



Annual Report
Privacy Commissioner
1984-85

**Annual Report
Privacy Commissioner
1984-85**



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

(613) 995-2410 — Collect calls are accepted and the switchboard is open from 7:30 a.m.
to 6:00 p.m., Ottawa time.

© Minister of Supply and Services Canada 1985

Cat. No. IP 30-1/1985

ISBN 0-662-53847-1

"The purpose of this act is to extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to such information."

Section 2,
Privacy Act
effective July 1, 1983

The Honourable Guy Charbonneau
The Speaker
The Senate
Ottawa

June 28, 1985

Dear Mr. Charbonneau:

I have the honour to submit to Parliament my annual report. This report covers the period from April 1, 1984, until March 31, 1985.

Yours sincerely,



John W. Grace
Privacy Commissioner


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

June 28, 1985

Dear Mr. Bosley:

I have the honour to submit to Parliament my annual report. This report covers the period from April 1, 1984, until March 31, 1985.

Yours sincerely,



John W. Grace
Privacy Commissioner

Contents

Mandate	1
The New Challenges	2
Fewer Complaints — Better Rights	5
Some Observations — And a Problem	8
Access and the Bureaucrats	10
TBDF — And Closer to Home	11
Compliance — The Commissioner as Auditor	13
Issues of Special Interest	14
Of Special Interest — Complaints	19
Spreading the Gospel	24
Complaints Investigations	25
Access	26
Delays	32
Correction or Notation	35
Misuse	36
Index	37
Without Complaint	38
Inquiries	39
Notifying the Commissioner	40
Compliance Branch	43
The Privacy Act in Court	45
Corporate Management Branch	48
The Privacy Act and You	50
Appendices	
I Organization Chart	53
II Information Request Form	54
III Government Institutions Covered by the Act	55

Mandate

The *Privacy Act*, which became effective July 1, 1983, has three basic objectives: it 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 all files (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.

The New Challenges

"The information revolution means that I may find out everything about anything. But it also means I may learn more about you than you want me to know."

David L. Bazelon, *"The Changing Communications Landscape: Learning from the Past"*

This second report of the Privacy Commissioner, under the authority of the *Privacy Act*, is made to a new Parliament. For the first time, it covers a full 12-month period. Last year's annual report, submitted June 30, 1984, gave the previous Parliament an accounting for only nine months, from implementation of the *Privacy Act*, July 1, 1984, to March 31, 1984, the end of the government year.

Each reporting process, like implementation of the *Privacy Act* itself, has a sense of discovery. No routine has set in; the challenge of exploring a territory still largely unknown, remains daunting.

And so should it be — no matter how many annual reports and how many Parliaments. Privacy protectors cannot be staled by custom or allowed to be complacent. The challenges to privacy are new, urgent, various and ingenious, brought about by technology that never sleeps and is rarely denied.

The *Privacy Act* is the federal government's code of data protection principles. It tells the collectors and holders of personal information that their duties go beyond simply building or managing bigger, faster systems and linking up ever more terminals to ever larger data bases. The Act holds managers accountable for the manner in which they collect and use personal information and can even challenge the right to collect such information in the first place.

For more than a century Canada got along without specific legislation covering the way in which the federal government handled personal information files. Few persons felt uncomfortable by the absence of such legislation.

Yet, if the *Privacy Act* were to disappear, even those who are unaware of the protection which the legislation affords (and too many are) would be newly exposed and threatened.

There is a widely-felt need to protect individuals from the assaults on privacy which are possible by new technologies of surveillance and the miracle of computer-harnessed micro-electronics.

Perhaps the fear has been best expressed by Arthur Miller in a statement to a sub-committee of the U.S. Congress, and quoted recently by Arthur J. Cordell in his study for the Science Council of Canada: "The computer, with its insatiable appetite for information, its image of infallibility, its inability to forget anything that has been put into it, may become the heart of a surveillance system that will turn society into a transparent world in which our home, our finances, our associations, our mental and physical condition are laid bare to the most casual observer."

In short, personal privacy could be the victim of efficiency.

In the past, the expense, the drudgery and the sheer physical impossibility of mining, systematically and exhaustively, personal information from vast holdings of manual records provided built-in privacy protectors. The wizardry of the computer and electronic data processing have removed that protection.

The modern state is the greatest custodian of personal information of any institution in human history. Now there is the potential of an ominous shift in the delicate balance of power between the individual and the state; a shift to the side of the custodians of these great reservoirs of instantly-retrievable, personal information.

Information gives power, and power is usually exercised; thus the qualitative change which the unchecked computer could impose on society. And a computer not only never forgets, it never forgives.

The real nightmare of Big Brother, even in this - let us be grateful - unOrwellian year, is one which George Orwell could not have foretold. It is not the unblinking eye of surveillance, though, of course, this is with us; it is the possibility of becoming a monitored society through the invasive, indiscriminate use of the computer in gathering, storing and comparing the personal information of each individual.

Unwanted and unauthorized "profiles" can be drawn up on the basis of a person's buying, travelling or television watching habits: no laws prevent this in the private sector as the *Privacy Act* does in the federal domain, impeding government from compiling profiles based on citizens' manifold dealings with the state. Such profiles could show not only what an individual has done but what the individual may be expected to do. The prospect is chilling, both for the threat posed to personal freedom, and ultimately, to democracy itself. It is nothing less than the prospect which Kafka feared: a society in which everyone is watched because everyone is suspect.

The *Privacy Act* and data protection principles are not all that stand between us and Orwellian and Kafkian visions. Ours is not such a fragile democracy that it is about to be crushed easily by the wonders of the

information society. Privacy of some kind will endure; but it needs help if it is not to be unacceptably limited.

How a society values the privacy of its members is a measure of that society's commitment to human — and humane — values. If privacy is a luxury, dispensed with lightly in favor of some momentarily more attractive purpose, the likelihood is that other rights or privileges will begin to be eroded.

The price Canadians could be paying for the efficiency of data banks is a total loss of control over who knows what about that part of their lives which once was considered to be personal and confidential. According to Dr. Cordell, a credit bureau association exchanges credit information with 3,000 businesses in Montreal alone. Thus, he points out, at least 3,000 persons in Montreal "have at their command detailed information on the financial affairs of millions of other people."

The same writer quotes a social worker who had requested information from a patient's hospital records: "I needed maybe one little piece of paper. Instead, I was sent the entire medical and social services record, including notes of anyone who had treated this person. Much of the material was of a highly personal nature and had nothing to do with what I needed . . .".

Because the computer and huge data bases can provide information easily, we should not accept sloppy or non-existent privacy protection. To the contrary, the sudden availability of so much personal information should be the stimulus for rigorous data protection codes.

Privacy protection begins with the conviction that (1) informational self-determination is essential to human dignity and (2) that a few common-sense principles and ordinary prudence can significantly diminish the dangers.

For example, the technique variously called computer-matching, cross-matching or computer-linkage is a far-reaching, insidious threat to the way our society thinks and works. This system involves the comparison of separate and unrelated records, making it possible to screen, almost instantly, vast and disparate sets of personal information in search of similarities or differences.

The Privacy Commissioner must challenge computer-matching as a tool even to achieve desirable goals. First, it means using information collected for two different purposes for yet another purpose, and that is a violation of a basic principle of fair information practices. Individuals have a right to know that the information which they gave to government will be used only for the purpose for which it was collected.

Matching operations of the kind conducted regularly by Revenue Canada and Employment and Immigration, for example, with these departments' own data and for their own mandated purposes are not in violation of the *Privacy Act*. But matching information collected by different institutions for different purposes would be against both the letter and the spirit of the privacy protection legislation.

This is not merely a doctrinaire admonition of a privacy advocate. A recent report of the U.S. General Accounting Office warned that computer matching's "potential for saving public money is rivaled only by its potential for infringing on personal privacy". When accountants and auditors speak like this, a privacy commissioner need not fear that he may be crying wolf.

Another reason why computer-matching is wrong is more subtle, yet more dangerous for that. The technique can turn the presumption of innocence into a presumption

of guilt. A computer match begins with the assumption that everyone stands a chance of being found guilty unless cleared by a computer.

A computer match is instigated not because a particular person is suspected of fraud - as in a traditional investigation - but because a whole class or group of persons has come to the attention of government for either good or frivolous reasons. Thus do old-fashioned "fishing expeditions" pose as high technology. What is wrong about "fishing expeditions" is wrong about unrestrained computer-matching: it changes the way a government looks at its citizens.

At the time of the three-year Parliamentary review of the *Privacy Act* the question of cross-matching will be among the most important to be examined. (The Privacy Commissioner received a complaint during the past year about alleged matching: the case is discussed in some detail on page 19.)

Parliament will hear powerful arguments to allow matching in the interests of cost-effectiveness and to detect welfare fraud. These are not contemptible or frivolous arguments. But Parliament will want to assure itself that the cost will not be an unacceptable encroachment of soft-edged technology on important human values, an encroachment all the more dangerous for seeming so benign.

Fewer Complaints — Better Rights

"... An individual in the late twentieth century can no longer adequately protect his or her privacy without the assistance of regulatory authorities."

*Professor David H. Flaherty
Protecting Privacy in Two-
Way Electronic Services*

Professor Flaherty of the University of Western Ontario in London is a specialist in privacy theory and practice. His premise will come as a counsel of despair to those clinging to the older civil virtues of self-reliance and rugged individualism. And it goes against the anti-regulatory current said to be running strong.

Yet who will say that he is wrong? The second year's experience of the *Privacy Act* demonstrates that in dealing with their federal government "the assistance of regulatory authorities" is necessary to protect the privacy rights of a growing number of individuals. The numbers speak for themselves. According to statistics gathered by Treasury Board, which is responsible for administering the *Privacy Act*, 36,391 applications for personal information were made between July 1, 1983, and December 31, 1984.

These numbers are impressive, especially so because no publicity campaign has exhorted the public to use the *Privacy Act*. Interest did not wane after the initial impetus provided by the attention the Act received upon coming into force. Eventually the number of requests will level off or even decline. But there is as yet no indication when a peak will be reached or at what level.

There is no doubt that the Act would be used even more if there were an effort to make it more widely known beyond that provided by occasional attention in the media and by the *Privacy Commissioner's* forays across

the land. However, the goal should not be to increase requests for the sake of increase alone: it is to assure that those who need the Act know it and use it.

The departments which receive the bulk of the requests are those which hold the greatest number of personal files or whose decisions touch intimately the lives of many people. Thus, Employment and Immigration, the Royal Canadian Mounted Police, Canadian Security Intelligence Service, National Defence, Public Archives, Revenue Canada, and Correctional Service Canada account for about 91 per cent of the users of the *Privacy Act*.

But are users obtaining their personal information and in a timely fashion? The answer to that question is more important than the mere number of applicants.

The most recent (October - December, 1984) quarterly Treasury Board statistics report that 83 per cent of all applicants received all, or some, of their records: 58 per cent all, 25 per cent some. Three per cent were denied all information being sought. The remaining percentage is accounted for by non-existent information or by abandoned or insufficiently documented requests.

With one exception, these figures have shown little variation from July, 1983. The exception is that the success rate for receiving all personal information dropped to 58 per cent from an earlier high of 68 per cent. It is probably too soon to speak about trends. But it would be of concern if the lower, rather than the higher, figure prevailed over a substantial period.

The record of timely responses to requests is, however, of immediate concern.

During the first year in which the *Privacy Act* was in force, some 80 per cent of applications were handled within the 30 days prescribed in the Act. Upon notice, and with sufficient reason, a further 30-day response time is permitted.

The last quarterly figures from Treasury Board show that only 49 per cent of requests were answered within 30 days. The dramatic and unsatisfactory change is attributed entirely to the performance of two departments, National Defence and, to a considerably lesser extent, Correctional Service Canada.

Though these two departments have received a disproportionately large number of requests and they have devoted considerable resources to handling them, the fact is that a provision of the *Privacy Act* is being flouted. When 41 per cent of applications now require more than 60 days to be processed, as opposed to two per cent in the first quarter after the Act came into effect, a serious breakdown has occurred. Both departments know of the Privacy Commissioner's concern. Each pleads that it is devoting all available personnel to handling the volume of requests. Clearly, that number is insufficient if the terms of the *Privacy Act* are to be respected.

