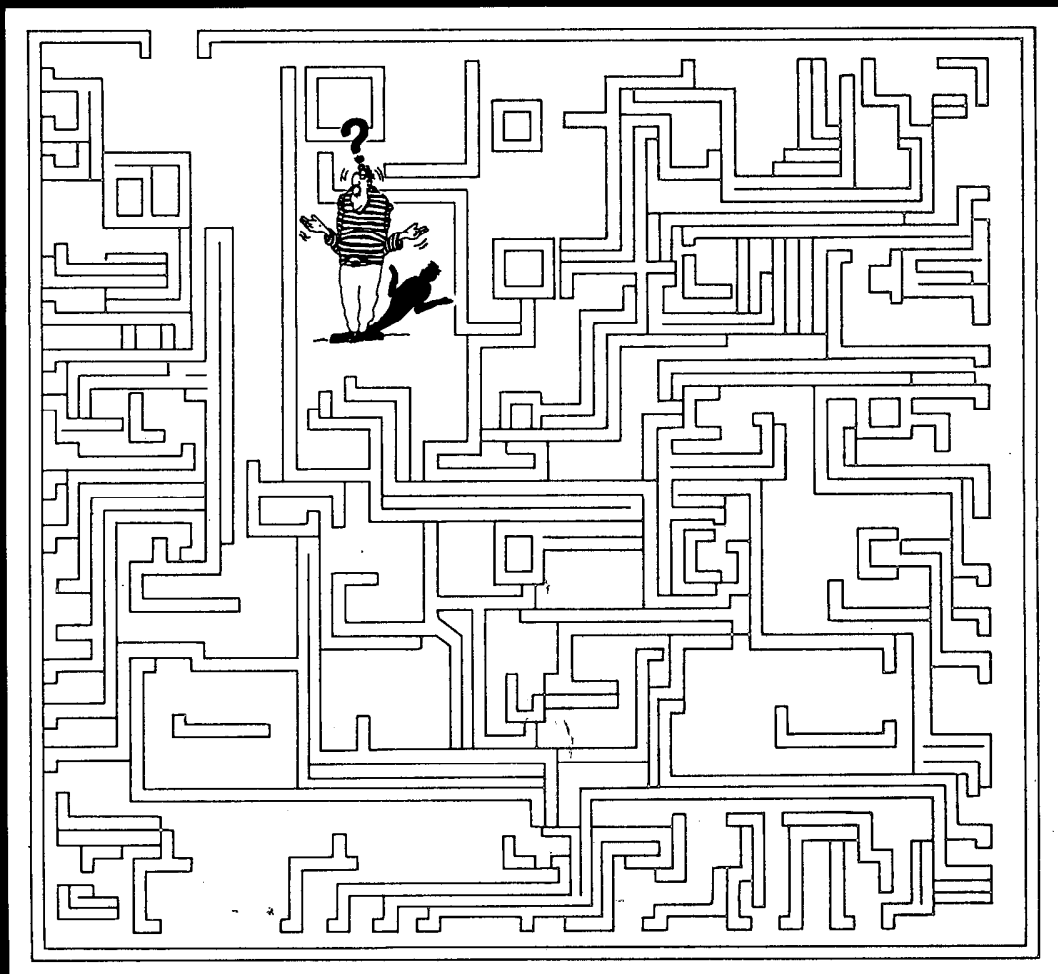


# Annual Report Privacy Commissioner 1986-87



---

---

**Annual Report  
Privacy Commissioner  
1986-87**



---

---

**The Privacy Commissioner of Canada  
112 Kent Street  
Ottawa, Ontario  
K1A 1H3  
(613) 995-2410, 1-800-267-0441**

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

**© Minister of Supply and Services Canada 1987**

**Cat. No. IP30-1/ 1987**

**ISBN 0-662-55287-3**

---

---

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

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

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

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

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

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

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

The *Privacy Act*

---

---

---

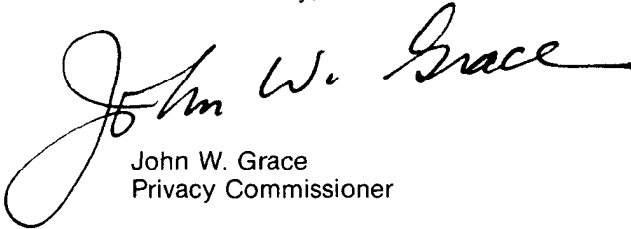
The Honourable Guy Charbonneau  
The Speaker  
The Senate  
Ottawa

June 30, 1987

Dear Mr. Charbonneau:

I have the honour to submit to Parliament my annual report. This report covers the period from April 1, 1986, to March 31, 1987.

