies or provincial government agencies, none of which are covered by the Act.

The remaining inquiries concerned a range of subjects including wiretapping and electronic surveillance, credit reporting, and Statistics Canada surveys. There was contact from several federal public servants who were concerned about the implications of the government's new reporting requirements under the conflict-of-interest guidelines.

Twenty of 26 inquiries about credit reporting concerned a federal government directive that credit bureaus collecting overdue Canada Student Loans (under contract for Supply and Services Canada) may not reveal to client businesses that an individual had defaulted on a student loan. Letters had been sent by individual credit bureaus to local MPs who had subsequently asked the Privacy Commissioner for advice. The credit bureaus held that without this information their reports to creditors were inaccurate and incomplete.

The Commissioner advised the MPs that there was "no conflict between the *Privacy Act* and the current practice of assigning difficult or overdue accounts to a collection agency for action." The government has the right to employ collection agencies and it must give sufficient information to enable them to collect the debt.

However, the personal information that students supply to government to obtain a loan must be used only for that purpose. Applicants are not told that the information will be added to credit bureaus' information banks and to do so would be a "a violation of the *Privacy Act*", the Commissioner said.

While not unsympathetic to the credit bureaus' argument that complete files benefit both the borrower and creditor, the Commissioner determined that the Canada student loan program had special status.

"Against a credit bureau's desire to have complete and accurate credit histories, is the individual's right to privacy in dealings with the federal government. We would not expect Revenue Canada to reveal a taxpayer's indebtedness", he concluded.

The Commissioner's frequent public speaking engagements and media interviews often pique individuals' interest, leading them to phone or write for more information.

For example, a Toronto woman who had seen publicity about the Commissioner sought his help in finding her deceased father's place and date of birth. Statistics Canada had denied her request because the census records from 1881 to the present are confidential documents. The Commissioner was unable to help because, in the interest of collecting accurate data, an individual's responses to census questions receive absolute protection for 92 years, even though the person may be dead.

A man tracing his family history wanted the "Federal Department of Information" to help find his ancestors in the Netherlands. The Commissioner recommended books on the subject, enclosed a relevant magazine article, and referred the man to both the Public Archives and the Centraal Bureau Voor Genealogie in The Hague.

Notifying the Commissioner

The *Privacy Act* requires that government institutions notify the Privacy Commissioner when they intend to release personal information "in the public interest", or if they begin to use a class of personal information in a manner "consistent" with the purpose for which it was gathered but for a use not described in the Index.

In the Public Interest

Government institutions must notify the Privacy Commissioner when they intend to release personal information "for any purpose where, in the opinion of the head of the institution,

- (i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from disclosure, or
- (ii) disclosure would clearly benefit the individual to whom the information relates."

This advance notice gives the Commissioner an opportunity to advise the individual of the forthcoming release. If he considers the information improperly released, the Commissioner may initiate his own complaint.

Licensed pilots and magazine subscription list

In this example, Transport Canada notified the Privacy Commissioner that it proposed to release the names and addresses of federally-licensed Canadian pilots to the publisher of an aviation magazine. The department's rationale was that the magazine "makes a significant contribution by reinforcing the prominent features of safety and tech-

nical information" and "provides an independent non-government source and forum for the community".

The list had been released formerly under a contract between Transport Canada and the magazine but the contract was not renewed after a small number of pilots complained about the practice.

The Privacy Commissioner told the department that he could not reasonably notify some 90,000 pilots that their personal information was to be released. However, he pointed out that he would have to investigate any resulting complaints. The Commissioner suggested that the department give individuals an opportunity to block this type of release as licenses are issued or renewed.

Transport Canada changed its decision and will not now release the list to the magazine.

Ho Ho Ho

Just before Christmas Canada Post advised the Commissioner's Office that it proposed to release the name and address of an eight-year-old Chinese boy who had written to Santa Claus.

His letter, addressed to "Mr. Ho Ho Ho, Christmas Old Man, Canada North" was one of almost 38,500 which Canada Post received at postal code HOH OHO and which were answered by more than 6,000 volunteers under the Santa Letter Reply Program. The letter caught the eye of Santa's elves and its contents (but not the name) were released to the media.

Several newspaper readers, touched by the boy's letter, asked Canada Post for his name and address to send souvenirs and letters. The Commissioner, no Scrooge or Christmas Grinch, agreed that Ho Li Cheng of Canton, China, would clearly benefit. He did not advise Cheng that Santa would come to call.

The Commissioner received the following notifications during the past year.