All this being said, quantitative measurements as to how the Act is working should be interpreted with care. While the number of applications totally denied is a matter of special continuing interest, the success rate will depend upon the nature of the personal information being sought. For example, if a large number of applications were for personal information contained in the 20 banks closed to access because of the nature of their contents, then the percentage of refusals would be high. Yet such a figure would not in itself suggest a violation of the letter or spirit of the *Privacy Act*.

It should be a continuing objective to achieve a higher number of satisfied customers. If 80 per cent is good, 90 per cent would be better — as long as personal information was being disclosed within the provisions of the Act and other persons' privacy was not being violated.

The final part of this statistical report covers the number of complaints made by the *Privacy Act*'s dissatisfied customers, at least those who come to the Privacy Commissioner's office. Each case is taken up on behalf of the complainant, who receives the results of the investigation and representations made by the office. In the overwhelming majority of cases, investigations are conducted informally. Such a non-confrontational approach is preferred by both the Privacy Commissioner's office and government institutions, as it usually leads to discussion and understanding. Negotiations frequently result in the release of information which had been denied initially.

The disposition of complaints and their distribution are found in the accompanying tables, which show that the office completed 369 complaints in the 12 months covered by the report and received 366. Since the effective date of the *Privacy Act* the office has received 632 complaints and completed 510.

As a barometer of the Act's performance, these figures too should be approached with caution. The increasing numbers can indicate that the Act is being well used and that there is a growing awareness of privacy rights.

However, the privacy ideal would be realized in a year in which there were no complaints, unattainable as that may be. Though many

complaints may be a gratifying justification of the Privacy Commissioner (the numbers show how busy the complaints department has been), the objective should always be to keep complaints to a minimum. Fewer complaints suggest that more applicants for personal information are satisfied and fewer persons feel that their privacy rights are being violated.

The aim of a Privacy Commissioner, like that of a teacher, should be to make himself unnecessary. However, the statistical evidence of the past year tends to support Professor Flaherty's more realistic judgment that privacy protection requires regulatory assistance as never before.

Some Observations — And a Problem

Generalizations about the effectiveness of the *Privacy Act* are difficult and should be made tentatively. Indeed, it is safer to report upon experience with significant specific cases than to attempt pretentious conclusions. Yet, Parliament is entitled to some observations.

First, there is no evidence that the *Privacy Act* has frustrated law enforcement agencies or given aid and comfort to law-breakers. Neither the police nor anyone else has complained to the Privacy Commissioner that the right of individuals to see their personal records is causing valuable sources of information to dry up. Investigative bodies seem to have been able to protect their sensitive information while respecting the letter and spirit of the *Privacy Act*. Further, the legislation does not appear to be leading to less useful records, double-records or no records.

The primeval human urge to record information seems to overcome any apprehensions of danger or embarrassment from the *Privacy Act*. While the realization that personal information can be seen under the Act is undoubtedly a stimulus to more professional, less capricious or subjective evaluations, there have been no complaints of less valuable records because of less candor.

There are those who argue that the *Privacy Act* makes it too easy to deny applications for information. These critics tell the Privacy Commissioner that the Act provides for too many exceptions.

Exemptions for information received in confidence from a province (section 19) alone justify such criticism. Of course, as long as any personal information is withheld, there will be frustration. Maintaining the delicate balance between, for example, the legitimate demands of national security or

criminal investigations on the one side and an individual's right to know on the other will always mean the denial of some personal information.

The existence of 20 banks exempted from general right of access also frustrates applicants. Departments may release information from these banks at their own discretion; however, they rarely do. The principle of closed banks is defensible, though whether a particular bank should be closed and whether files are appropriately consigned to an exempt bank can only be verified by compliance auditing.

Section 19

Unfortunately, section 19(1) of the *Privacy Act* provides no flexibility and gives no discretion to a federal institution.

This section, which continues to give the *Privacy Act* a bad name, allows some provinces to throw a blanket of confidentiality over all personal information they give to the federal government. This issue was raised in last year's report of the Privacy Commissioner. It remains unresolved, a major source of frustration to applicants and this office. If a province asks for confidentiality, the Act says "the head of a government institution shall refuse to disclose any personal information requested", regardless of how innocuous the information. That's what lack of discretion means.

Some initial provincial caution towards a new Act was understandable. The need for confidentiality for some personal information being passed from government to government is also understandable. But the claim which both Alberta and Ontario have made for total confidentiality shows no sensitivity to fair information principles. The same promiscuous use of the confidentiality provision occurred again this year, with the same

potential destructiveness to the credibility of the *Privacy Act*.

Rather than blindly accepting this barrier to access, privacy investigators ask departments to approach provincial officials for permission to release the material, case by case. However, most departments refuse.

Individuals, therefore, have been placed in the position of being refused access to personal information which had been available before the new legislation came into force; thus, an Act to convey a privacy right has, in this case, denied the right.

Quebec's new privacy and access to information act requires Quebec government agencies to release information to another body only when there is an agreement in force with that body. Since Quebec's act is quite comprehensive, one would expect federal agencies to make agreements with Quebec agencies to enable release of information. Without such agreements, the federal government department holding the information must refuse to release it but could advise the applicant to ask for the information under the Quebec act.

When other provinces have legislation as comprehensive as Quebec's, section 19 will be less of a problem. Until then, access to information will be frustrated.

The Privacy Commissioner repeats his recommendation of last year:

"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."

This particular problem apart, the continuing experience with the Act suggests that the competing rights of public and individual interest are in healthy balance. The satisfying level of cooperation and support which the Privacy Commissioner and his staff continue to receive from public service managers may be accounted for, in part at least, by the perception that the balance is about right.

Access and the Bureaucrats

Awareness of the *Privacy Act* in the public service remains high. Public servants are not only responsible for implementing the Act, they are its largest single group of users — a sign of faith in its efficacy.

Yet many provisions of the *Privacy Act* go against the bureaucratic grain — against the honorable and paternalistic tradition of using personal information in the best interests of a government institution, which do not always coincide with that of an individual. The legislation therefore makes running a bureaucracy more difficult.

The importance of privacy coordinators to the sensitization process in the public service can hardly be over-stated. They continue to be the privacy consciences of their institutions. They are on the front line and they are often confronted with difficult cases. Theirs is a responsibility to help their colleagues appreciate the theory and practice of data protection principles.

Privacy coordinators' worth is measured not by the number of requests for information they handle, but by their success, or otherwise, as privacy animators and defenders of fair information practices.

TBDF — And Closer to Home

A privacy report cannot attain intellectual respectability without at least a bow before those marvellously intimidating initials, TBDF, so staunchly acronym-resistant, and meaning (in full glory) Transborder Data Flow. Though the term may betray the English language, the issues are real and they are serious and they are complex.

Privacy protection gave the original impetus to concern for the vast amounts of personal information crossing national boundaries for use — or potential abuse — and storage in foreign countries. Questions involving the security and control of such data were raised, if never satisfactorily resolved by government policy.

However, privacy issues gave way rather quickly to sovereignty and protectionism which immensely complicated the subject. Discussion focussed not so much on the adequacy of privacy protection laws in foreign jurisdictions, but on the economic impact such transfer would have on the domestic data processing industry. Unfortunately, agreement about such issues is more difficult to achieve than agreement on privacy protection principles. For this reason, privacy should be separated from other considerations in continuing transborder data discussions.

Somewhat encouraging and overdue was a recent conference on TBDF, sponsored by the law schools of the University of Victoria and the University of British Columbia, which gave renewed attention to privacy considerations.

Last June Canada announced its decision to adhere formally to the Organization for Economic Cooperation and Development (OECD) "Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data." As one of the OECD countries which had taken a

commendable leadership role in the formulation of the guidelines, it was an anomaly that Canada was among the last to announce adherence.

The guidelines are an admirable attempt to set minimum, consistent standards of privacy protection laws and fair information practices among signing countries. The standards cover the collection, use, disclosure, security and quality of personal information. They provide, for example, that individuals should have the right of access to information about themselves.

How the guidelines work depends upon the depth of commitment and goodwill of the signatories. But the fact that a code was agreed upon at all demonstrates the growing level of interest and concern.

As a result of its adherence to the guidelines, the Canadian government committed itself to undertake a program "to encourage private sector corporations to develop and implement voluntary privacy protection codes."

This important commitment should be discharged with conviction and vigor and without further delay. Such initiative should encourage private companies to put privacy guidelines in place. A few companies have already adopted codes, instructing their employees on how personal information should be protected. An increasing number of customers are looking for assurances of such protection.

Two arguments support such a campaign:

- 1) Self-regulation is better than government regulation;
- 2) Privacy protection is good business.

It is ludicrous to worry about what could happen to personal information going outside the country while being less concerned, if not studiously indifferent, to what is happening to the same information in the hands of our federal or provincial governments and our private institutions.

If there are no consistent, integrated privacy protection laws in Canadian jurisdictions — and there are not — it comes perilously close to hypocrisy to complain at international forums about loss of privacy when our personal information crosses borders. Like charity, good privacy practices should begin at home.

Compliance — The Commissioner as Auditor

The Privacy Commissioner, as specialized ombudsman for privacy complaints, remains better known than the Privacy Commissioner as auditor of the federal government's personal information handling. Though the investigation of complaints continues to consume the larger share of the office's resources, the compliance role is at least as important.

The auditing responsibility gives the Privacy Commissioner the mandate to determine whether government is treating personal information in compliance with the data protection principles of the *Privacy Act*. Though a cluster of complaints could lead to a general compliance audit, an investigation under this mandate is usually undertaken at the initiative of the Privacy Commissioner.

A staff of four compliance investigators has undertaken two such general audits. The report of the compliance branch provides further details of this and other activities commenced since the arrival of the investigators last fall.

The departments which made history by being selected for the first audits were not singled out because of any special concerns. The audits had to start somewhere and the choice was made on the basis of the size of the task and degree of difficulty.

The results of these first investigations will provide information about a department's state of compliance and of the effectiveness of the auditing procedures.

The fact that a compliance investigation can be made at any time in any federal institution covered by the *Privacy Act* should have a salutary effect upon the handlers of personal information throughout the government. In the end, the best protection is achieved by a system-wide adherence to privacy protection principles.

Issues of Special Interest

To SIN or not to SIN

From the start the question most often asked of the Privacy Commissioner's office is: "When (or why) must I give my social insurance number?" That question was asked by a journalist in Newfoundland, who complained that two large food chains were requiring social insurance numbers before accepting cheques. It was asked by a woman who had to give her SIN before being admitted to the emergency department in an Ottawa hospital. (She didn't argue at the time, though she later discovered that another Ottawa hospital admitted patients without a SIN.) It was asked by a man in New Brunswick who resented his union demanding his SIN. It was asked by individuals in Prince Edward Island where a SIN is assigned to every newborn child.

The quick answer is that the *Privacy Act* protects the way federal government departments collect and use a SIN, as it does any other personal information. But most provinces and the private sector are not covered by specific privacy legislation; thus there are no statutory ground-rules for their use of SIN.

Nine statutes give federal agencies the legislative authority to request a SIN. Those statutes are:

Unemployment Insurance Act, 1971
Immigration Act, 1976
Income Tax Act
Canada Pension Plan
Old Age Security Act
Family Allowances Act, 1973
Canada Elections Act
Canadian Wheat Board Act, and
Canada Student Loan Act.

That's all. Of course, anyone inside and outside of government may also ask. There's no law now against it, nor is there a law against denying a service if a SIN is not produced. An individual makes the trade off: to give or not to give a SIN in return for some service. Should this be changed?

After a special study of the question, Inger Hansen, the Privacy Commissioner under the *Canadian Human Rights Act*, decided not to recommend placing any restriction upon the use of SIN. She felt that would be a dangerous solution because it would provide a false sense of privacy security. She contended that some private identifier would inevitably take the place of the social insurance number and the danger of improper data linkage would rest unchallenged as this other number, or, perhaps, non-numerical information, would be used.