Yours sincerely,

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

John W. Grace  
Privacy Commissioner

---

---

---

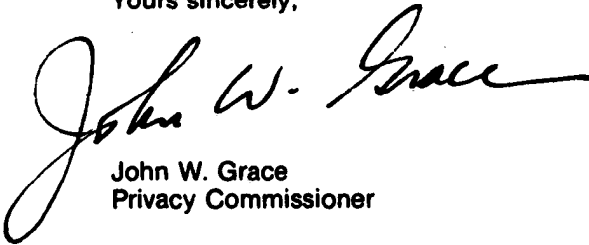
The Honourable J. Fraser, P.C., Q.C., M.P.  
The Speaker  
The House of Commons  
Ottawa

June 30, 1987

Dear Mr. Fraser:

I have the honour to submit to Parliament my annual report. This report covers the period from April 1, 1986, to March 31, 1987.

Yours sincerely,



John W. Grace  
Privacy Commissioner

---

# Contents

---

Mandate .....	1
Clouds With Silver Linings .....	2
Did the Country Lose its Wallet? .....	8
Completed census forms fall of Winnipeg truck .....	8
Parole Board files stolen from car .....	9
Staff records on Ottawa street .....	10
The Toronto microfiche incident .....	10
The Saskatoon incident .....	12
Veterans' microfiche lost in the mail .....	14
Passports "lost in mail" .....	15
EIC microfiche in BC dump .....	16
MP finds surveys on street .....	19
Post script: EIC's unemployment insurance survey .....	19
SIN—the Continuing Issue .....	20
SINs on envelopes .....	21
On Old Age Security Cheques .....	21
SINs to Cash Money Orders .....	22
And Pick Up Registered Mail .....	22
Fund Drives and Payroll Deductions .....	22
And Now The Bad News .....	22
Exempt Banks .....	24
Parolees and Inmates .....	26
Timely Access .....	26
Information to Third Parties .....	26
Confidentiality of Inmate Correspondence .....	27
Personal Information and Public Servants .....	28
The Conflict of Interest Code .....	29
Consulting the Privacy Commissioner .....	31
The New Security Policy .....	31
Employment Equity Act .....	32
Commissions of Inquiry .....	33
Notifying the Commissioner .....	35
In the Public Interest .....	35
Consistent Uses .....	38
Complaints Branch .....	40
Compliance Branch .....	49
Analyzing the Audit Population .....	49
Outside the Plan .....	49
The Privacy Act in Court .....	51
Corporate Management .....	52
Inquiries .....	54
Spreading the Word .....	55
Appendices	
I Organization Chart .....	56
II Information Request Form .....	57
III Government Institutions Covered by the Act .....	58

---

---

## Mandate

---

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

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

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

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

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

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

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



---

## Clouds With Silver Linings

---

It was the worst and the best of times for privacy protection. The theft of the personal information of 16 million taxpayers from a government office — the Chernobyl of privacy disasters — by itself makes it the worst year. Add a copycat incident at another office; passports missing in the mail, microfiche containing thousands of veterans' records not reaching their destination; microfiche holding sensitive personal information (were microfiche ever so famous?) turning up in a garbage dump; boxes of census forms falling off a truck; government employees' personal information blowing down a city street.

These are not the incidents to warm a privacy commissioner's heart. On such evidence alone, the privacy state of the nation would appear perilous.

And yet...

The past year certainly cannot be the first time in Canadian history when personal records were lost, whether massively or on a lesser scale.

The difference today is that such events are becoming both public and matters of public concern, - and that is encouraging, if in a bizarre way.

In two cases, cabinet ministers admirably reported such incidents directly to Parliament. The Privacy Commissioner is now being notified of lost records out of a sense of moral responsibility, rather than any narrow legal requirements of the *Privacy Act*.

Depressing though it may be, the catalogue of missing files should not necessarily be taken as a sudden new sloppiness about or indifference to personal information protection. Quite the contrary. An increasing awareness of and sensitivity to the *Privacy Act* may be the more compelling explanation for the new compulsion to Parliamentary and public confession.

Now the media is on the alert, vigilant to the news potential of meandering microfiche, disappearing data or suspicious surveys. Incidents which might have gone unreported previously and never seen the light of day are being brought to the public's attention.

Even if more incidents of lost or missing personal information continue to surface, despair should not be the reaction.

The worst possible result of the privacy horror stories of the past year would be a widespread public attitude that it is impossible to have effective protection of personal information in the custody of the federal government. Such an attitude is not justified.

Nor is it justified to expect absolute privacy protection. Like absolute anything in this world, absolute privacy protection is not possible. Even a security system which can stop the most clever hacker is vulnerable to someone's breach of trust. But it is entirely reasonable to expect that personal information entrusted to government (or any public or private entity) is not subject to carelessness or to easy malicious, mischievous abuse.

Unfortunately, some of the evidence of the past year indicates that such a reasonable assumption is not yet always possible.

---

There is another "And yet..." to be entered in the face of the discouraging breaches of privacy.