Department	Released
Canada Post	— name and address of child who had written to Santa Claus at postal code HOH OHO to media and readers who wished to send souvenirs and letters. (see above)
Canadian Security Intelligence Service	— information on an individual requested by a film company (notification not required, as information was publicly available).
Correctional Service Canada	— personal information and parole status of two inmates to a judge who had sentenced them and was concerned about his safety. — <i>personal information of an inmate who had been corresponding with a female in China who was coming to Canada based on inmate's representations.</i> — family history and photograph of deceased inmate to law firm to handle estate.
Indian Affairs and Northern Development	— band lists to various provincial organizations to verify status of band members. — band lists to university providing health care, to avoid confusion in patients' files. — list of members of B.C. Indian bands to fisheries officials to confirm eligibility for food fishery privileges.
National Arts Centre	— personal information on employees to Ottawa Police after a break-in at the Arts Centre.
National Defence	— War Crimes Investigation Unit Report released to Deschenes Commission of Inquiry.
National Parole Board	— general information about parole status of inmate to media.

Public Archives	<ul style="list-style-type: none"> — medical documents concerning ex-serviceman required in an emergency by a doctor.
Secretary of State	<ul style="list-style-type: none"> — citizenship records of an individual requested by spouse. Children wished to become dual citizens. (No information was held by department on the individual concerned. Therefore, no notification had been required.) — date deceased spouse obtained Canadian citizenship to help survivor obtain veterans' benefits. — confirmation of Canadian citizenship of an individual required by Swedish government in a custody case. — last-known address, landing record, date and place of birth of man to Montreal police to locate next-of-kin.
Solicitor General	<ul style="list-style-type: none"> — RCMP report from investigation of a public official released in the public interest.
Statistics Canada	<ul style="list-style-type: none"> — records relating to deceased's place of birth required by an individual seeking American citizenship. — information about deceased man's place of birth to son to pursue application for Canadian citizenship.
Transport Canada	<ul style="list-style-type: none"> — names and addresses of federally-licensed Canadian pilots requested by publishing company. (see above)
Veterans Affairs	<ul style="list-style-type: none"> — medical information concerning father's hospitalization prior to death to daughter. — information on veterans or dependants searched by summer students to ascertain eligibility for benefits. — personal information on some veterans to Royal Canadian Legion doing a survey on single veterans housing. — list of Toronto area veterans to Toronto Transit Commission to allow veterans qualified for War Veterans Allowance reduced fare on transit system.

"Consistent Use"

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, as required by the Act. In fact, the Commissioner received only three such notices during the reporting year.

Once the Commissioner is notified the department is required to ensure that the new use is described in the next edition of the Index. If individuals find a government institution using information for a purpose not described in the Index they may complain to the Commissioner.

First Notice

In May 1985 Veterans Affairs Canada notified the Commissioner that the Index description of uses was incomplete for three of its banks. The department advised that personal information in Pensions and Compensation bank (VAC/P-PU-055), Pension Review Board Appeals bank (VAC-P-PU-080), and Legal Services for Pension Applicants (VAC/P-PU-090) is used occasionally to support other similar pension claims. The amended descriptions appear in the 1985 Index listings.

Second Notice

The Department of Indian Affairs and Northern Development (DIAND) advised that Employment and Immigration Canada (EIC) wanted a printed list of status natives and Indians by name and province, and a computer tape of the information in the printed list but including first and last names, date of birth and sex.

EIC wanted to determine whether the lists would help identify "status Indians (Canadian)" at Canadian border-crossing points. According to DIAND, often Indians refuse to carry the cards identifying them as status Indians, and lend the cards to others. The resulting confusion causes "numerous delays" at border crossings.

DIAND advised the Commissioner that it intended to enter into a written agreement with EIC "which would restrict the use of this personal information to the purposes stated by EIC and to prohibit further disclosure of this information without prior consent from our department".

The Commissioner said that the proposed disclosure was unrelated to the reason that DIAND collected the information and that EIC had no program which would allow it to have these data. Following discussions between DIAND and EIC, Indian Affairs declined to release the information, but offered to contact specific bands whose members EIC found were causing significant problems.

Third Notice

Employment and Immigration notified the Commissioner's office that to help claimants it occasionally released claim status and payment schedule information about unemployment insurance claimants to advocacy groups. The office asked EIC for further details and examples of this type of release and suggested a meeting to examine the issue. The Commissioner's Office is awaiting a response.

Compliance Branch

The Commissioner describes government institutions as the "front line in the battle for effective data protection". Departments are responsible for collecting, maintaining, using and destroying personal information in a manner consistent with the "fair information practices" set out in sections 4 to 8 of the *Privacy Act*. The Commissioner, as authorized by section 37, ensures that departments meet this standard by having his Compliance Branch conduct a type of information "audit".

The Commissioner reports his findings from each audit to the head of the department and includes any recommendations he considers appropriate.

In February 1986 the Commissioner obtained an internal auditing specialist to write and put in place a detailed auditing plan, procedures and reports. The resulting guide is available to all government privacy coordinators to help them measure their agencies' procedures against the Privacy Commissioner's standards.

Fisheries and Oceans Audit

Early in 1985-86 the Commissioner sent his findings from the Compliance Branch's first detailed audit to the Deputy Minister of Fisheries and Oceans Canada.