Ms. Hansen recommended that a person or institution collecting personal information to provide benefits or services be required by law to disclose the proposed use. If the collector went beyond the disclosed or consented uses, it would constitute a criminal offence. Ms. Hansen advocated that such protection of law should cover information given to governments, doctors, insurance brokers, banks, or any person or institution. The same protection would cover disclosures compelled by law and information stored in home computers.

Another method of controlling the use of SINs could be legislation, such as Perrin Beatty, MP, proposed in 1979: "to restrict the use of the social insurance number within the federal government . . . along with some initial steps to limit the use of the social insurance number outside the federal government."

It was Mr. Beatty's view that, with a few exceptions, "government should not be able to deny a benefit or impose a penalty because of a refusal to disclose a SIN number." It was also his view that an individual should not be forced to use SIN as an identifier "in order to get a library card, cash a cheque, join a minor hockey league, take ballet lessons, or to collect medicare." Identifiers, in other words, should not be trivialized. That, of course, is right.

But neither should the law be trivialized. Putting more laws on the books to tell persons what they can, and cannot do, with a SIN, making a new crime with offenders subject to fines or imprisonment should be a course of last resort.

Social insurance numbers and other identifiers are here to stay. If such identifiers are used only to prevent persons from being confused with others, they could even protect privacy. Though we may long for a simpler time, and whatever apprehensions we have over being recorded as numbered entities, not many of us are about to turn in our credit cards because each card holder is identified by a number.

The sooner the lingering notion that somehow SINs, or any numerical identifiers, can be legislated out of existence, the quicker the more important issue of effective data protection codes can be addressed. State-of-the-art computers can accomplish with almost as much ease with a name, address and birthdate, what a non-personal identifier can do. The irony is that many persons who refuse to give their SIN have no hesitation in revealing other personal information.

No one should be cavalier about the uses of SIN or any other item of personal information. The danger in focusing exclusively on SIN is that other dangers, at least as insidious for privacy, are overlooked.

When is an MP not an MP?

The dissolution of the previous Parliament following the July 9, 1984, call for the federal election, created an unanticipated situation for the *Privacy Act*. Section 8(2)(g) of the Act allows a department to disclose personal information about an individual "to a member of Parliament for the purpose of assisting the individual to whom the information relates in resolving a problem". The provision is one of the exceptions from the general principle that personal information should be released only to the person it concerns.

Dissolution of Parliament raised a question which the *Privacy Act* does not answer. When is an MP not an MP?

Even after Parliament is dissolved and an election has been called, constituents continue to seek MP's help in locating cheques, following the progress of an immigration application, or finding out how to apply for a grant. These requests for help require a government institution to disclose personal information to the MP.

The Honourable John Roberts, then Minister of Employment and Immigration, believed that MPs should receive such personal information. Consequently, he notified the Privacy Commissioner on July 31, 1984, that under another section of the *Privacy Act*, which permits release if it benefits the individual, he had "delegated all officers of the Employment and Immigration Commission who receive inquiries from Members of Parliament to respond under this authority".

Mr. Roberts gave notice to the Privacy Commissioner of each of the 821 disclosures. Compliance branch staff reviewed each one to make sure of an individual benefit.

The Commissioner chose not to exercise his option to notify each person that information had been released since it was evident that a constituent had asked for the service and a letter from the Privacy Commissioner might cause confusion.

However, the Minister's action created two problems:

1. On July 31, 1984, there were no Members of Parliament and the *Privacy Act* accrues no residual rights to former MPs. Further, the release of third-party information to former members might well be perceived by other candidates as conveying an advantage upon someone whose status in law is no different than theirs.
2. To have given "any officer or employee" of his Commission, as the ministerial order did, the power of the head of a government institution, even for a specific and possibly admirable purpose, seems to be a use of the powers of delegation not contemplated by Parliament in this Act. No other ministers chose this course.

The Privacy Commissioner told Mr. Roberts that he would be raising the matter in the annual report and would recommend that Parliament consider an amendment to the *Privacy Act* to cover periods when there are no Members of Parliament. He now so recommends.

Inmates' Addresses

The *Privacy Act* protects an individual's address as it does all other personal information. Thus, an inmate's location in a federal penitentiary is private because inmates do not lose their privacy rights.

But Correctional Service Canada was concerned that friends, relatives, or lawyers acting for inmates, might arrive at a penal institution to see a prisoner and find him or her moved to another institution. Could Correctional Service give the visitor the new "address" without the inmate's approval?

The lawyer's situation is easy: to deny a lawyer information regarding the whereabouts of a client is a denial of natural justice. If the visitor is a relative or friend, the answer is more complicated.

Though the Act provides that a prison address may be withheld if "it is injurious to the security of penal institutions", relatives and friends have pressured prison authorities to release an address without the inmate's authorization.

Correctional Service, in the assumption that prisoners want close relatives and friends to know their addresses, has guidelines to cover such disclosures. However, if an inmate specifically wishes no visitors and wants his address kept confidential, the *Privacy Act* protects that right.

The Act specifies that the Privacy Commissioner be notified when personal information is given out. Correctional Service has not followed this direction and its officials have told the Privacy Commissioner that they will continue to release addresses unless they have been specifically asked not to by inmates.

While this office has yet to receive a complaint on this issue, it is at best an untidy situation because an administrative practice, however sensible, is at variance with the law.

Exemptions: The Shotgun Approach

Some federal institutions invoke more than one *Privacy Act* section when exempting material. While more than one section may be appropriate for the exemptions, the use of such a "shotgun approach" can lead an applicant to believe that the exempted material is extraordinarily sensitive and important. In fact it is only a department's extraordinary caution.

Such caution is unnecessary.

Should a department select the wrong section to deny information and later be challenged either by the individual or the Privacy Commissioner, it is entitled to change the section to a correct one.

The practice of section shopping could unnecessarily alarm an applicant and lead to complaints which would not otherwise be made.

Often privacy investigators will question the use of particular sections to justify exemptions. During this informal process, departments may agree with the investigator and subsequently release the information requested. By the time the investigator reports to the Privacy Commissioner, both the investigator and the department may agree on the exemptions the department finally claimed. The Privacy Commissioner, equipped with the investigator's report, takes into consideration the fact that personal information was released during the investigation and may, as a result, conclude that he need make no adverse finding.

In this way, it is estimated that applicants received hundreds (perhaps thousands) of documents. However, the number of released pages is not the real measure of success as one paragraph of crucial information could be more significant than many pages.

The positive thing is that the involvement of the Privacy Commissioner's office often produces reconsideration of original decisions and more satisfied applicants. This suggests the widespread acceptance of the spirit, as well as the letter, of the *Privacy Act*.

Workers' Compensation

Federal government employees are subject not to provincial workers' compensation legislation but to the *Government Employees Compensation Act*. Since there is no federal workers' compensation board, the federal government and the various provincial workers' compensation boards have agreed to leave the adjudication of public servants' claims to the board of the province in which a claim arose.

Public servants have had a difficult time gaining access to their medical records held by provincial boards. There have been no appeals launched so the courts have not ruled on whether the federal government owns the medical records of its employees. Many provinces are now amending their legislation to allow claimants either to have access personally to their own records or to have the information explained to them by advocates appointed by the province. The Commissioner hopes that all provinces will amend their legislation to give claimants access to their records, especially when the board has refused compensation.

Micros are Computers Too

Personal or microcomputers, those new status symbols in federal government (as in other) offices, pose yet another new challenge to personal privacy. These machines give their users the capability of creating their own systems of records and, unless protective steps are taken, of having access to central databases without leaving an audit trail.

Yet information in personal computers should be accessible to requests made under the *Privacy Act* and should be given the protection the Act specifies for all personal information, be it in computers or in filing cabinets.

The microcomputer puts added responsibilities on public service managers. They are accountable for all the times a diskette has been copied, where such copies can be located, how they are used, how they are secured and how they are scrubbed once the information contained is no longer required.

The enforceability of data protection principles in the era of proliferating microcomputers is a far more serious data protection issue than the better publicized threat of so-called "hackers" penetrating highly-sensitive data bases.

Stricter security is being developed belatedly and computer manufacturers and users are making breaking-in a much more difficult, if perhaps never quite impossible, technical feat. This is good. But it is vital that action be taken to ensure that access to personal information in all instances is stringently limited to those with a right to know, to collect, store and retrieve.

The *Privacy Act* should provide an incentive to computer companies and software designers to provide built-in protection. A market has been created. If the provinces and private sector were to adopt effective privacy protection codes, the incentive would be irresistible.

The Quebec Act

When Quebec's *Act respecting Access to documents held by public bodies and the Protection of personal information* came into force on July 1, 1984, it was another landmark for data protection in Canada.

Quebec's is the most comprehensive law of this kind of any Canadian province and the appointment of three full-time Commissioners, called for by the Quebec Act, indicates its great scope and complexity.

The chairman of the Quebec Commission, Marcel P  pin, and his two colleagues, Th  r  se Giroux and Caroline Pestieau, as well as members of the staff, visited the Office of the Privacy Commissioner in Ottawa. Subsequently, Mr. P  pin received the Privacy Commissioner and a member of his staff and provided an orientation program covering his office organization and the work of his first year.

Such full, frequent and cordial consultations are valued. They call attention to the absence of similar consultations and other privacy protection legislation in this country.

Of Special Interest — Complaints

The diversity of complaints and other matters referred to the Privacy Commissioner is illustrated later in this report — some cases are worth special mention.

“Cross-matching” and Revenue Canada

Although the *Privacy Act* provides anonymity, the complainant in this case, Perrin Beatty, a Member of Parliament, is identified because he released both the fact of his complaint and the Privacy Commissioner's finding.

Mr. Beatty complained that Revenue Canada attempted to obtain access to individuals' records maintained in data banks of the City of Kitchener, Ontario. He alleged that such access would contravene section 4 of the *Privacy Act*, which prohibits government institutions from collecting information “unless it relates directly to an operating program or activity of the institution.” (The city eventually refused Revenue Canada access to the documents, which included records of payments made by the city to individuals, groups, companies and corporations.)

Mr. Beatty also asked the Privacy Commissioner to investigate and report on whether “the cross-matching of computer data on a whole group of citizens . . . instead of inquiring solely about specific individuals, poses a new and dangerous threat to the privacy of Canadians.”

The Privacy Commissioner isolated the following three issues raised by Mr. Beatty:

1. Does the information which Revenue Canada attempted to collect from the computerized data bank of Kitchener relate to an operating program or activity of the department?

2. If the answer to this question is affirmative, does the manner in which the information was to be collected and used constitute “cross-matching”?

3. Should information of this type, once collected, be accessible under the *Privacy Act*?

The following are quotes from the text of the Privacy Commissioner's findings:

1. Among the objectives of Revenue Canada, as stated in its departmental estimates, are “to administer and enforce the *Income Tax Act*” and “to enforce taxpayer compliance with the law”. Enforcement responsibilities are “to ensure that the taxpayer has complied with the requirements of filing, reporting and payment provisions of the *Income Tax Act*.”

The information sought by Revenue Canada from the municipal records of the City of Kitchener is relevant to the department's operating programs of collecting taxes and determining compliance with the *Income Tax Act*. The collection of such personal information is authorized by section 4 of the *Privacy Act*.

Whether records are held by a taxpaying or a non-taxpaying body, by public or private institutions, by a municipality, school board or hospital, is not relevant. Nor is it relevant whether such records are on tapes, in computers or are those relics of a suddenly ancient time, paper files. What is relevant is that any information obtained related directly to an operating program of the department.

The fact that it is possible for Kitchener to supply Revenue Canada with selective financial data appropriate to its mandate, and not other personal information, allays an important privacy concern: namely that information not related to the department's program would be collected.

In seeking such information from Kitchener, Revenue Canada did not violate the *Privacy Act*.

2. . . . in the case under investigation, the facts reveal that the cross-matching of data would have been done manually. Having found that Revenue Canada had the right to collect the information which it was seeking from Kitchener, the proposed manual data-matching would not pose a new and dangerous threat to the privacy of Canadians.
3. Our concern is that this particular class of personal information, had it been obtained, would not have been accessible between the time it was collected and the time it was transferred to tax files of individuals. The department's failure to have this class of information described in the Personal Information Index is an apparent contravention of sections 10 and/or 11 of the *Privacy Act* which require that all personal information under control of a government institution must be included in the Personal Information Index.