It is that public consciousness of personal privacy danger in the age of microfiche, microforms and micro-computers is raised more by one horror story than it is through a thousand speeches or, annual reports.

News of missing files has made the *Privacy Act* newly relevant and urgent. No longer do advocates of rules and legislation for protecting personal information need to be defensive about their mission. The danger is now demonstrable, not merely hypothetical. Privacy disasters have created a fresh national awareness of the vulnerability of stored personal information and, even, to the existence of something called the *Privacy Act*.

None of this, of course, is to make the case that a privacy Chernobyl is somehow to be welcomed. It is simply to say that even out of the worst of times for privacy should come something of value.

But "the best of times"? Isn't the contradiction too logic-defying to be sustained even as a literary device? Perhaps not.

In three years the *Privacy Act* has made a profound impact upon the 147 institutions of the federal government which must respect its provisions. No longer is it necessary to "sell" to the Public Service the concept of privacy as an important human value and the *Privacy Act* as an indispensable instrument.

Public servants as a whole have come to accept the protection of personal information as an integral part of doing business. They now live more comfortably with the *Privacy Act*. Privacy investigators receive few arguments over principles. Discussions are over interpretation and often honourable persons can differ, so complex some cases may be.

These generalizations could have been made had a single microfiche not strayed.

Though the job of consciousness-raising is never finished, three years of implementing the *Privacy Act* have left an indelible mark. After more than 120,000 privacy requests and 1,200 complaints, after the missionary work of many privacy coordinators, the importance of privacy has been all but universally recognized in the minds of senior public service managers. It is perhaps the major achievement of the first three years.

It means that the focus now shifts from selling to managing privacy; from investigating specific complaints to the comprehensive audits of information holdings of government institutions for general compliance with the principles of fair information practice as set forth in the *Privacy Act*.

Complaints from individuals will continue to be both encouraged and investigated with vigor. However, the object of the whole exercise is to build in an irreversible, systemic adherence to the principles of fair information practices so that the number of complaints will drop.

---

Managing privacy means proceeding in an orderly way with systematic examinations or audits of the personal information handling practices of government institutions. Each federal institution under the jurisdiction of the *Privacy Act* has now been analyzed from the point of view of the relative risk of the personal information under its control to breaches of the data protection principles of the legislation.

Above all, the year has been a special time because the Justice and Solicitor General Committee completed its review of the operation of the *Privacy Act* and published a report called: '*Open and Shut: Enhancing the Right to Know and the Right to Privacy*'. The apt oxymoron sums up the inherent contradictions and tensions. The Standing Committee's report was tabled in the House of Commons on March 31, which happens to be the last day of the Privacy Commissioner's reporting year.

The review made parliamentary history, being the first time that such a task was carried out in response to such a statutory requirement. Subsection 75(2) provides that the Committee designated or established by Parliament...shall, within three years of the coming into force of this Act, undertake a comprehensive review of the provisions and operations of this Act".

The Privacy Commissioner participated actively in the review, submitting a written response to both the issues and questions raised by the Committee, as well as appearing as a witness on May 13, 1986. In fact, last year's annual report contained the main body of the Privacy Commissioner's brief to the Committee.

It is neither possible nor prudent to pass judgment here upon each of the Committee's 108 recommendations touching upon the *Privacy Act*. After study, precise and detailed responses will be made to MPs and government. Should legislative amendments to the *Privacy Act* proceed, and that is certainly the Privacy Commissioner's hope and recommendation, there will be formal opportunities to make views known about changes. Committees may propose; Parliament still disposes.

But let this be said in immediate and general reaction to the Committee members' work: theirs is a report of remarkable sweep, important both for what it proposes to change and what it leaves alone. If implemented, the Committee's recommendations would enhance significantly the quality of personal data protection in this country. The report is a unanimous affirmation of the conviction that private lives, if they are to have reasonable assurance of privacy, now require broader public laws. It is a report which responded alertly and specifically to the developing privacy issues of the day; it is a report which makes thoughtful suggestions for improvements to the *Privacy Act* three years on.

Yet, for all the constructive and busy recommendations, the principles of fair information practices which form the philosophical core of the legislation have been tested and upheld. The delicate balance built into the Act, the balance between individual and public good, is left unchanged.

---

In keeping the balance, the Committee has concluded, implicitly that the police chiefs and the civil libertarians were both wrong in their initial criticism. The law has not made life any easier for criminals: informants did not stop coming forward for fear of exposure because of privacy legislation. The exceptions to the right of access to one's personal information for carefully defined reasons do not make a mockery of the general principle.

In some ways, the most significant conclusion of the Committee review is one which does not find its way into any of those 108 recommendations. It is this: Parliament had the basics and the balance right the first time: Should all the recommendations be accepted, turned into amendments and passed by Parliament, the essentials of the present *Privacy Act* would remain untouched. It is reassuring that after an intensive Parliamentary review, the *Privacy Act* is in fact confirmed. That should be kept in mind even as attention turns in the days ahead to improving the legislation.