The investigation had included an examination of files and records and a review of forms and procedures in St. John's, Winnipeg, Vancouver, and the department's head office in Ottawa. Recommendations the Commissioner made were that Fisheries and Oceans

- delete the listing for bank FO-P10, Fisheries Experimental Data system, from the Index and dispose of the personal information because the

bank was to have served as a prototype data base for a program which had been discontinued,

- make clear in its description of bank FO-P30, Commercial Fishermen's Licensing and Vessel Registration, that native food fishing and recreational fishing licenses are also kept in the bank,
- remove the Index listings for banks FO-P80, Loans Program; FO-P90, Fisheries and Oceans Science Human Resources, and FO-P120, Fish Chilling Assistance Records, because P80 and P120 contain business, not personal, records, and P90 is empty as the program has been discontinued and the files destroyed,
- amalgamate banks FO-P70, Fishing Vessel Subsidy Program, and FO-P130, Fishing Vessel Assistance Program, because the information is virtually the same, with greater detail kept in regional office files,
- establish a retention schedule for all banks,
- adopt a standard departmental procedure for using SIN as identification.

Investigators also audited the Canadian Saffish Corporation and the Freshwater Fish Marketing Corporation. The Commissioner recommended that both agencies list their limited personal information holdings under their own names in the Index, rather than combined with Fisheries and Oceans, and that the Freshwater Fish Marketing Corporation also describe in the Index its files on the 3,500 fishermen from whom it purchases fish.

Employment and Immigration Canada's closed banks

The branch audited Employment and Immigration Canada's two closed banks, EIC-P430, Immigration Security and Intelligence Data Bank, and EIC-P440, Enforcement Information Index System, in May and June 1985.

Section 18 of the *Privacy Act* specifies that the files in these banks must contain predominantly "personal" information that, if disclosed, could harm Canada's, or its allies' international affairs or defence and the efforts to detect, prevent or suppress hostile or subversive activities. Files may also contain law enforcement and security investigation material.

Investigators found no evidence that EIC had examined the files individually before applying to have the bank closed. Some of the files in P430 contained little or no personal information, a number of non-personal policy and administration files were considered to be part of the bank, and many files were found to be inactive and out-of-date, despite the presence of a departmental disposal schedule.

The Commissioner concluded that the two banks had been improperly closed and that "any complaints received by my office after this date (October 21, 1985) will be treated by me as complaints against an open personal information bank and my investigation of those banks will be carried out in the manner appropriate for open information banks".

"Pocket audits"

The branch continued its so-called "pocket-audits" to check inconsistencies in Index descriptions and to meet the staff of small agencies not listing personal information, to verify that no personal files exist.

During the reporting year the Compliance Branch met with staffs at

- *Canadian International Development Agency (to correct an improper bank code);
- *Health and Welfare Canada (missing banks transferred to Transport Canada);
- *Labour Canada (banks transferred to Canadian Human Rights Commission, another bank missing in error, a third destroyed to comply with destruction schedule);
- *National Capital Commission (two banks discontinued as out-of-date, and containing non-personal information);
- *National Defence (five banks discontinued including three which duplicated information in employee banks, one that contained statistics only, and a fifth that was lost through oversight);
- *National Research Council (discontinued bank files integrated in two other banks);
- *Public Service Staff Relations Board (discontinued bank files duplicated elsewhere or contained no personal information);
- *Canada Post Corporation (two discontinued bank files integrated into employee banks); and
- *External Affairs (nine banks dropped including one combined with another, integration of files from five others into three existing banks, and three which contained no personal information).

Section 8(2)(e) Investigations

The *Privacy Act* was amended by the act creating the Canadian Security Intelligence Service to remove the requirement that an individual's file show when an investigative body had used the file. This record is now kept separately.

Removal of this requirement means that the Privacy Commissioner is the only outsider who may check investigative bodies' uses of personal information. In 1985 the Commissioner's investigators began a systematic examination of these requests and of the agencies' internal handling procedures.

By the end of the reporting year, investigators had examined the records of 45 government institutions. Of these, 11 had received the following requests:

	Requests	Disclosures
Agriculture	2	2
Bank of Canada	33	30
Canada Mortgage and Housing Corporation	46	45
Canada Council	1	1
Canada Post	83	69
Canadian Cultural Property Export Review Board	1	0
Consumer and Corporate Affairs	1	0
Communications	1	1
Energy, Mines and Resources	34	19
Indian and Northern Affairs	6	2
Secretary of State	437	164
(273 were refused either because no record was found or there was insufficient information given to search. Most requests were from Deschenes Commission or RCMP.)		
TOTAL	645	333

The remaining agencies had received no requests but the investigation served to remind each one about the *Privacy Act* and its specific requirements on handling investigative bodies' requests.