The Privacy Commissioner recommends that Revenue Canada either establish a new information bank, modify the description of an existing one, or incorporate in the Personal Information Index a description of a class of information received as a result of similar requests of municipalities, school boards and any other source."

Among general comments made by the Privacy Commissioner were:

The cross-matching which Revenue Canada was proposing to carry out with information from Kitchener is of a type which has been used by the department for many years. It is ominous and threatening only to potential tax evaders. Checking information on tax returns against other specifically financial data, whether performed manually or mechanically, is a basic technique of Revenue Canada's trade and poses no conflict with the *Privacy Act*.

The Privacy Commissioner recognizes the heavy and important responsibility placed upon Revenue Canada. The duty of the department to ensure compliance with the *Income Tax Act* requires intrusions upon personal privacy. Privacy protection is not an absolute.

Restrictions placed upon the tax authorities in the name of personal privacy should not be so onerous as to give aid and comfort to tax evaders. The new computer technology, under appropriate controls, should be put to the service of the state in the interest of compliance with tax laws. Indeed, the uses of technology are rarely denied.

But the threat to cherished human values is real. The comments contained in this finding attempt to protect these values without placing unreasonable and merely doctrinaire constraints upon those performing their somewhat thankless task on behalf of all Canadians.

The danger in proposing a set of privacy protection controls over cross-matching is that it may encourage a practice that the *Privacy Act* prohibits. But the Act applies only to federal government institutions and cross-matching goes on outside of the Act's jurisdiction. (Last year a United States Congressional Committee was told that some 500 computer-matching programs are routinely being carried out by U.S. federal and state authorities.) The issue may soon be not whether cross-matching should take place but on what ground rules should it be allowed.

Leggatt Commission and Confidential Inmate Files

A city police chief complained to the Privacy Commissioner that personal information which a detective gave in confidence to a caseworker for a parolee's National Parole Board file had found its way to the individual during The Commission of Inquiry on Habitual Criminals, conducted by Judge Stuart M. Leggatt. The chief alleged that, by giving the file to the inquiry, the Parole Board breached the *Privacy Act* because federal agencies are required to protect material which they receive "in confidence" from a province.

A lengthy investigation found that the information was included in a file given to Judge Leggatt to study what should be done with individuals who had been designated "habitual criminals" in federal penitentiaries.

The Parole Board chairman believed the judge had subpoena powers and would confine the information to the study team. However, the individual inmate obtained the information.

The privacy investigator examined files both at the Parole Board and the Department of Justice and found nothing to establish subpoena powers for the judge. Had the judge subpoenaed the file, however, the Parole Board would still have been obligated to stress the confidential nature of the information when it transferred the file.

The investigation showed that the Parole Board chairman had taken extensive precautions to protect the confidentiality of the information. However, they proved to be inadequate. The Board attempted to prevent a similar disclosure in another province by sending a team to review the files with the judge's staff. This consultation never occurred because the Minister of Justice ordered the files released immediately, leaving the matter of privacy protection to the judge.

The Commissioner concluded that not all blame rested with the Parole Board but a confidence had been breached and for that the Board had to bear the ultimate responsibility. He found the complaint to be justified and he recommended that documents appointing commissions of inquiry which require access to personal information should give notice of the need to preserve the privacy of individuals and to respect the provisions of the *Privacy Act*.

Such notice should be given whether or not the commission possesses the power to subpoena records. It was provided in the terms of reference for Mr. Justice Jules Deschênes' inquiry into the alleged presence of war criminals in Canada. It should have been given to the Leggatt Commission as well.

Government Pay Cheques and Privacy

A public service union complained to the Privacy Commissioner that Correctional Service Canada was not respecting the confidentiality of pay cheques when it gave them to shift supervisors for distribution. It was pointed out that in some penitentiaries up to four supervisors handled the open cheques, which list all deductions and any garnishment information.

The Privacy Commissioner considered the complaint justified.

After a series of meetings between the Privacy Commissioner's office and Treasury Board, Correctional Service agreed to put the cheques in envelopes.

The investigation showed that the problem was not confined to Correctional Service as many departments failed to protect the confidentiality of employees' cheques. The Commissioner asked Treasury Board to consider a public service-wide solution.

In a February 1985 memo, the secretary of the Treasury Board informed deputy heads that Supply and Services Canada would place all pay cheques in window envelopes. Thus, pay staffs will be able to check the employees' name, payroll number and cheque number against their files while insuring confidentiality of sensitive personal information.

The story of how each federal government pay cheque now has (or is about to have) its own envelope is a testimonial to privacy enlightenment at Treasury Board and a model of systemic privacy protection.

Leaving personal pay cheques and their stubs on desks or distributing them like cards from a pack were invitations to privacy

violations. Perhaps more indefensible was the discriminatory pay cheque delivery practice of giving most senior officials their cheques in envelopes. Lower ranks — the cut-off point depended upon arbitrary and inconsistent decisions — somehow seemed entitled to less privacy with less pay.

After the Privacy Commissioner brought this matter to his attention, the secretary of the Treasury Board reacted with initiative and leadership. He convinced a government with economy on its mind to give the pay cheques of employees at least the same level of protection that is given almost universally by other employers.

Department of National Defence - Delay

A large backlog of applications for access to one National Defence bank P-470 (Performance Evaluation files) has dogged DND's privacy office and is one cause of 47 complaints of delay to the Privacy Commissioner in the past year. The number of complaints is a remarkably small percentage of the well over 10,000 requests made since DND opened this formerly closed bank on July 1, 1983. The majority of applicants have accepted patiently delays of many months.

While the problem is primarily processing and not privacy, the *Privacy Act* deems a delay of more than 60 days to be a denial of access. At the end of March, 1985, DND was some 4,500 requests behind and continuing to receive requests at the rate of 75 to 100 a week.

DND has assigned 22 persons to work full time (and, often overtime) to handle the volume of work. Nevertheless, with no foreseeable lessening of the request flow, the department should either assign a staff adequate to the need or change its

procedures to give rapid access to at least some kinds of personal information. More effective would be the routine release of personnel evaluation files without recourse through the *Privacy Act*.

Departments should remember that the *Privacy Act* was not meant to replace informal employer/employee communication.

Opinions about Others

A woman complained that Employment and Immigration Canada invaded her privacy by identifying her as the person who complained to the department about an employee's political activities while on sick leave.

Upon request, the department told the employee who had complained. He subsequently revealed it during media interviews.

The Commissioner dismissed the complaint because the *Privacy Act* grants an individual the right to know who expressed an opinion, or lodged a complaint, about him or her.

The *Privacy Act's* catalogue of "personal" information lists such self-evident items as address, fingerprints, religion, and marital status. Much less self-evident is that the definition of personal information also includes "views or opinions of another individual about the individual".

To some it comes as a shock that what they have said about others, even for the most public-spirited of reasons, may be read by the subject of the comment. Not only may the opinion be disclosed under the *Privacy Act*, so may the name of the person who has expressed the opinion.

Some have argued that the effect of such a disclosure will inhibit the release of information which might serve a useful public purpose. The woman in the case cited clearly believed she was being a good citizen and acting in the public interest. One can appreciate her horrified reaction to the release.

There is, however, a greater danger in not giving such information to the person concerned as individuals could become the victims of unknown and malicious accusations. A difficult trade-off has been made and the public should be aware of that trade-off.

Spreading the Gospel

Inherent in the role of Privacy Commissioner will always be a responsibility to tell Canadians about their rights under the *Privacy Act* and, at least as important, to hear them air their fears about privacy invasion. Those fears, ranging from abuses of their social insurance number to vulnerability of their information to computer "hackers", are significantly more developed than the general knowledge of federal privacy legislation.

That is why it is especially important in the initial stages of a new act to accept all speaking invitations, no matter the size, or the remoteness, of the group, and to be available to the news media for such things as interviews and radio open-line programs.

In the past year, the Privacy Commissioner has spoken to such diverse groups as the Canadian Bar Association and the Consumers' Association of Canada annual conventions, the Conference Board of Canada, Canadian Clubs, the Canadian Credit Institute, the College of Physicians and Surgeons of Ontario, the Data Processing Institute, a government of Ontario privacy conference, a computer class of the University of Toronto, a conference on Transborder Data Flow sponsored by the law schools of the University of Victoria and the University of British Columbia, the American Society of Access Professionals, a conference on health records, and a Science Council of Canada privacy conference.

These and other engagements gave the Commissioner the opportunity to appear in Alberta, British Columbia, Saskatchewan, Manitoba, Ontario, Prince Edward Island, Quebec and Yukon. In the previous year, he was in Nova Scotia and New Brunswick. Newfoundland and the Northwest Territories will be among the first parts of the country visited in the coming months.

The Privacy Commissioner represented Canada at a meeting of data commissioners held last year in Vienna. Provincial representatives from Quebec and Ontario also attended this meeting, the only such annual international forum that provides a valuable opportunity for the exchange of information on data protection issues.

Complaints Investigations

The Commissioner's powers to investigate are considerable. He may enter premises, interview personnel, compel both oral and written testimony, require that witnesses produce documents or other records, and administer oaths and receive evidence. However, the Commissioner's investigators operate as informally as possible, reserving formal procedures for only the most difficult cases.

Complications in the Public Service Commission staffing process prevented permanent investigators from joining staff until late in 1984. In the interim three skilled contract investigators handled the complaints. After an intense orientation period the permanent investigators whittled away the backlog and by the end of the 1984/85 fiscal year, the Complaints Branch had undertaken 366 new investigations and completed 369. Of these, 132 were carried over from the preceding year.

Most of the complaints cited denial of access to some, or all, of the material, 49 per cent, while the balance concerned delays of more than the initial 30 days, 40 per cent; denial of a correction or notation, three per cent; misuse of the information, six per cent; documents not in the applicant's official language, .3 per cent; deficiencies in the Personal Information Index, .5 per cent; and the collection, retention and disposal of personal information, 1.4 per cent.

The following case summaries illustrate the many complaints handled by the office during the past year. Researchers interested in details of particular cases may examine copies of write-ups on each complaint, available in the library of the Privacy and Information Commissioners.

Our example cases omit names because the Act assures privacy to anyone filing a complaint. Some departments crop up frequently in the case summaries, as five account for 91 per cent of the applications and 66 per cent of the complaints. This occurs because some have huge workforces (National Defence), some have considerable public contact (Employment and Immigration), and others keep files that by their nature are interesting to the public (RCMP and Correctional Service). The fifth department — the Public Archives — is a repository for all outdated documents such as old personnel files, military records and census data.

Access

This category includes complaints from individuals who have been denied all, or some of, the information in their personal files. The *Privacy Act* permits departments to withhold information for a number of reasons. Examples are: if the information concerns another individual, 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 50.)

Investigation Prompts Release of More Documents

In this case a New Brunswick man complained that following his request to see his personal information, Employment and Immigration Canada (EIC), withheld eight documents.

EIC claimed it exempted the documents because they related "to the physical or mental health of the individual" and their release "would be contrary to the best interests of the individual". This exemption is permitted by section 28 of the *Privacy Act*. EIC medical staff tried to reach the authors of each of the withheld documents to determine whether they would permit release of the information. Conflicting opinions and an inability to find all the authors convinced the department not to release the medical information.

In discussion with EIC the Commissioner's investigator arranged release of three of the eight documents. The Privacy Commissioner considered the balance to have been properly withheld but ruled that the complaint was justified.

Complaint Is Private

A public servant preparing an appeal of a staffing decision applied to see specific documents held by the Public Service Commission (PSC). The PSC provided all of the material it believed the *Privacy Act* allowed and one extra document from which it had deleted some information it maintained concerned another individual.

During subsequent hearings, court was told that some of the evidence the employee's lawyer presented was obtained through the *Privacy Act* and that some of it was incomplete. PSC's lawyer provided open court with a revised version of the document, including the deleted information.

As a result the public servant complained to the Privacy Commissioner that revealing he had obtained information through the *Privacy Act* was itself a breach of that Act, and that the deleted information revealed during the hearing was personal and should have been given to him in response to his original request. PSC argued that by providing a document the applicant had not requested — but which clearly related to his request — it had "operated in a spirit of openness" and was not obliged to make sure that any deletions met the tests set out in the *Privacy Act*.