The most far-reaching of the Committee's recommendations is the proposed extension of the jurisdiction of an amended *Privacy Act*. In calling for an expansion of the territory (if not the empire!) covered by the legislation to include the federally-regulated private sector, the Committee pushed privacy further than even the Privacy Commissioner had advocated.

Such a political will to uphold, to say nothing of extending, privacy protection principles is not much evident these days in governments of other countries. In the United States, no significant amendments to existing laws are in sight. The few legislators who have interest in the subject work without party or government encouragement. In Western Europe, second generation privacy laws are not being examined and pushed ahead. Data protectors report they are discouraged at both the lack of support for their efforts and by trends which put mere efficiency before privacy.

The Canadian Privacy Commissioner does not have such a reason for discouragement, and not only because of the Justice and Solicitor General Committee's report. Senior public service managers and their privacy coordinators continue to deepen their commitment to the letter and spirit of the *Privacy Act*. And perhaps most significant of all, in their thousands of requests for their own personal information, and in a widely shared concern over the protection of their information, Canadians have demonstrated their reliance upon the *Privacy Act*.

A cautionary note should be sounded in the overture of praise for *Open and Shut*. It is that extending the reach of the *Privacy Act* and discharging all the other new responsibilities which the Committee proposes to be given to the Privacy Commissioner's Office is at least as daunting as it is a vote of confidence.

---

It is much too soon to estimate, with any useful precision, resource increases which would be necessary to carry out a greatly expanded mandate. A quick estimate, however, is that the doubling of financial and human resources would be required at the outset.

The quality of privacy protection now in place should not be diminished by re-directing already strained resources to respond to new responsibilities, however exciting and important.

For example, bringing all Crown Corporations under the *Privacy Act* would be, by itself, beyond the Privacy Commissioner's existing resources. Adding the federally regulated private sector, as the review Committee has proposed, presents an additional challenge which simply cannot be calculated.

Even if generous additional resources were at once forthcoming, recruiting and staffing would require perhaps a year's lead-time before the Privacy Commissioner would be in a position to handle the new load.

This, too, must be said, perhaps more with a sense of nostalgia than realism, that it will be a matter of regret to move at once from a present staff of 20 to one of 40 and, perhaps soon afterwards, to 50 or more. If implementing privacy values requires an ever-burgeoning bureaucracy, the attractive virtues of a small operation are lost. One of the most persuasive arguments in selling privacy protection to Canadians has been that the cost is small.

The Committee's report recognizes the need for additional staff. But nothing is quantified and the quick impression is that the increase may be much more than the Committee may have realized.

No matter how good the cause and reasonable the case for extending the *Privacy Act's* jurisdiction, the perception would be all wrong if the Privacy Commissioner were seen to be an empire-builder. Another good cause, that of ombudsman, has been damaged in this country and elsewhere by incumbents who grew too large, or too lavish or who pushed their claims too far.

Thus, an expanded mandate from Parliament should take effect in careful, incremental stages.

These cautionary words provide only a context in which the work of examining and implementing the Parliamentary Committee's report should proceed. The energy, intelligence and momentum which that report presents should be translated into important changes in the law. If this Committee's distinguished work is allowed to languish, it would be a dismal precedent.

### **A Different Report**

The review of the Justice and Solicitor General Committee controlled the year's discussion agenda of privacy issues. Matters which have been raised in the previous three of these annual reports, from computer-matching to exempt banks, to transborder data flow - and more - have now also had the benefit of the Committee's examination and recommendations.

The report of that examination has been given to Parliament and it would be redundant at the least to cover the same ground here. The Committee has given Parliament the authoritative last word this year on the main privacy issues of the day.

---

---

As a result, this annual report consists mainly of an accounting of the year's activities of the Privacy Commissioner's Office. These activities divide into two large categories:

First, investigations made in response to an increased number of complaints from individuals;

Second, investigations initiated by this office into how government institutions were handling personal information.

Issues have become more various and more complex. The reports which follow speak for themselves.

---

## Did the Country Lose its Wallet?

---

As one journalist put it, this was the year the country "lost its wallet". In what appeared to be a litany of lost, stolen, spilled and trashed personal documents, Canadians gradually awoke to just how much the government knows about them, and how carefully it is guarding their secrets.

Over the past year, the Privacy Commissioner inquired into 12 incidents involving the theft or loss of personal information held by government. These do not represent all the cases in which personal information was compromised. The *Privacy Act* does not require departments to notify the Commissioner when personal information is lost or stolen. The Commissioner learned of the incidents either through the courtesy of departmental officials, by media reports or as a result of discovery by the Commissioner's staff.