The remaining agencies investigated were:

Advisory Council on the Status of Women, Atomic Energy Control Board, Canada Labour Relations Board, Canada Ports Corporation, Canadian Aviation Safety Board, Canadian Commercial Corporation, Canadian Dairy Commission, Canadian Human Rights Commission, Canadian Import Tribunal, Canadian Institute for International Peace and Security, Canadian Patents and Development Limited, Farm Credit Corporation, Finance Canada, International Development Research Centre, Investment Canada, Law Reform Commission of Canada, Medical Research Council, National Arts Centre, National Capital Commission, National Energy Board, National Farm Products Marketing Council, National Library of Canada, National Museums of Canada, National Parole Board, National Research Council, Natural Sciences and Engineering Research Council of Canada, Pension Appeals Board, Public Service Staff Relations Board, Restrictive Trade Practices Commission, Science Council of Canada, Social Sciences and Humanities Research Council, Standards Council of Canada.

The Privacy Act in Court

The *Privacy Act* gives dissatisfied complainants the right to ask for a Federal Court review if they were denied personal information, providing that the Privacy Commissioner has investigated and reported on the complaints. Information about this right is included in the Commissioner's report to complainants. If the Commissioner is dissatisfied with the institution's handling of the complaint, he may — with the complainant's consent — take the case to Court himself.

This right to a Court review applies only to denial of personal information. It does not extend to complaints of delay, misuse, correction, inappropriate collection, retention or disposal, the language of the documents, or the adequacy of the Personal Information Index. However, the Commissioner may ask the Court to review any file he believes is improperly contained in a closed bank.

A complainant has 45 days from the time the Commissioner's report is received to apply for a Court review. The Court may, however, exercise its discretion and allow more time. The Court reviews the government's denial of the information from the initial application. The Court does not review the Privacy Commissioner's investigation.

Between April 1, 1985, and March 31, 1986, there were 12 applications for Court review, of which two have been withdrawn.

The following summarizes the cases currently under Court review.

Ternette vs Solicitor General of Canada

Mr. Ternette's application to see personal information in RCMP Bank P-130 (Security Service Records) was denied because the bank was closed by the Governor-in-Council. Ternette complained to the Privacy Commissioner who examined the bank but could neither confirm nor deny that it contained the information. However, he assured Ternette that he had not been denied any rights under the *Privacy Act*.

Mr. Ternette exercised his right to apply to the Federal Court for a review. The Department of Justice argued that the review envisaged by the *Privacy Act* confined the Court to pass judgment only on whether the bank in question had been closed legally. The Court supported the applicant in concluding that it was empowered also to examine a file to determine whether it was properly contained in a closed bank. The Solicitor General appealed. The Minister of Justice withdrew the appeal, agreeing that a judicial review would be meaningless if the Court could not examine records in exempt banks.

In September 1985 the Solicitor General conceded to Ternette's counsel that there was no evidence that the individual files in RCMP Bank P130 had been examined to ensure that they belonged in the closed bank. Therefore, the bank was improperly closed.

Since the bank is now to be treated as open, the Commissioner decided to investigate the complaint.

There is no indication when the case will return to Court to be argued on its merit.

Barry Yanaky vs Canada Employment and Immigration Commission (CEIC)

The Canada Employment and Immigration Commission denied Mr. Yanaky four documents in his file on the ground that they were covered by solicitor-client privilege. In meetings with Mr. Justice Jerome, CEIC agreed that three of the disputed documents were not covered and released them. The parties agreed that the fourth was outside the scope of the original request and was privileged. Mr. Yanaky withdrew his action.

Suresh Kothari vs Energy, Mines and Resources

Mr. Kothari applied to Energy, Mines and Resources for information about an award he maintains he received for energy research. The department was unable to locate any information and Mr. Kothari applied for a Court review.

Paul Copeland vs Solicitor General of Canada

Mr. Copeland, a Toronto lawyer, began action in the Federal Court when he was denied the opportunity to see whatever information the RCMP had about him in its files. This request was denied on the grounds that the information was exempted under section 22 of the *Privacy Act* which restricts the release of data which could be injurious to a lawful investigation or a Canadian law. He complained to the Privacy Commissioner who found the exemption had been properly applied.

Neil A. Davidson vs Solicitor General of Canada

Mr. Davidson applied for personal information from an RCMP investigation conducted for the B.C. Attorney General between June 1980 and April 1981 under the terms of a policing agreement as set out in section 20 of the *Royal Canadian Mounted Police Act*. Mr. Davidson obtained some of the material but was denied other parts when the department invoked section 22 of the *Privacy Act*.

Mr. Davidson complained to the Privacy Commissioner who found that the exemptions had been applied properly and advised the complainant of his right to apply for a Federal Court review. Mr. Davidson so applied.

Patricia MacCulloch vs Minister of National Revenue and the Solicitor General

Ms. MacCulloch applied to see personal information in RCMP bank P-20, Operational Case Records. Revenue Canada (Customs and Excise), which received the original request, redirected it to the RCMP and so advised Ms. MacCulloch. When the RCMP told her it required a 30-day extension to consult with other departments, Ms. MacCulloch complained to the Commissioner. She subsequently complained when the RCMP withheld some of the documents because they were obtained in confidence from another government; were prepared by the RCMP while acting as provincial police; their disclosure could injure law enforcement or a lawful investigation; and because documents contained personal information about other individuals.