The Privacy Commissioner disagreed and considered that complaint justified. Since the parties disagreed on who revealed the existence of a *Privacy Act* request, and the complainant decided not to pursue the process to search the appeal records, the Commissioner made no finding on the second complaint. He reminded the Public Service Commission, however, that access requests under the *Privacy Act* are themselves personal information.

Compensation Board Withholds Medical Report

An Ontario man, refused a disability pension under the Canada Pension Plan, complained to the Privacy Commissioner that he was denied access to the report which generated the refusal. The complainant had authorized Health and Welfare Canada to obtain proof of his disability from the Workers' Compensation Board. The Board provided the report but refused to release it to the applicant when he was denied the pension.

Section 19 of the *Privacy Act* requires federal organizations to withhold personal information obtained in confidence from a province. The Board's letter to Health and Welfare Canada was specific — the report was "privileged information" and not to be released. Health and Welfare suggested the applicant contact the Board directly.

The Privacy Commissioner found that Health and Welfare Canada was bound by section 19 and dismissed the complaint.

Section 19 Prevents Statistics Release

A B.C. man also ran into difficulties with section 19 when he tried to obtain information from Statistics Canada's vital statistics bank. He was refused a request for information about his place and date of birth and particulars about his parents and their names because the information was given to the federal government "in confidence" by the provincial registrar general.

The Privacy Commissioner sympathized with the applicant's frustration at being caught in what appeared to be a "bureaucratic maze" but he had to refer the request directly to the registrar general of the province in which the applicant was born — and dismiss the complaint.

Canada Post's Employee Banks Cause Problems

A Canada Post employee asked to see all the personal information 18 standard employee banks held about him. After receiving the material he complained to the Privacy Commissioner that the information banks were incomplete and not organized as described in the Personal Information Index, that he did not receive all of the material, that the exemptions claimed on some documents were unjustified, and that copies of some of the documents were illegible.

The investigation found that Canada Post had not organized its employee banks as listed in the Index. This is not a breach of the *Privacy Act* as the Index recognizes that some federal institutions organize their personnel records differently. The Act does, however, require that employees know what is kept and be able to see it.

To respond to the request Canada Post had to retrieve the personal information from its employee records and then organize it according to the standard bank classification. The Commissioner agreed with the applicant that the material he received was not sufficiently organized for him to identify the source bank or access request. Canada Post officials agreed to re-release the material, properly identified, or show the applicant the segregated packages of material at their offices. They also agreed to replace any illegible copies.

The Commissioner did not agree with the applicant's claim that some material was exempted incorrectly. The Commissioner examined the documents and agreed with Canada Post's position that some information was a privileged exchange of information between solicitor and client, and some concerned other individuals.

The Commissioner concluded that, despite some shortcomings, Canada Post had gone to "exceptional lengths" to find all retrievable information about the applicant.

Because of the complaint, Canada Post has examined its employee banks description and these will be revised in an upcoming edition of the Treasury Board bulletin.

Citizens and Permanent Residents Only

A lawyer complained that Employment and Immigration Canada (EIC) "perverted" the *Privacy Act* by using it to refuse him a copy of his client's deportation order which he needed to assess the man's chances of being admitted as a permanent resident.

EIC refused the document on the ground that the lawyer's client was neither a Canadian citizen nor a permanent resident as required by the *Privacy Act*.

After the Privacy Commissioner received the complaint, EIC told an investigator that the lawyer had been sent the document already, but his client did not meet the citizenship requirements. The Privacy Commissioner dismissed the complaint noting that EIC had provided the document despite its not being required to by the *Privacy Act*.

Personal Information About Others

A personality conflict between two Employment and Immigration Canada employees brought about an internal investigation. One of the women asked for access under the *Privacy Act* to all the material about the investigation and most of it was provided. However, eight documents were exempted because they also contained information which concerned other individuals.

The applicant objected to the material being withheld and complained to the Privacy Commissioner. The complaint was dismissed after an investigator examined and reviewed the documents and concluded they did concern other individuals.

Job Competition Documents Incomplete

A Quebec woman asked to see all Canada Post documents pertaining to her candidature for a 1981 postmaster competition. She received the material but complained to the Privacy Commissioner that Canada Post had withheld, without explanation, two telexes, a letter and a handwritten note and removed information from documents she did receive.

Canada Post was unable to find the items in the regional office competition files and copies of telexes, kept at Canada Post headquarters, are destroyed routinely after two years. Canada Post officials speculated that the material may have been destroyed between October, 1981, (when Canada Post became a Crown Corporation and not subject to the privacy protection in Part IV of the *Canadian Human Rights Act*), and July 1, 1983, when it became subject to the new *Privacy Act*.

The investigator confirmed that the information was not in the files and found that the original document from which information was withheld contained paragraphs assessing the other candidates. Since applicants may not see personal information about other individuals, the material was properly exempted under the *Privacy Act* and the Commissioner dismissed the complaint.

However, the Act requires a department to tell an applicant why information is withheld. Canada Post eventually advised the applicant that the information concerned someone else but the Commissioner considered justified this aspect of the complaint.

Solicitor-Client Correspondence

A Toronto man applied for his records from Employment and Immigration's Employment Centre at York University. He complained to the Privacy Commissioner about the delay and about being required to complete a second access request to see material in the Minister's office.

The investigation revealed that EIC had sent the material within the 30-day time limit and that the request to see material from the Minister's office should have been made on a separate form as applicants must use separate request forms for each bank they wish to examine. The Commissioner dismissed both complaints.

Shortly after receiving the material, the applicant filed another complaint because EIC had withheld information as it was "subject to solicitor-client privilege". He asked for a list of the documents withheld because he had never had a legal dispute with the department, and for any written guidelines on how to apply to the Federal Court for a review.

The investigator examined the documents and confirmed that the material was correspondence between the department and its lawyer. The Commissioner dismissed the complaint, explaining to the applicant that the solicitor-client privilege was between the department and its own lawyers. The Commissioner also explained the court review procedures and enclosed the relevant sections of the *Privacy Act*.

Complaints Prompt Release

Three individuals complained to the Commissioner that the Public Service Commission (PSC) denied them access to personal information about an anti-discrimination directorate investigation. The investigator's examination found one master file with about 600 documents concerning all three individuals, and individual files containing approximately 150 documents each.

The PSC claimed that the directorate was an investigative body under the *Privacy Act* and investigative reports could be withheld.

The Privacy Commissioner pointed out that only the investigative bodies listed in the regulations to the Act could withhold investigation files and the anti-discrimination directorate was not on the list. Therefore, it could only refuse to disclose the information if it "could reasonably be expected to be injurious" to any law of Canada or a law of the province or the conduct of a lawful investigation .

After a review PSC released all but approximately 100 of the papers sought and advised the complainants that the material was being withheld either because it concerned other individuals or its release could interfere with a lawful investigation.

The Privacy Commissioner considered the original complaint justified. The resolution of this complaint prompted the PSC to review the contents of several personal files kept by its Appeals and Investigations Branch and to release some or all documents requested by other complainants.

The anti-discrimination directorate has since been disbanded and public servants' discrimination complaints are now investigated only by the Canadian Human Rights Commission, which is not an investigative body under the *Privacy Act* either.

Canada Post Releases Complaint Letters

An Ontario man whose rural mail contract was not renewed complained to the former Privacy Commissioner that Canada Post delayed in providing him access to his personnel record.

At the time, Canada Post was a Crown Corporation and not subject to the privacy protection contained in Part IV of the *Canadian Human Rights Act*. When the new *Privacy Act* took effect July 1, 1983, and Canada Post was covered the Commissioner brought the complaint forward. In November, 1983, the local postmaster advised the applicant that the documents could be consulted in his office, but the complainant objected to having to deal at the local level. The Commissioner concluded that he had no mandate to tell the post office how to route its correspondence.

The applicant's examination of the material found several pages had been exempted because they concerned other individuals. He complained to the Commissioner because he believed the exempted documents explained why his contract was not renewed. The investigator's examination concluded that the exemptions had been applied too broadly. Several of the exempted documents were letters from residents on the applicant's route complaining to the local postmaster about mail in the wrong boxes, obscene language and garbage in mailboxes.

Following the investigation Canada Post agreed to release some of the letters, omitting the writers' names and addresses because it was concerned that the complainant would retaliate. The Commissioner agreed with this exemption but considered both the delay and other exemption complaints justified.

More Information Found

An inmate complained that Correctional Service Canada (CSC) had delayed in providing files from four banks and had denied his application to see personal information in two other CSC banks P-70, (Institutional Security Threats Records), and P-50, (Preventive Security Records). Both banks are closed by order of the Cabinet and CSC would neither confirm nor deny the existence of any personal information about the complainant in either bank. The investigator examined the files in all the banks and found documents he believed CSC should release. The department agreed and sent these to the inmate, apologizing for the oversight.

The Commissioner found the delay complaint justified since CSC had taken more than 60 days to provide the information. He dismissed the complaint that access was denied because the Cabinet has designated both banks as closed. Nevertheless, the Commissioner assured the complainant that these banks had been examined and that he had not been denied any rights under the *Privacy Act*.

Copies Must Be Legible

A P.E.I. man complained to the Commissioner that requested documents from Revenue Canada were largely illegible, contained incomprehensible codes and that the department had effectively denied him access to the material.

The investigators agreed that the copies were illegible and the department offered to provide new copies of the documents and to explain the internal codes. The Privacy Commissioner considered the complaint justified.

However, the man complained again because he felt that referring to the individual by the initials "TP" (taxpayer) was degrading. This complaint was beyond the Privacy Commissioner's mandate.

Won't Cross Match Files

A retiring university professor applying for his pension complained to the Privacy Commissioner because Health and Welfare would *not confirm his residence in Canada* by checking his files at Employment and Immigration and Revenue Canada. Although he had authorized Health and Welfare to cross-reference his information, it refused because the *Privacy Act* forbids departments from using personal information for a purpose unrelated to its original collection.

The professor had worked and taken sabbatical leave outside of Canada and needed the other departments to prove that he and his wife, who had accompanied him, met the residence qualifications for old age pension.

A phone call from the Privacy Commissioner's office broke the logjam. Health and Welfare reviewed the file and approved the application without further documentation.

The Commissioner dismissed the complaint because the department obeyed the *Privacy Act* by refusing to cross-match unrelated personal information in another organization's banks.

Delays

Delays continue to be a frequent reason for complaint to the Privacy Commissioner.

Commissioner. The *Privacy Act* provides departments with up to 30 days to furnish information or to advise an applicant that up to 30 days more time is needed to consult with other departments or to avoid seriously disrupting operations. A department needing the extra 30 days must advise applicants of their right to complain to the Privacy Commissioner. An extension of longer than 60 days is considered a denial of access.

Correctional Service Canada continues to experience difficulty in handling requests within the time limits. The problem occurs because inmates' files have to be carefully screened to ensure that no information is released which could endanger third parties or disrupt the security of a penal institution. More than 90 applicants have complained of delays to the Privacy Commissioner since July 1, 1983, but following representations from the Commissioner, CSC attacked the backlog and the number of complaints was greatly reduced.

Department of National Defence too has fallen seriously behind in handling information applications. The department's opening of the Performance Evaluation Report files (Bank ND-P-P470) prompted a deluge of requests from those interested in seeing the assessments on which promotions are based. In the October to December, 1984, quarter alone, DND received 3,516 applications to examine all types of personal files. By the end of the 1984/85 fiscal year, the Privacy Commissioner's office had received 47 complaints from DND applicants who had tired of waiting for information.

Taxation Finds Information Elsewhere

In June, 1984, an applicant asked to see personal information in a Revenue Canada-Taxation bank in order to prepare an income tax appeal. The bank, which contains files on individuals being investigated for tax avoidance, is one of the 20 to which the *Privacy Act* does not automatically give the right of access. However, departments may exercise their own discretion and release information from these banks.

Revenue Canada told the applicant that because the bank was closed there would have to be consultation with the Department of Justice, which would delay action beyond the 30 days allowed in the *Privacy Act*. Revenue Canada advised him of his right to complain to the Privacy Commissioner about the delay and he did.