While he appreciates the cooperation extended by Revenue Canada, Employment and Immigration Canada and the National Parole Board, the Commissioner recommends that the government's new security policy be amended to require government institutions to notify formally and immediately the Commissioner of any unauthorized disclosure of personal information.

### **July — Completed census forms fall off Winnipeg truck**

On July 15, 1986, a *Winnipeg Free Press* reporter told the Privacy Commissioner that two boxes of completed census forms had fallen off the back of a truck en route to the census processing centre. The driver did not notice the loss immediately and delivered the depleted load to the centre where an employee signed for it as being in good order.

Returning by the same route, the driver stopped to investigate papers blowing around the street. He found they were census forms from his truck and, with the help of pedestrians and the staff of a nearby McDonald's, retrieved as many as possible and took them to the centre.

Meanwhile, centre staff had realized that two boxes were missing and alerted the local census office. The manager organized a search-and-rescue operation; six staff members were dispatched to scour the area and go door-to-door, leaving their names and phone numbers so residents could call should forms be found.

The combined searches recovered 339 intact forms. However, 26 forms were lost entirely and four were found with pages missing. A detailed long form was among the documents lost entirely.

The Commissioner concluded that the loss of the boxes was a preventable accident. Statistics Canada had not provided adequate protection for the census forms. Shipping directives for completed census forms were inadequate. A directive requires staff to "investigate the availability of steel cages with bonded carriers in the area", but does not require their use, nor does it prohibit the use of open trucks.

The Commissioner recommended that Statistics Canada amend its directives to require shipment in closed, locked trucks and/or steel cages, and that there be written contracts with shipping companies, setting out these security requirements.

---

He also asked Statistics Canada to advise those whose forms were lost or compromised of their right to complain to the Privacy Commissioner. Statistics Canada replied that it had already spoken to representatives of all households whose questionnaires had been lost or destroyed, and apologized for the incident.

### **October — Parole Board files stolen from car**

Early in November, National Parole Board (NPB) staff called to notify the Commissioner that some personal files had gone temporarily astray. On October 23, the parked car of an NPB member was broken into on a Montreal street. The stolen items included a briefcase containing file resumés on nine inmates whose parole was being considered. The files contained institutional reports, criminal records, psychiatric records, community assessments and various other reports.

The next morning a restaurant manager found the files — minus the briefcase — in his parking lot. The parole board member's business card was among the documents and the manager called the local parole board office about his find.

The investigation found that the briefcase had been left on the back seat of the car and covered by the member's personal belongings. When the owner discovered his car had been broken into and the briefcase and his personal belongings stolen, he notified the police.

Privacy investigators examined the recovered files and nothing appeared missing; no staples had been removed or replaced. Given the condition of documents, and the speed with which they were found, there was nothing to suggest that copies had been made.

The investigation found the parole board had no written policy on handling resumés compiled for parole hearings, although there was a general directive on handling operation case files, the complete files from which resumés are extracted. The confidential case files were not to be removed from the office; but the resumés were unclassified.

Though the board briefed its members on security, it relied primarily "on common sense" rather than written policies.

As a result of the investigation, the Commissioner concluded that the regional office staff knew little about the *Privacy Act* and its requirement to protect personal information from unauthorized disclosures; that there were no specific policies about handling the type of documents stolen; that the member had not protected the documents adequately, and that the inmates' confidentiality had been compromised.

He recommended that the board set out clearly defined procedures for handling personal information, regardless of its classification, and issue these to all officials and regional offices. He also asked the board to make its staff, and particularly the board members, better aware of the *Privacy Act*.



---

Since this incident, the board has tightened its procedures for handling both case files and the extracts for board members. It organized a training session for board members on protection of personal information and the *Privacy Act*, issued a directive to all staff, and is developing a training package on the *Privacy Act* for staff and board members.

### **November — Staff records on Ottawa street**

On November 7, one of the Commissioner's staff found personnel information listings from the Department of Regional and Industrial Expansion (DRIE) scattered along Wellington Street. The documents contained employees' home addresses, phone numbers and, in one case, the social insurance number.

The forms had apparently fallen from a truck transporting waste to a garbage dump. The Commissioner notified DRIE that he was investigating the incident and asked the department to keep the forms for his investigation.

That investigation found that DRIE's financial staff had reviewed the internal forms and set two boxes aside, clearly marking them for classified waste disposal. Cleaning staff, later removing debris from a nearby renovation project, picked up the two boxes and included them for delivery to the dump.

DRIE staff was unable to determine the number of forms spilled, recovered and still missing. They did not catalogue the recovered material, and on or about November 12, these documents were destroyed after investigators examined them, but before the investigation was finished.

Following the investigation, DRIE's security manager reminded financial staff about procedures for classified waste disposal and issued a department-wide memo about protection and disposal of personal information. DRIE also determined that the staff listing form did not need employees' home addresses and phone numbers. The form will be revised.