The investigator persuaded the RCMP to release 21 more complete pages and portions of two more.

The Commissioner concluded that the delay complaint was not justified since the consultation with other departments was reasonable. However, he found justified the complaint that access was denied, since some of the material had been improperly withheld. The Commissioner advised Ms. MacCulloch of her right to ask the Court to review the denial of the remaining documents. She did so in July 1985.

Jack Gold vs National Revenue (Taxation)

Mr. Gold applied for personal information in a number of banks after he failed to meet the "Secret" security requirement of a position. He received more than 100 documents from his file in Revenue Canada (Taxation)'s bank RC-T-S-8, but about 40 pages were withheld. Following investigation, the Commissioner concluded that all but one document had been properly withheld. Five more pages of this document were released with exemptions applied. Several other pages numbered in the file and not released were found not to contain personal information about any individual.

Mr. Gold was advised of the Commissioner's conclusions and of his right to ask for a Court review and he appealed.

James Buchan vs the Public Service Commission and Fisheries and Oceans

Mr. Buchan was denied documents, or portions of documents, concerning his dismissal because the deleted information either concerned other individuals or was the subject of a solicitor-client privilege. Investigation led to the release

of more documents. Mr. Buchan exercised his right of a Court review but his application was later withdrawn.

Barry Kohn vs Solicitor General

Mr. Kohn applied for personal information in three closed Solicitor General banks — SGC-P80, P110 and P120, Protection of Privacy (as defined in section 178.1 and 178.23 Inclusive of the Criminal Code), Police and Law Enforcement — RCMP Operational Records, and Commissions of Inquiry banks respectively.

The Commissioner advised Mr. Kohn that he could neither confirm nor deny the existence of a record about Mr. Kohn in these banks, but that the complainant had a right to ask the Court to review the denial of access. Mr. Kohn applied in July 1985 for such a review.

Shahnaz Dadvand vs Department of Justice

Mrs. Dadvand applied to see her security clearance file after she was turned down by the Department of Justice for a position which required a security clearance. She complained to the Privacy Commissioner when some of the material was exempted because it concerned other individuals and it could injure the conduct of international affairs or defence.

During the investigation additional material was released but the Commissioner concluded that the balance of the material was properly withheld. Mrs. Dadvand was advised of his conclusions and of her right to a Court review. She applied in February 1986.

Corporate Management

Corporate Management provides both the Information and Privacy Commissioners with financial, personnel, administrative and public affairs services.

Personnel

There were 51 person years used against the 57 allocated in the 1985-86 main estimates. Two senior employees retired under the Early Retirement Incentive Program and 11 staffing activities were conducted in 1985-86.

Finance

The 1985/86 budget for the entire organization was \$3,363,000, which was reduced by \$25,200 as a result of government restraint programs. Included in the budget was \$1,128,845 for Corporate Management, \$1,128,845 for the Privacy Commissioner, and \$913,820 for the Information Commissioner. However, an additional \$104,106 was spent by the Information Commissioner to cover salaries of the Assistant Information Commissioners and their support staff and the preparation of the Special Annual Report.

Public Affairs

The unit provided writing/editing, media, publication production and distribution services for the two Commissioners. During the year the unit produced and distributed two annual reports, a special report, and material for the Commissioners' submissions to the Legal and Justice Affairs Committee which will be reviewing the administration of the *Privacy Act* and the *Access to Information Act*. Public Affairs also distributed copies of information material to approximately 7,000 locations where individuals can consult the index and register and pick up forms to apply under both Acts.

Office Automation

The office now has 19 personal computers providing statistics, record keeping, data manipulation, word processing and access to outside legal and research data banks. Special networking features have been built in to allow managers access to facilitate complaint investigations.

Expenditures

The following are the Offices' expenditures for the period April 1, 1985, to March 31, 1986.

	Information	Privacy	Administration	Total
Salaries	\$ 715,153	\$844,136	\$ 650,087	\$ 2,209,376
Employee benefit plan contributions	95,820	133,323	95,845	324,988
Transportation and communications	26,557	40,253	79,942	146,752
Information	75,179	36,439	8,646	120,264
Professional and special services	104,951	32,964	127,696	265,611
Rentals	—	—	11,567	11,567
Purchased repair and maintenance	—	—	4,633	4,633
Utilities, material and supplies	—	—	33,586	33,586
Construction and equipment acquisition	—	—	65,001	65,001
All other	266	695	185	1,146
Total	\$1,017,926	\$1,087,810	\$1,077,188	\$3,182,924

The Privacy Act and You

What information does the government have about me?

Without knowing your personal circumstances we can't tell exactly what information the federal government has about you. No single file in Ottawa contains everything about you; there are a number of files depending on what contacts you have had with the government.