After consulting with Justice, Revenue Canada opened the bank and did not find the information he requested. However, the regional office near the applicant's home found the desired information and arranged for him to pick it up in time for his appeal.

Although the department's response was delayed it did look for a file in a closed bank to track down any relevant information. Nevertheless the Privacy Commissioner considered the complaint of delay to be justified.

Inmate Abandons Complaint — and B.C. Penitentiary

A B.C. penitentiary inmate asked to see files in Correctional Service Canada (CSC) and National Parole Board banks to prepare his day parole application. When the departments told him that they would need more than the normal 30 days to consult with other agencies, he complained to the Privacy Commissioner.

The Parole Board gave him the material within the extended time limit and the Commissioner dismissed the complaint. CSC was unable to provide him with the documents until almost a month and a half later. The Commissioner considered this complaint justified.

Once he had the files, the inmate complained that several documents were about someone else and others referred to crimes he was supposed to have committed while he was in custody. He asked the Commissioner to have the information corrected but since requests for correction have to be made to the department holding the records, the Commissioner sent him copies of the appropriate form and referred him back to the department.

Denied parole, the inmate asked for documents from the hearing and from an RCMP bank to prepare an appeal. When some of these were withheld, he again complained to the Commissioner and the investigator found the RCMP had withheld records gathered while the force was performing policing services for a province — a mandatory exemption under the *Privacy Act*. The investigator also found that the Parole Board's exemptions were also correct.

The Commissioner dismissed both complaints and so advised the inmate as he also acknowledged receipt of yet another complaint. Shortly afterward, Correctional Service informed the Commissioner that it would not be releasing that file — the complainant had escaped.

Phone Acknowledgements Won't Do

A member of the armed forces complained to the Commissioner when National Defence had not arranged for him to examine his personnel evaluation reports three months after he had applied. His

application was sent to the DND access to information unit. (DND is one of the few departments with separate privacy and access to information offices.) The department advised him that his application had been forwarded to the privacy office. The applicant heard nothing further and lodged his complaint two months later.

The investigator found that DND's privacy office had more than 2,400 applications and the staff was working overtime to clear the backlog. Rather than writing to confirm receiving requests, staff telephoned acknowledgements. They had been unable to reach the applicant.

The Privacy Commissioner, finding the delay complaint justified, cautioned DND that a phone acknowledgement is not sufficient. The *Privacy Act* requires that applicants be advised in writing when the 30-day deadline cannot be met, and of their right to complain to the Privacy Commissioner. DND now acknowledges in writing, as required.

Delays Monitored

An Employment and Immigration Canada (EIC) employee who applied to see personal documents in July, 1984, to pursue a grievance was told the department would need up to 30 more days for "consultations" before providing the information.

The applicant had not received the information in time for a second-level grievance hearing and believed that if the extension was granted, he would not get the documents for the third level hearing, tentatively set for mid-September, 1984. In late August he complained to the Privacy Commissioner.

During the third week in September the applicant received one full document and 10 with information withheld because it concerned another individual.

The investigator found that EIC's delay reflected the large number of privacy requests, a staff shortage in its access and privacy office and the need to consult a regional office. The Privacy Commissioner agreed that meeting the original 30-day deadline would have "unreasonably interfere(d) with operations". He dismissed

the complaint. However, the Commissioner was concerned that EIC not invoke the 30-day extension automatically to consult with its own regional offices. The Privacy Commissioner's office has seen an improvement in EIC's performance, but will continue to monitor the situation.

DISTRIBUTION OF COMPLETED COMPLAINTS BY GOVERNMENT INSTITUTION AND RESULT

Department, Ministry or Institution	Abandoned	Justified	Dismissed	Total
Agriculture Canada	—	—	2	2
Canada Deposit Insurance Corporation	—	—	1	1
Canada Mortgage and Housing Corporation	—	—	2	2
Canada Post	—	3	3	6
Canadian Human Rights Commission	1	1	—	2
Canadian Security Intelligence Service	—	—	1	1
Correctional Service Canada	1	46	47	94
Department of Justice Canada	—	—	1	1
Employment and Immigration Canada	—	10	30	40
Energy, Mines and Resources Canada	—	—	1	1
External Affairs Canada	—	—	3	3
Farm Credit Corporation Canada	—	—	1	1
Fisheries and Oceans	—	2	1	3
Health and Welfare Canada	—	1	7	8
National Defence	4	44	7	55
National Film Board	—	—	1	1
National Parole Board	1	12	12	25
Pacific Pilotage Authority	—	—	1	1
Ports Canada	—	1	2	3
Privy Council Office	—	—	1	1
Public Archives Canada	—	—	7	7
Public Service Commission of Canada	—	11	5	16
Public Service Staff Relations Board	—	—	1	1
Revenue Canada - Taxation	1	4	14	19
Royal Canadian Mounted Police	1	3	44	48
St. Lawrence Seaway	—	—	1	1
Secretary of State	—	—	1	1
Solicitor General Canada	—	—	9	9
Statistics Canada	—	—	2	2
Supply and Services Canada	—	—	1	1
Transport Canada	—	2	2	4
Veterans Affairs Canada	1	—	8	9
Total	10	140	219	369

Correction or Notation

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 judgements 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.

Language Skill Challenged

A "student" who annotated a teacher's evaluation in his language training file following a complaint to the Privacy Commissioner, complained again when no notation was made on the computer record. He also complained because the *Public Service Commission (PSC)* had refused to tell other agencies which had the information about the notation.

During investigation it became apparent that PSC had in fact told the complainant it would notate the record. The staff would not, however, commit itself to a particular method until the computer program was examined to determine how to do it without introducing extensive modifications to the entire system. Two months later, PSC notified the investigator that it could flag the computer record and so advised the complainant. The investigator also confirmed that the information in the bank is used only by the Language Training School and not distributed.

The Privacy Commissioner dismissed both complaints.

Notates 66-Year-Old Record

An applicant asked to see medical documents in Veterans Affairs' bank P60 (Post Discharge Treatment) to support an application for a pension review. The search exceeded the allotted 30 days and he complained to the Commissioner about both the delay and his medical assessment following discharge from service.

Since the Records Management Division was in the midst of moving to P.E.I., and the required records dated back to 1918, the response was delayed but the records were eventually found at the Public Archives within the 60 day allowable extension limit. The Commissioner considered the delay reasonable and dismissed the complaint.

Public Archives refused the applicant's request to correct one record because there was no evidence to refute the medical examiner's diagnosis. However, the applicant was unhappy with a reference to his mother's health and asked to annotate the file. The Archives agreed and in April, 1984, — 66 years after the form was completed — the veteran clarified a comment about his mother's health.

Misuse

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

The chairman of the appeal hearing refused to admit the letter as evidence but the Commissioner concluded that EIC had breached the *Privacy Act*. The department amended its administrative policy guidelines to ensure the breach did not recur.

Witness' Documents Given Hearing

The Privacy Commissioner received a complaint when it was alleged that Employment and Immigration Canada (EIC) had copied a letter of reprimand from a personnel file in order to discredit an individual as a witness at another individual's hearing.

The *Privacy Act* allows departments to use personal information consistent with the original purpose of collection providing they have notified the Privacy Commissioner. The complainant believed that using his personnel file to discredit his testimony at a hearing for someone else was not a "consistent" use and the Privacy Commissioner agreed.

GROUPS OF COMPLAINTS AND INVESTIGATION RESULTS

Grounds	Abandoned	Justified	Dismissed	Total
Misuse	—	5	17	22
Access	4	27	151	182
Correction	—	—	10	10
Language	—	—	1	1
Index	—	2	—	2
Collection/retention/ disposal	—	—	5	5
Delay	6	106	35	147
Total	10	140	219	369

Index

Persons may complain to the Privacy Commissioner if they believe that the Personal Information Index — the listing of all the federal government's information banks and classes of personal records — is deficient in some way.

DND Bank Missing

An Ottawa man complained that the index contained no listing of personal information held by National Defence's Communications Security Establishment (CSE). The Commissioner's office confirmed that CSE does hold personal information files and that they were not listed in the 1983 edition of the index.

The investigator found that DND had already realized the omission and taken the necessary steps to have the bank listed in the 1984 edition where it appears as Bank ND-P70, Security and Intelligence Information files. The Commissioner considered the complaint justified.

ORIGIN OF COMPLETED COMPLAINTS BY PROVINCE AND TERRITORY

Newfoundland	1
Prince Edward Island	2
Nova Scotia	14
New Brunswick	12
Quebec	84
National Capital Region Quebec	7
National Capital Region Ontario	36
Ontario	79
Manitoba	24
Saskatchewan	16
Alberta	33
British Columbia	54
Northwest Territories	1
Yukon	1
Outside Canada	5
Total	369

Without Complaint

Periodically there are situations which warrant the attention of the Privacy Commissioner but have not been the focus of a complaint. For example, an issue with privacy implications caught the office's attention during the final stages of hiring the Commissioners' own investigators.

After winnowing a list of 644 candidates down to those 41 who qualified, the Public Service Commission (PSC) prepared lists which ranked the successful candidates by merit and language capability.

Copies were made and envelopes were prepared to all candidates when the Commissioner's staff questioned whether distributing the comparative rankings to all of the original candidates infringed on the privacy of those on the short list.

Clearly it was "in the public interest" to inform the candidates of the ultimate winners to ensure the fairness and openness of the procedure. It was also apparent that candidates were not told that their names would so appear and no PSC information bank description identified this type of information.

The Privacy Commissioner brought the apparent omission to the attention of the chairman of the PSC. Subsequently, representatives of PSC and the Privacy Commissioner reviewed a new application form containing a direct reference to the *Privacy Act*. The PSC agreed to review the description of the Index bank to ensure that job applicants were aware that rankings of successful candidates could be given to individuals wishing to lodge appeals.

Here is another example.

After Treasury Board released the 1984 edition of the Personal Information Index, the Privacy Commissioner's staff found that the RCMP's Security Service Record (bank RCMP-P-130) was no longer listed and had not been transferred to the new Canadian Security Intelligence Service (CSIS) listing. The new edition describes CSIS and shows that RCMP personal information holdings have "been substantially transferred to . . . CSIS". However, no specific information banks are listed and without the 1983 Index an applicant cannot know what kind of personal information is gathered.

The Privacy Commissioner told the Treasury Board president that the omission breached the *Privacy Act* and that the information bank was effectively lost to applicants. He hoped that Treasury Board could make the Canadian public aware of the existence of this information bank.

The president advised the Commissioner that the structure of CSIS' holdings "may not necessarily replicate the structure of the previous organization" and that when details were settled a description of holdings would be published "at the earliest opportunity".

This solution does not address the problem that, for an applicant's purpose, the bank is non-existent until listed in an interim Bulletin.

Inquiries

Much of the investigators' time is devoted to answering letters and telephone inquiries about the *Privacy Act* and how it can be used.

The staff handled 1,008 inquiries during the past year, including 112 that concerned the use (and perceived abuse) of social insurance numbers. Callers questioned a Toronto newspaper's contest which drew readers' SIN for prizes and a Saskatchewan university's using SIN as student numbers. However, one person wanted to use a SIN instead of other personal information.

Another 584 inquiries came from individuals who believed the Privacy Commissioner's office to be the access point for personal information. In these cases, investigators helped callers with the process and, when necessary, redirected application forms to the proper agencies.

The remaining 312 inquiries were beyond the Commissioner's mandate, although staff often provided information and referred callers to the appropriate organizations. Individuals asked for access to personal records held by Crown corporations, credit bureaus, hospitals and provincial governments; a man objected to his employer's inquiries in order to have him bonded; a woman wanted to know whether any legislation prohibited private sector employers from sending client data to the United States, and several callers were concerned about Statistics Canada asking "personal questions" for surveys about family finances and post secondary education.

Notifying the Commissioner

The *Privacy Act* defines two situations which require a government department to notify the Privacy Commissioner of actions they plan or have taken.

In the Public Interest

Section 8(2)(m) requires the department to notify the Commissioner of a release of 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."