The Commissioner asked that he be told of any such future loss or compromise of personal information and he reminded DRIE that found documents must be retained for his investigation and so that he may notify the individuals if he considers it appropriate. He could not notify anyone in this case because the documents had been destroyed.

### **November — The Toronto incident**

On November 17, the Minister of National Revenue informed the House of Commons that a set of microfiche records "containing information on some 16 million Canadian taxpayers was missing".

The Minister was told on November 4 that the records had been lost from the Toronto District Tax Office at 36 Adelaide Street after working hours October 30. The following day he advised the RCMP Commissioner who immediately launched an investigation. Revenue Canada and the RCMP agreed not to reveal the loss and subsequent investigation until both were certain that public disclosure would not compromise the investigation.

---

On Friday, November 14 the Deputy Minister of Revenue Canada/Taxation advised the Privacy Commissioner of the loss. Early the following Monday, the Privacy Commissioner informed Revenue Canada that he would investigate the incident.

The next day (November 18) a lawyer representing a Revenue Canada employee turned over to the RCMP in Toronto what appeared to be the missing set of microfiche.

### **The investigation**

The lost microfiche set, called T1 Alpha, contained names, addresses, birthdates, spouses' names, social insurance numbers, nearest district tax offices, last tax filing year, and a code which broadly describes the taxpayer's principal income source.

Prior to the incident, microform sets were stored in unlocked cabinets in the Identification and Compliance Section (IC). All microfiche held in that section were kept in the same room, unlocked and unsupervised during working hours. All section staff had access; staff from other sections had access simply by signing a log maintained by the receptionist, which showed dates but no times. The room was locked after working hours but opened for cleaners accompanied by a commissioner.

The Privacy Commissioner's investigators also examined microfiche procedures in the Initial Assessing Section (IAS) on the second floor of the 36 Adelaide Street office. The employee charged with theft of the set worked here. Here too the microfiche were open on a desk

during working hours, accessible to all section staff in the open-concept office, and to Collections Section staff on the same floor. No record was kept of their use.

The department did not require employee reliability checks.

### **Conclusions**

The T1 Alpha set was removed from the IC section when the room was unlocked for the cleaners. It had been left in a tray on the top of a cabinet.

Failing to lock the microfiche in a cabinet jeopardized the security of the information, as did opening secured areas outside working hours for cleaning staff.

Employee access and record verification controls were inadequate. Microfiche were at risk because:

- \* Revenue Canada staff was allowed to examine the microfiche, or any other record on the 16th floor simply by signing the register;
- \* staff were bypassing security controls on their own sets by examining the IC set;
- \* there were inadequate controls on the individual sheets within the sets;
- \* staff was allowed to override the security procedures in the department's own manual which restricts access to tax sensitive information to authorized personnel staff on a job-related, need-to-know basis.

---

The failure to verify adequately employees' reliability put personal information at risk.

There was no evidence that the stolen microfiche had been used to cause harm to anyone and no evidence to indicate that the information was used to obtain unauthorized access to other personal information.

### **Recommendations:**

- \* that Revenue Canada ensure that all employees working with microforms are made aware of the particular vulnerability of information in this format;
- \* that the department amend its security manual to include additional protective measures;
- \* that the department distribute copies of departmental procedures about microform protection to all employees who handle and control them;
- \* that Revenue Canada ensure that new systems provide a record of individuals who have used the material.
- \* that employees with access to microfiche containing personal information be subject to the enhanced reliability checks described in the government's security policy.

In mid-April, Minister of National Revenue Elmer MacKay responded to each of the Commissioner's recommendations. The actions he said had been taken, or would be taken, respond fully to the Commissioner's concerns. To reveal some of the specific recommendations for improving security procedures would compromise their effectiveness.

### **The Saskatoon Incident**

On or about December 22, portions of a microfiche sheet from the Saskatoon office of Revenue Canada, Customs and Excise (RCCE) were sent anonymously to the Saskatoon offices of the RCMP, the CBC, and the *Star-Phoenix* newspaper. Following media reports of the matter, the Privacy Commissioner expanded his investigation of the Toronto incident to include the one in Saskatoon.

### **The Investigation**

The microfiche in question was a defective part-fiche that had been sent to the Saskatoon office from headquarters in Ottawa. It contained information about Westerners who receive federal fuel tax rebates. The defective fiche was apparently stolen and cut into pieces, which were sent to the Saskatoon offices of the RCMP, the CBC, and the *Star-Phoenix*. The individual charged with the theft refused to make any statement and a search of his home failed to locate any microfiche.

There have been no known previous occasions when the Saskatoon office had received a damaged part-fiche. In this case copies of the same defective fiche were also received by offices in Winnipeg, Thunder Bay and Regina. Those copies have all been accounted for.