Some information on most Canadian residents will turn up as a result of at least one of the following:

- Income tax files
- UIC contributions
- CPP deductions or benefits
- Student loan applications
- Social insurance number applications
- Passport applications
- Old age security benefits
- Customs declarations

Perhaps your name appears in the files of those who have applied for a home insulation grant or who have auditioned at the National Arts Centre.

If you have ever worked for the federal government, your department and the Public Service Commission may still have your personnel file, a record of any job competitions you entered, your annual performance appraisal, any applications for parking spaces and information about your pay and benefits. The Personal Information Index will indicate how long these files are kept.

Where do I find The Personal Information Index?

Copies of the Index are available at public and federal departmental libraries, and some rural post offices, along with the forms needed to apply for access. The Personal Information

Index explains what each institution does, how to apply for access, and lists the files each government institution keeps.

One section lists files concerning the public; another, federal employees. If you believe there is information about you but cannot find an appropriate bank listed in the Index, the Act still ensures you access if you can provide the department with sufficient specific information for it to be found by staff.

How do I see personal information about me?

From the Index, determine which banks could contain information about you. Complete a Personal Information Request Form (see Appendix II) for each bank you wish to examine and send it to the coordinator listed under each institution. There is no charge. The department must respond within 30 days of receiving your request but may ask for a 30-day extension.

Are there information banks I can't see?

Yes. However, following a court challenge to one of the closed banks the status of the original 20 is in question. Many are now being treated as open, although much of the material may still be exempt under other provisions of the *Privacy Act*.

Individuals who are interested in personal files which may be in an exempt bank should apply to the department in question and await its response.

The following departments still consider these banks closed:

Privy Council Office	PCO/P-PU-005, Security and Intelligence Information Files
Canadian Security Intelligence Service	SIS/P-PU-010, Canadian Security Intelligence Service Records
National Defence	DND/P-PU-040 CSE, Security and Intelligence Investigation Files
RCMP	CMP/P-PU-055, Protection of Personnel and Government Property
Solicitor General	SGC/P-PU-025, Security Policy and Operations Records SGC/P-PU-055, Commissions of Inquiry SGC/P-PU-030, Police and Law Enforcement Records Relating to the Security and Safety of Persons and Property in Canada SGC/P-PU-035, Protection of Privacy (wire-tapping — Criminal Code)

Does this mean I may see everything else?

No, not quite. Some material in other banks may be excluded because the personal information:

- was received in confidence from a municipal, provincial or national government;
- could injure Canada's defence or conduct of its affairs;
- was collected by an investigative body during the investigation of a crime;
- could threaten an individual's safety;
- is the subject of a solicitor-client privilege;
- relates to an individual's mental or physical health if the knowledge could be contrary to his/her best interest (the information may be released to the person's doctor);
- concerns security clearances (although this exemption is not mandatory);
- is a confidence of the Queen's Privy Council;
- was obtained by Correctional Service Canada or the National Parole Board while the person making the request was under sentence for an offence against any act of Parliament, if the disclosure "could reasonably be expected to"
 - lead to a serious disruption of the person's institutional, parole or mandatory supervision program, or
 - reveal information about the person obtained originally on a promise of confidentiality, either express or implied.

Can the government disclose my personal information to someone else?

The act generally requires a government institution to obtain your permission before it releases personal information. However, there are several circumstances when your consent is not required. Personal information may be released:

- to comply with another act of Parliament;
- to comply with a warrant or subpoena;
- for the Attorney General of Canada to use in a legal proceeding;
- for the use of an investigative body (such as the RCMP or Military Police) when enforcing a law;
- to another government in order to administer or enforce a law when there is an arrangement between the two governments;
- to a member of Parliament who is trying to help you (with your consent);
- to carry out an official audit;
- to the Public Archives for storage;
- for statistical or research purposes providing that the researcher agrees in writing not to disclose the information;
- to help native people prepare claims;
- to collect a debt to the Crown or to pay an individual a debt owed by the Crown;
- to further the public interest;
- or to benefit you. (In these last two cases the institution must notify the Privacy Commissioner who may in turn notify you.)

Which government departments are covered by the Privacy Act?

Most of the federal departments, agencies and commissions are covered by the Act but not those Crown corpora-

tions which compete with the private sector as do CBC, Air Canada and CN.

A complete list of the institutions covered is in Appendix III.

What can I do if I think the information is incorrect?

Write to the privacy co-ordinator at the institution holding the information, explaining the error and setting out the corrections you would like made. Generally there is little difficulty correcting factual errors. If you are refused, you have the right to attach a notation to the information showing the correction you wanted made.

If you are denied these rights you may complain to the Privacy Commissioner.

What should I do if I have been refused access?

If it is not clear to you why the institution has refused your request, the first step is to ask the appropriate privacy co-ordinator to explain the problem to you. Many departments and agencies will accept collect calls. Perhaps there has been a misunderstanding.

If, after talking to the co-ordinator, you still think you have been wrongly denied the information, call or write to the Privacy Commissioner's office.