Once he is notified, the Commissioner may advise the individual of the release if he considers that appropriate. He may also initiate his own complaint if he is not satisfied that the information was properly released.

The Commissioner received the following 18 notifications during the past year:

Department Information Released

Bank of Canada	-a deceased employee's projected earnings to widow's legal counsel to pursue claim against the bank
Correctional Service	-information about an inmate to legal counsel representing clients in a civil suit -location of two offenders to solicitors to arrange legal action against offenders

-parole status to inmate's wife because she was a victim of an offense for which the inmate was imprisoned

External Affairs

-collection of information about Canadians in country where Canada has no representation (notification not required)

International Development Research Centre

-fact that former employee's academic credentials false released to Public Service Commission and several other departments and non-government organizations

National Defence

-notice of imminent release of inmate of forces's prison sent to municipal police to protect inmate's brother whom he had threatened
-current addresses of service personnel holding Medic-Alert bracelets to Canadian Medic-Alert Foundation
-name of executrix of estate released to legal counsel of person with claim against estate

National Parole Board -citizens group denied information about inmates, only parole status released
 -parole status of inmate released to local media (case had received considerable local media coverage, much of the information available elsewhere)

-medical file of recently deceased man, to his daughter concerned about illnesses among other members of family
 -coroner's report to deceased man's sister to reassure that death was from natural causes.

“Consistent Use”

Public Archives -personal details about man alleged to be armed, holding hostages and threatening suicide, to RCMP
 -man's address and phone number to RCMP to find him and advise daughter in custody in U.S.

The *Privacy Act* permits a government institution to use personal information for a purpose “consistent” with the one for which it was originally gathered, providing that the department notifies the Privacy Commissioner “forthwith” and then ensures that the new use is described in the the next edition of the index. Individuals may complain to the Privacy Commissioner if they find their personal information is being used for a purpose not described in the Personal Information Index.

RCMP -material to librarian/ researcher writing book about man dead more than 20 years (notification not required)
 -information about a candidate for an order in council appointment to Veterans' Affairs

Four departments notified the Commissioner about consistent uses during the year.

Veterans' Affairs -information about man to step-son to apply for survivor's benefits
 -to estate officer to verify status of deceased and his heirs

1. The Treasury Board released the comparative ratings and answer sheets of four candidates to a Public Service Staff Relations Board hearing into a competition being appealed by one of the candidates.
2. The RCMP advised the Commissioner of new uses for information in two of its banks. RCMP-P10 (Criminal History Records) is used by the Insurance Crime Prevention Bureaux to combat arson, and RCMP-P20 (Operational Case Records) is used by federal departmental security officers for security and reliability screenings. These new uses will appear in the next edition of the index.

-
-
3. Employment and Immigration Canada told the Commissioner it intends using its personal information banks for internal audit purposes and will make this use clear in the next edition of the index.
 4. The Secretary of State advised that applications for and proof of Canadian citizenship in Bank SS-P70, (Application and Assessment for Canadian Citizenship), are now shared with the Canadian Security Intelligence Service for purposes of administering the *Citizenship Act and Regulations*. (They were already shared with the RCMP).

The Commissioner noted that there were several new uses for information listed in the 1984 edition of the index of which he had not been notified. His staff will question departments about the lack of notification as they investigate information banks.

Compliance Branch

The Privacy Commissioner ensures that the federal government exercises fair information practices when it collects, uses, retains and disposes of personal information. This day-to-day responsibility is carried out by the Compliance Branch.

This responsibility demanded that the branch develop expertise, methodology and staff before beginning any effective investigation of the government's complex records system. It also had to establish priorities and the resources needed to monitor some 140 government institutions which maintain about 2,200 personal information banks governed by the *Privacy Act*.

The Commissioner and his staff consulted experts in general auditing procedures, security of record-keeping systems, statistical analysis and data program evaluation. Recognizing an audit role similar to that of some European data commissioners who have had much experience in this field, the Commissioner drew on the expertise of the office of the Federal Data Protection Commissioner of the Federal Republic of Germany whose representative spent five days in Ottawa at the invitation of the Compliance Branch. While his advice helped develop the branch's methodology both priorities and methodology may need refining as experience is gained from on-site investigations.

Watching the Index

The Commissioner keeps a watching brief on the accuracy and completeness of the Personal Information Index, which is the individual's tool for access to personal information. Following inquiries, the Compliance Branch recommended several new information banks and foresees recommending the removal of listings which contain information no longer required, and the improvement of some banks' descriptions.

A routine comparison of the 1983 and 1984 editions of the Index, showed that 49 banks listed in 1983 were dropped from the 1984 edition. Explanations revealed that in all but three cases the banks were dropped because departmental programs had been amalgamated, discontinued or the information was anonymous statistical data. However, three banks omitted by oversight were: Canadian Security Intelligence Service, formerly RCMP bank P130 — (Security Service Records); Department of National Defence, ND-P-P430 (Personnel Security Investigation File); Department of Labour, LAB P-110 (Labour Adjustments Benefit Program). The Compliance Branch notified Treasury Board, which was aware of two of the omissions.

Many departments hold personal information not used for administrative purposes or not organized for retrieval by name. The *Privacy Act* gives individuals the right to access this information if they can supply enough detail to permit it to be found. Not all departments mention their inventories of this type of information in the index, an oversight which should be corrected.

The Personal Information Index has two sections, one containing listings for the public, and the second containing banks of federal employees. Without addressing the somewhat academic question of what constitutes an employee, the Compliance Branch found banks listed in the general public section which might better be in the employee section. Such banks concern individuals on contract, under appointment, or those who provide the government with functions or services without coming under the *Public Service Employment Act*.

Compliance Audits Begin

History was made in late 1984 when privacy investigators began the office's first compliance investigation at the Department of Fisheries and Oceans, the Canadian

Saltfish Corporation and the Freshwater Fish Marketing Corporation. Final reports had not been sent to the agencies, selected for their modest size, by the end of the reporting year.

Other smaller government agencies visited by investigators during the past year included the Canadian Commercial Corporation, Canada Deposit Insurance Corporation, Canadian Patents and Development Limited, Canadian Import Tribunal (formerly the Anti-Dumping Tribunal), Foreign Investment Review Agency (Investment Canada), National Energy Board and the Standards Council of Canada.

None of these institutions have information banks concerning the public listed in the Personal Information Index and have had few or no exchanges with the Privacy Commissioner's office. The Standards Council and Canada Deposit Insurance Corporation agreed that they have programs which generate a minimal amount of personal information and officials assured investigators that such information will be listed in the next edition of the Index.

The Privacy Commissioner is empowered to examine the files in 20 personal information banks which the Governor in Council has designated as exempt from the general right of access. In April the branch began to investigate two closed Employment and Immigration banks: Immigration Security and Intelligence Data Bank, EIC-P430, and Enforcement Information Index, EIC-P440.

The experience from actual investigations may lead to new investigatory approaches. For example, it may be more effective to investigate an issue government-wide than conducting investigations department by department.

Other Issues

During the year other issues concerning the government's treatment of personal information were brought to the Privacy Commissioner's attention and some required investigation. One such issue concerned a report that Revenue Canada, Taxation, gave SIN numbers to some credit bureaus during income tax investigations. The investigation found that the credit bureaus already have the SIN numbers and by comparing numbers Revenue Canada ensured investigation of the correct individuals.

Another investigation concerned a traveller's contention that Revenue Canada customs declaration forms unnecessarily asked for the claimant's birthdate. It was found that the department asks for the information to identify the proper claimant and to ensure that under-age individuals do not import alcohol or tobacco. This investigation did, however, raise the broader question of whether all government forms should explain why personal information is being collected. Although not required by the *Privacy Act*, the explanation would allay people's fears and perhaps eliminate some complaints. The Commissioner was pleased to learn that Treasury Board is considering this possibility.

During the past year the Compliance Branch responded to requests for advice about sections of the Act dealing with the use, collection and disposal of personal information. For example, staff helped a policy consultant to the government's Affirmative Action program determine the *Privacy Act's* impact on the program. These requests are rare because most agencies have their own privacy coordinators and legal counsel. The branch will, however, help where it can, without prejudicing its ability to investigate.

The Privacy Act in Court

The *Privacy Act* gives individuals the right to have the Federal Court review a department's denial of the information requested, providing that the Privacy Commissioner has investigated and reported on the complaint. The Privacy Commissioner is required to advise complainants of this right in his report.

It is important to underline that the Privacy Commissioner's finding is not reviewed because it is not a binding decision, only a recommendation.

The complainant should apply to the Federal Court within 45 days of receiving the Privacy Commissioner's report, although the court, at its discretion, may allow more time.

Since July 1, 1983, only five complainants have taken advantage of this right — perhaps an indication of the hope of the architects of the *Privacy Act* that the Privacy Commissioner would save excessive and expensive recourse to already over-burdened courts. The low number may also be an early sign that complainants have confidence in the independence and efficacy of the Privacy Commissioner's office, the reputation and integrity of which must be earned with every complaint.

A summary of the complaints which have gone for court review follows.

Luis Ernesto Reyes and the Secretary of State

Mr. Reyes, a Chilean refugee, was the first case heard under the *Privacy Act*. He had applied for personal information from the Secretary of State after his citizenship application was denied. He was refused the information under section 21 of the Act which prohibits the release of information which could endanger Canada's defence,

the conduct of its international affairs, or its efforts to detect hostile or subversive activities. The department later applied a second exemption (section 22) because release could be injurious to a lawful investigation or a Canadian law. After receiving a complaint from Mr. Reyes, the Privacy Commissioner examined the documents and concluded that the exemptions had been applied correctly. The Commissioner advised Mr. Reyes of his right to appeal and he did so in early 1984.

Associate Chief Justice James Jerome began the hearings by addressing the difficulties of inquiring into highly confidential matters while preserving the openness of the judicial system.

He said: "Proceedings in our courts must take place in full public view and in the presence of all parties. Exceptions to this principle...must be kept to the minimum of absolute necessity to safeguard the public interest in the administration of justice and the rights of any parties excluded from the proceedings".

Since the issue concerned confidential documents, Mr. Justice Jerome had to restrict attendance to the parties to the case, hold hearings *in camera* and much of it in the absence of the complainant and his counsel (*ex parte*). In addition he could not allow Mr. Reyes' lawyer to see the documents.

Mr. Justice Jerome concluded that the Secretary of State is obligated to conduct routine investigations to determine whether citizenship applicants meet the requirements of the *Citizenship Act*. He was satisfied that the department had applied the exemptions correctly.

Paul Copeland and the Solicitor General of Canada

Mr. Copeland, a Toronto lawyer, applied to see whatever information the RCMP had about him in its files. His 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. Mr. Copeland began action in the Federal Court but there were no hearings by the end of the reporting year.

Neil A. Davidson and the Solicitor General of Canada

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

Mr. Davidson complained to the Privacy Commissioner who confirmed 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 but hearings had not begun by the end of the reporting year.

Nicholas Ternette and the 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 has been closed by the Governor in Council. He complained to the Privacy Commissioner who examined the bank. While he could neither confirm nor deny that information existed, the Commissioner assured Mr. Ternette that he had not been denied a right under the *Privacy Act*. He advised the complainant of his right to apply to the court for a review.

In a preliminary hearing, the federal Department of Justice argued that the "review" envisaged by the *Privacy Act* confined the court to simply confirming that the bank in question was closed legally. The applicant maintained that the review was meant to permit the court to examine the files to determine whether they should be closed.

Mr. Justice Barry Strayer concluded that the court was empowered to determine whether a file is properly in a closed bank and ordered the Solicitor General to file an affidavit as to the existence or non-existence of a file, and if such a file existed, to attach it to the affidavit.

The Solicitor General appealed. Justice Minister John Crosbie announced in November, 1984, that the government was dropping the appeal because "the right of judicial review is an essential safeguard of individual rights under the *Privacy Act* and this right would not have meaning if the court were not empowered to examine records contained in exempt banks".

The Solicitor General complied with Justice Strayer's order and hearings are expected to begin in mid-1985.