The Commissioner's investigation found there were no specific written procedures in the Saskatoon office for the storage, handling, or control of the microfiche. Personnel were told to treat microfiche as "confidential/protected". Following the incident the office placed tight control on the records, but found this interfered with operations as the fiche are used frequently by the eight auditors in the office.

---

Procedures now require that the fiche be kept in full view during working hours and locked in a cabinet during breaks and quiet hours. One person has been given responsibility for their custody.

Investigators found that during the seven years the office has been at 601 Federal Building, there has been no security survey or inspection. Although there is a departmental security manual (C&E Administrative Management Manual 1982) in the office, it is not used.

Since 1984 the office has hired eight persons locally, including the person charged. The district manager said that in each case staff had verified previous employment and reliability by phoning past employers. All new employees are required to take the standard public service oath or affirmation of office and secrecy. However, the office had not conducted reliability checks as prescribed by the government security policy of June 18, 1986.

## Conclusions

Although staff members were unfamiliar with formal departmental security procedures, they were aware that personal information needed protection. Even before the incident, cleaners were only allowed into the office accompanied by staff members. Care was taken to ensure the office was locked outside of normal working hours.

The departmental security manual did not mention microfiche. However, microfiche were covered by procedures for the handling and storage of general information. The manual describes the type of information disclosed as "Protected" and requires its protection to at least the minimum National Security level for "Restricted". There was no evidence that the microfiche was not protected to this level.

The office could have provided a greater degree of protection if it had conducted the required reliability checks prescribed in the new government security policy. The departmental security officer is now having checks done throughout RCCE.

The Commissioner found no evidence of specific harm caused to individuals as a result of the disclosure and no evidence to indicate that the information was used by any third party to obtain unauthorized access to other personal information.

## Recommendations:

- \* that all staff working with microforms attend security briefings on handling personal information held in these formats;
- \* that the department inform employees who handle and control information in this format of the procedures required to protect microforms;
- \* RCCE convert the data from microfiche to an on-line system capable of recognizing coded identifiers, providing a record of users, and controlling access;
- \* staff handling microfiche containing personal information undergo enhanced reliability checks.

The Minister of National Revenue informed the Privacy Commissioner of the actions RCCE has taken, or will take, as a result of this incident. They respond fully to the concerns and recommendations raised in the Privacy Commissioner's report. The new procedures will be examined in the course of regular audits by the Privacy Commissioner's office.

---

## **December — Microfiche Lost in Mail**

In December 1986 Veterans Affairs Canada (DVA) mailed 31 packages of microfiche to its various district offices. Two of the packages were damaged and the 148 fiche were lost.

At last count 44 of the lost fiche had been recovered from the Post Office. The remaining fiche are presumed to be permanently lost.

Following the incident, DVA stopped sending microfiche to the district offices and went to an on-line system for pay inquiries; notified officials at Canada Employment and Immigration, Health and Welfare Canada, Revenue Canada and Supply and Services Canada of the loss of the microfiche; notified all regions of the need for increased security for handling telephone inquiries.

DVA advised the Privacy Commissioner of the loss on January 26, 1987, and he initiated an investigation.

### **The Investigation**

Investigators interviewed departmental officials in Ottawa and Charlottetown, PEI where most DVA offices are located.

They found no written procedures covering microfiche security. The only policy related to security of information is in the part of DVA's administrative management manual dealing with the physical security of information. The manual does not specifically mention microfiche or packaging requirements for mailing microfiche, referring to sending records by Priority Post, when available.

DVA security staff considers microfiche confidential, though not in the sense of having national security implications and, therefore not requiring special handling. Staff handling the fiche were not required to have security clearances.

As well, investigators found that staff handling the fiche were not required to have security clearance.

For the past 11 years the department has sent microfiche in cardboard packages by Priority Post to the regional offices for distribution to the district offices. Where priority service is not available, the packages go first class mail.

Both of the lost packages could have been sent by priority. The Ottawa package was incorrectly addressed "New Terminal, P.Q.", instead of "P.O." The mailroom staff could not find a priority service to the Quebec address and sent it first class. In fact there is priority service to "New Terminal, P.O.", which is the Ottawa Post Office.

In the Edmonton case, someone decided it would take too long for the priority bag to be returned from the previous run. The package went first class.

The interviews disclosed that financial control sends transmittal notes with each package of microfiche. The recipient is required to sign and return the note. Financial control people said that district offices are slow to return the transmittal notes even when reminded by telephone. Further, district offices often claim that a microfiche package was not received when, in fact, it had been.

---

The DVA security section reviewed the physical security of microfiche in December 1986. However, the review did not consider the mailing procedures or packaging requirements for fiche. DVA is also reviewing all machine-readable media. The security section is preparing a form for taking inventory of the various media.