The Privacy Commissioner of
Canada
112 Kent Street, 14th Floor
Ottawa, Ontario
K1A 1H3

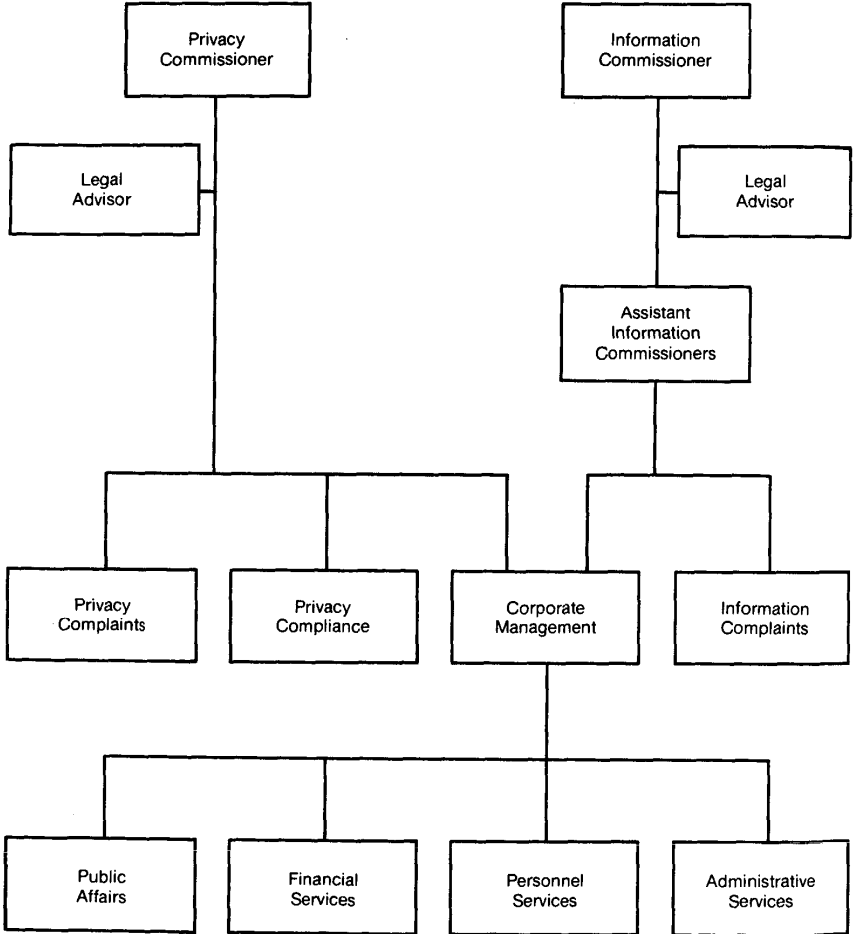
(613) 995-2410. 1-800-267-0441

The switchboard is open from 7:30 a.m. to 6:00 p.m., Ottawa time.

Appendix I



Offices of the
Information and Privacy
Commissioners of Canada



Appendix II



Government of Canada / Gouvernement du Canada

Privacy Act

Personal Information Request Form

For official use only

Individuals are required to use this form to request access to personal information about themselves under the Privacy Act.

STEP 1: Decide whether or not you wish to submit a request under the Privacy Act. You may decide to request the information informally, without using the procedures required by the Act, through the local office of the appropriate government institution or through the Privacy Co-ordinator listed in the Index of Personal Information. Copies of the Index are available in public libraries, post offices in rural areas and government information offices.

STEP 2: Consult the Index of Personal Information. If you have decided to exercise your rights of access under the Privacy Act, review the descriptions of personal information for institutions which are most likely to have the information you are seeking. Decide on the personal information bank or class of personal information likely to contain the information.

STEP 3: Complete this personal information request form. Indicate the personal information bank or class of personal information to which you are requesting access, and include any additional information indicated in the bank description to locate the information you are seeking, or to verify

your own identity. Indicate whether you wish to receive copies of the information, examine the original in a government office, or if you are requesting other arrangements for access. There is no application fee for making a request under the Privacy Act.

STEP 4: Send the request to the person identified in the Index as the appropriate officer responsible for the particular personal information bank or class.

STEP 5: Review the information you received in response to your request. Decide if you wish to make further requests under the Privacy Act. You may wish to exercise your rights to request corrections or to require that notations be attached to the information when corrections are not made. You may also decide to complain to the Privacy Commissioner when you believe that you have been denied any of your rights under the Act.

Federal Government Institution

Registration Number and Personal Information Bank or Class of Personal Information

I wish to examine the information As it is All in English All in French

Provide other details specified in the Index to aid in locating particular information or to verify identity of applicant. (Present or former members of the Canadian Armed Forces requesting military records must provide additional information as specified in the D.N.D. section of the Index.)