Bernard Dufourd and The Office of the Privacy Commissioner of Canada

Mr. Dufourd applied for but was refused information about himself in three banks maintained by the Solicitor General of Canada and designated as closed by the Governor in Council. The Privacy Commissioner examined the files and dismissed Mr. Dufourd's subsequent complaint, finding that he had received everything to which he was entitled under the law.

Mr. Dufourd appealed the decision to the Federal Court. However, while the *Privacy Act* provides for a court review of a department's refusal to grant access, the Commissioner's decision is not challengeable in court. This was explained to the complainant and his action was withdrawn.

Corporate Management Branch

The Corporate Management Branch is a common service providing financial, personnel, administrative and public affairs support to both the Information and Privacy Commissioner's offices (see Appendix I for the organization chart.)

Personnel

Staffing of the organization to make it fully operational was a 1984-85 priority. Eleven investigators were appointed in the fall, 1984, including nine for Privacy and two for Information. The appointments followed a competition, launched in the spring of 1983, which entailed screening 644 applicants and conducting 61 interviews in seven cities across Canada. At the end of the reporting year, three appeals of these appointments were still outstanding.

Staff strength increased from 32 to 49 during the year. On March 31, 1985, there were 19 staff members in the Privacy Commissioner's office, 12 in the Information Commissioner's, and 18 in the Corporate Management Branch. A total of 42 person years was used against the 46 allocated in the 1984-85 estimates.

Office Automation

The offices obtained three personal computers for test purposes early in 1984. Following successful trials, an additional eight were purchased and are currently used for word processing, capturing and reporting complaints data, and statistical analysis. The equipment provides legal counsel, library and public affairs staff with access to outside data banks. Specialized software is being introduced for record keeping and cataloguing the library's growing collection.

Finance

The 1984/85 budget for the entire organization was \$2,908,000, including \$790,000 for the Information Commissioner, \$1,116,500 for the Privacy Commissioner, and \$1,001,500 for the Corporate Management Branch. Actual expenditures, shown in the table, reflect a lapse of \$500,093 largely attributable to staffing delays.

Public Affairs

Public Affairs provides both Commissioners with writing/editing, media and publication production services. During the year the office produced the final annual report of the Privacy Commissioner under Part IV of the *Canadian Human Rights Act*, separate annual reports for the Information and Privacy Commissioners, an indexed office consolidation of the *Privacy Act* and an explanatory leaflet on the Information Commissioner's role and procedures.

Expenditures

The following are the Offices' expenditures for the period April 1, 1984, to March 31, 1985.

	Information	Privacy	Administration	Total
Salaries	\$442,265	\$595,374	\$543,591	\$1,581,230
Employee benefit plan contributions	63,000	86,000	80,000	229,000
Transportation and communications	44,991	51,640	69,109	165,740
Information	32,296	41,341	6,032	79,669
*Professional and special services	49,725	122,529	60,058	232,312
Rentals	—	—	17,147	17,147
Purchased repair and maintenance	—	—	3,915	3,915
Utilities, material and supplies	—	—	35,218	35,218
Construction and equipment acquisition	—	—	61,245	61,245
All other	175	787	1,469	2,431
Total	\$632,452	\$897,671	\$877,784	\$2,407,907

*Includes the salaries of five contract investigators retained for part of the year.

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, 20 of the approximately 2,200 banks are closed. All are listed in the Index with descriptions of their contents.

They are:

- | | |
|----------------------|--|
| Canada Post | -Postal Related Crimes/Offenses (CP-P-130) |
| Correctional Service | -Preventive Security Records (CSC-P50)
-Institutional Security Threats Records (CSC-P70)
-Security Inquiries Records (CSC-P90) |

Employment and Immigration	-Enforcement Information Index System (EIC-P440) -Immigration Security and Intelligence Data Bank (EIC-P430)	-Police and Law Enforcement Records Relating to the Security and Safety of Persons and Property in Canada (SGC-P70) -Protection of Privacy (wiretapping as defined in s. 178.1 to 178.23 inclusive of the Criminal Code) (SGC-P80) -RCMP Operational Records (SGC-P110)
National Defence	-Military Police Investigation, Case Files (ND-P-P440) -Communications Security Establishment, Security and Intelligence Investigation Files (ND-P70)	
Revenue Canada	-Customs Intelligence Records (RC-CE-P40) -Tax Evasion Cases (RC-T-P60) -Tax Avoidance Cases (RC-T-P70)	Does this mean I may see everything else? 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 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"
Privy Council Office:	-Security and Intelligence Information Files (PCO-P10)	
RCMP:	-Criminal Operational Intelligence Records (RCMP-P120) -Security Service Records (RCMP-P130) (to be transferred to CSIS) -Protection of Personnel and Government Property (RCMP-P140)	
Solicitor General:	-Security Policy and Operational Records (SGC-P60) -Commissions of Inquiry (SGC-P120)	

- 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.

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

For a complete list of the institutions, see Appendix III.

Can others see my personal information?

The Act generally requires a government department to get 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.)

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

In writing, explain the error to the privacy coordinator at the institution holding the information, 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 do I do if I'm refused access?

If it is not clear to you why the government has refused your request, ask the appropriate privacy coordinator to explain the problem. Perhaps there has been a misunderstanding.

If, after talking to the coordinator, you still think you have been wrongly denied information, call or write the Privacy Commissioner's office at:

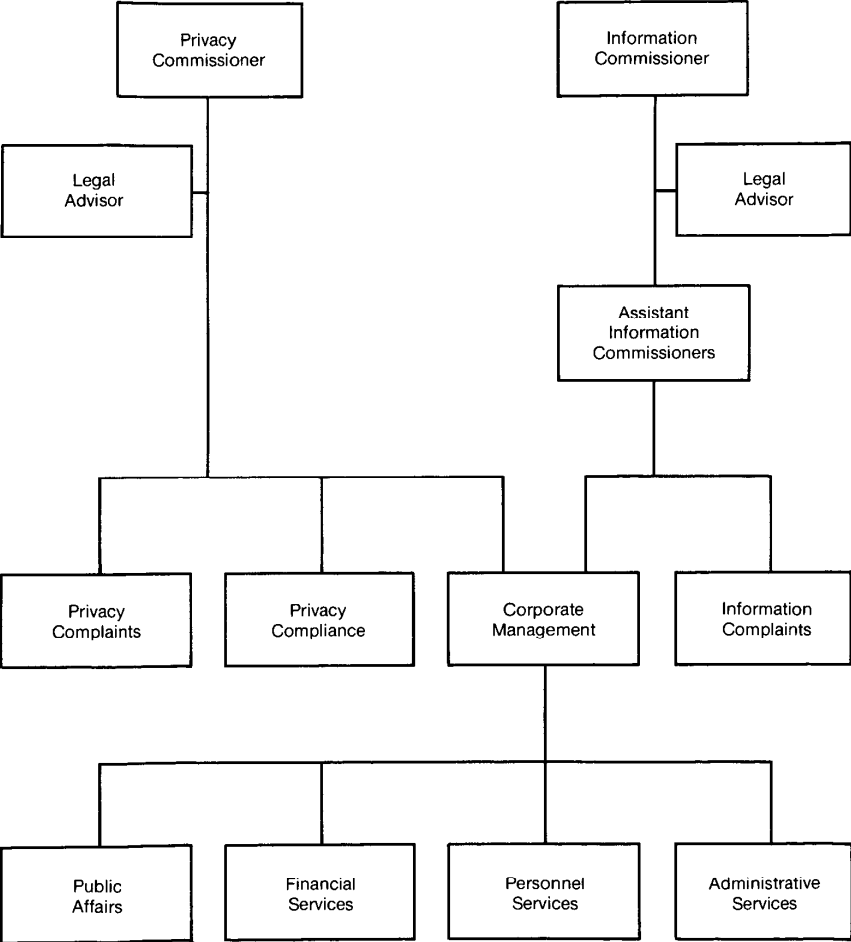
The Privacy Commissioner of Canada,
112 Kent Street, 14th Floor,
Ottawa, Ontario K1A 1H3
(613) 995-2410

Collect calls are accepted and the switchboard is open from 7:30 a.m. to 6 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. If you cannot identify the institution, you may seek the advice of the Privacy Commissioner at the address shown in the Index. 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 to 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 (83/2)

Appendix III

Government Institutions Covered by the Act

Departments and Ministries of State

Department of Agriculture

Department of Communications

Department of Consumer and Corporate
Affairs

Ministry of State for Economic and
Regional Development

Department of Employment and
Immigration

Department of Energy, Mines and
Resources

Department of the Environment

Department of External Affairs

Department of Finance

Department of Fisheries and Oceans

Department of Indian Affairs and
Northern Development

Department of Insurance

Department of Justice

Department of Labour

Department of National Defence
(including the Canadian Forces)

Department of National Health and
Welfare

Department of National Revenue

Department of Public Works

Department of Regional Industrial
Expansion

Ministry of State for Science and
Technology

Department of the Secretary of State

Ministry of State for Social
Development

Department of the Solicitor General

Department of Supply and Services

Department of Transport

Department of Veterans Affairs

Other Government Institutions

Advisory Council on the Status of
Women

Agricultural Products Board

Agricultural Stabilization Board

Atlantic Development Council

Atlantic Pilotage Authority

Atomic Energy Control Board

Bank of Canada

Bilingual Districts Advisory Board

Board of Trustees of the Queen
Elizabeth II Canadian Fund to
Aid in Research on the Diseases
of Children

Bureau of Pension Advocates

Canada Council

Canada Deposit Insurance Corporation

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
Canadian Commercial Corporation	Crown Assets Disposal Corporation
Canadian Cultural Property Export Review Board	Defence Construction (1951) Limited
Canadian Dairy Commission	The Director of Soldier Settlement
Canadian Film Development Corporation	The Director, The Veterans' Land Act
Canadian Government Specifications Board	Economic Council of Canada
Canadian Grain Commission	Energy Supplies Allocation Board
Canadian Human Rights Commission	Export Development Corporation
Canadian Import Tribunal	Farm Credit Corporation
Canadian Institute for International Peace and Security	Federal Business Development Bank
Canadian International Development Agency	Federal Mortgage Exchange Corporation
Canadian Livestock Feed Board	Federal-Provincial Relations Office
Canadian Patents and Development Limited	Fisheries Prices Support Board
Canadian Penitentiary Service	The Fisheries Research Board of Canada
	Foreign Investment Review Agency
	Freshwater Fish Marketing Corporation
	Grain Transportation Agency Administrator
	Great Lakes Pilotage Authority, Ltd.

Historic Sites and Monuments Board of Canada	Natural Sciences and Engineering Research Council
Immigration Appeal Board	Northern Canada Power Commission
International Development Research Centre	Northern Pipeline Agency
Jacques Cartier and Champlain Bridges Incorporated	Northwest Territories Water Board
Laurentian Pilotage Authority	Office of the Auditor General
Law Reform Commission of Canada	Office of the Chief Electoral Officer
Medical Research Council	Office of the Commissioner of Official Languages
Merchant Seamen Compensation Board	Office of the Comptroller General
Metric Commission	Office of the Coordinator, Status of Women
National Arts Centre Corporation	Office of the Correctional Investigator
The National Battlefields Commission	Office of the Custodian of Enemy Property
National Capital Commission	Pacific Pilotage Authority
National Design Council	Pension Appeals Board
National Energy Board	Pension Review Board
National Farm Products Marketing Council	Petroleum Compensation Board
National Film Board	Petroleum Monitoring Agency
National Library	Prairie Farm Assistance Administration
National Museums of Canada	Prairie Farm Rehabilitation Administration
National Parole Board	Privy Council Office
National Parole Service	Public Archives
National Research Council of Canada	Public Service Commission
	Public Service Staff Relations Board

Public Works Land Company Limited
Regional Development Incentives Board
Restrictive Trade Practices Commission
Royal Canadian Mint
Royal Canadian Mounted Police
The St. Lawrence Seaway Authority
Science Council of Canada
The Seaway International Bridge
Corporation, Ltd.
Social Sciences and Humanities Research
Council
Standards Council of Canada
Statistics Canada
Statute Revision Commission
Tariff Board
Tax Review Board
Textile and Clothing Board
Treasury Board Secretariat
Uranium Canada, Limited
War Veterans Allowance Board
Yukon Territory Water Board