Method of access preferred

Receive copies of the original Examine original in government office Other method (please specify)

Identification of applicant

Name (or previous name)

Social Insurance No. (or other identifying no. if applicable)

Street address, apartment

City or town

Province, territory, or other

Postal Code

Telephone number(s)

If this request follows a previous enquiry, quote reference number ►

I have a right of access to personal information about myself under the Privacy Act by virtue of my status as a Canadian citizen, a permanent resident within the meaning of the Immigration Act, 1976, or by Order of the Governor in Council pursuant to subsection 12(3) of the Privacy Act.

Signature

Date

Canada

Français au verso

TBC 350-58 (Rev. 85/8)

Appendix III

Government Institutions Covered by the Act

Advisory Council on the Status of Women	Canadian Commercial Corporation
Agricultural Products Board	Canadian Cultural Property Export Review Board
Agricultural Stabilization Board	Canadian Dairy Commission
Agriculture Canada	Canadian Film Development Corporation
Atlantic Development Council	Canadian Government Specifications Board
Atlantic Pilotage Authority	Canadian Grain Commission
Atomic Energy Control Board	Canadian Human Rights Commission
Bank of Canada	Canadian Import Tribunal
Bilingual Districts Advisory Board	Canadian Institute for International Peace and Security
Board of Trustees of the Queen Elizabeth II Canadian Fund to Aid in Research on the Diseases of Children	Canadian International Development Agency
Bureau of Pension Advocates	Canadian Livestock Feed Board
Canada Council	Canadian Patents and Development Limited
Canada Deposit Insurance Corporation	Canadian Penitentiary Service
Canada Employment and Immigration Commission	Canadian Pension Commission
Canada Labour Relations Board	Canadian Radio-television and Telecommunications Commission
Canada Mortgage and Housing Corporation	Canadian Saltfish Corporation
Canada Ports Corporation	Canadian Security Intelligence Service
Canada Post Corporation	Canadian Transport Commission
Canadian Aviation Safety Board	Canadian Unity Information Office
Canadian Centre for Occupational Health and Safety	The Canadian Wheat Board
	Communications, Department of

Consumer and Corporate Affairs Canada	Historic Sites and Monuments Board of Canada
Defence Construction (1951) Limited	Immigration Appeal Board
The Director of Soldier Settlement	Indian and Northern Affairs Canada
The Director, The Veterans' Land Act	Insurance, Department of
Economic Council of Canada	International Development Research Centre
Employment and Immigration Canada	Investment Canada (formerly Foreign Investment Review Agency)
Energy, Mines and Resources Canada	Jacques Cartier and Champlain Bridges Incorporated
Energy Supplies Allocation Board	Justice Canada
Environment Canada	Labour Canada
Export Development Corporation	Laurentian Pilotage Authority
External Affairs Canada	Law Reform Commission of Canada
Farm Credit Corporation	Medical Research Council
Federal Business Development Bank	Merchant Seamen Compensation Board
Federal Mortgage Exchange Corporation	Metric Commission
Federal-Provincial Relations Office	National Arts Centre Corporation
Finance, Department of	The National Battlefields Commission
Fisheries and Oceans Canada	National Capital Commission
Fisheries Prices Support Board	National Defence
The Fisheries Research Board of Canada	National Design Council
Freshwater Fish Marketing Corporation	National Energy Board
Grain Transportation Agency Administrator	National Farm Products Marketing Council
Great Lakes Pilotage Authority, Ltd.	National Film Board
Health and Welfare Canada	

National Library	Petroleum Monitoring Agency
National Museums of Canada	Prairie Farm Assistance Administration
National Parole Board	Prairie Farm Rehabilitation Administration
National Parole Service	Privy Council Office
National Research Council of Canada	Public Archives
Natural Sciences and Engineering Research Council	Public Service Commission
Northern Canada Power Commission	Public Service Staff Relations Board
Northern Pipeline Agency	Public Works Canada
Northwest Territories Water Board	Public Works Land Company Limited
Office of the Auditor General	Regional Development Incentives Board
Office of the Chief Electoral Officer	Regional Industrial Expansion
Office of the Commissioner of Official Languages	Restrictive Trade Practices Commission
Office of the Comptroller General	Revenue Canada
Office of the Coordinator, Status of Women	Royal Canadian Mint
Office of the Correctional Investigator	Royal Canadian Mounted Police
Office of the Custodian of Enemy Property	The St. Lawrence Seaway Authority
Office of the Inspector General of the Canadian Security Intelligence Service	Secretary of State
Pacific Pilotage Authority	Science and Technology Canada
Pension Appeals Board	Science Council of Canada
Pension Review Board	The Seaway International Bridge Corporation, Ltd.
Petroleum Compensation Board	Security Intelligence Review Committee
	Social Development, Ministry of State for
	Social Sciences and Humanities Research Council

Solicitor General Canada
Standards Council of Canada
Statistics Canada
Statute Revision Commission
Supply and Services Canada
Tariff Board
Tax Review Board
Textile and Clothing Board
Transport Canada
Treasury Board Secretariat
Veterans' Affairs Canada
War Veterans Allowance Board
Yukon Territory Water Board