DVA in Charlottetown still receives seven sets of microfiche from the producer in Ottawa. However, since the incident sets have been hand-delivered to Charlottetown, and within the Charlottetown offices. One copy of a fiche containing War Veterans' Allowances (WVA) payment data was sent to regional offices in January 1987 by bonded carrier.

### **Recommendations:**

- \* that DVA develop and disseminate procedures governing the handling, sortage or control of microfiche;
- \* that DVA review packaging and mailing procedures for personal information to ensure that the information gets appropriate physical security during mailing and transmission;
- \* that security officials consider the physical security of personal information during transmission when conducting security reviews;
- \* that all districts be directed to return transmittal forms promptly to the originator;
- \* that security-breach procedures be established governing the departmental response to incidents involving the unauthorized disclosure of personal information. Such procedures should include identifying

responsible officers, establishing investigation procedures, reporting to senior departmental officials and notifying the Privacy Commissioner;

- \* that employees handling personal information records be subject to at least the enhanced reliability checks provided in the government's new security policy.

Since the incident DVA has stopped mailing microfiche and has converted pay information for both disability pensions and War Veterans Allowances to an on-line system. DVA has also begun an institution-wide review of all machine-readable media.

The department's actions respond fully to the Privacy Commissioner's report. Their adequacy will be reviewed during the next audit by the Privacy Commissioner's office.

### **December - Passports "Lost in Mail"**

Media reports that passports and supporting documents were lost in Ottawa prompted the Commissioner to make inquiries of both External Affairs and Canada Post.

The two government agencies denied responsibility. The investigation found both had to shoulder some blame. The loss came to light when a passport applicant asked the post office to find a registered package, giving the registration number supplied by External Affairs. Canada Post could find no trace of the registration, or any part of the entire series contained in one of two bags delivered to the post office on December 8, 1986. The bags were locked and were to have been taken to a registration office to be signed to confirm receipt.

---

External Affairs staff had left the bags on the dock with the regular mail rather than delivering them to the registration office. The lost bag, mixed in with empty bags, was delivered to a postal sub-station where it sat for three weeks before the post mistress opened the empties and realized that one contained mail. She returned it to the depot where it was found to contain the missing passports.

The Commissioner concluded that a series of preventable human errors had occurred but that the privacy of the material had not been violated since the bag had remained locked. Both External Affairs and Canada Post have since reviewed and improved their handling of registered mail. The Commissioner will examine the improvements during his regular audits of both organizations.

### **January 1987 - EIC microfiche in BC dump**

The discovery of microfiche in the Christina Lake, B.C. dump was reported in a news story in the February 12 edition of the *Toronto Globe and Mail*.

According to the report, 18 microfiche contained names and detailed personal information about foreign citizens attempting to enter Canada. There were entries about individuals' criminal records, refugee appeal claims, records of desertions from duty, and failures to appear at hearings. The fiche were accompanied by an Employment and Immigration Canada (EIC) receipt to be signed in order to confirm destruction of the old set.

The fiche were said to have been found by a man scavenging paper at the dump not far from the Cascades, B.C. border crossing. He had given them to a friend who passed them to a journalist.

The fiche are created by Employment and Immigration for distribution to immigration centres in Canada, immigration offices abroad, and Canada Customs offices. At isolated border crossings (like Cascades), customs officers administer the *Immigration Act*. They receive the sets of fiche at irregular intervals.

According to Canada Post, the fiche were sent on December 18, 1986, by Priority Post to Vancouver, then by highway service to Customs and Excise at the Christina Lake post office in Cascades. Neither the post office nor the Customs superintendent have a record of the envelope arriving. The fiche were apparently found January 3, in a bubble-type envelope, accompanied by the receipt.

Customs reported that two other border crossing points in the vicinity received their sets on January 7 and 8. The RCMP screened the package for fingerprints but could not match the only useful print to any of the customs employees. Apparently the envelope was in remarkably good condition for having been exposed to winter weather. The RCMP did not establish a criminal intent or act.

It was not possible to establish with any certainty what caused the documents to go astray.

EIC has changed its internal controls to ensure that it can respond quickly when there is any delay confirming receipt of the microfiche sets.

---

The Commissioner will examine these controls during his regular privacy audit.

## **February - MP Finds Surveys On Street**

The Privacy Commissioner decided to inquire into a report in the February 19, 1987, *Ottawa Citizen* that a Member of Parliament had found survey responses on an Ottawa street.

The MP, who had picked up pages from about 20 completed survey forms on the evening of February 5, estimated that as many as 200 more were left near the busy downtown Elgin and Slater Streets intersection. The 27-page survey had been conducted by Employment and Immigration Canada (EIC) to determine how it could improve its job referral service. The only personal information appeared on five pages which contained the name, address and phone number of a friend or relative to call in case the subject of the survey could not be reached. The facing page with the survey subject's information had been removed. Many of the pages contained no personal information.

The completed forms had been boxed and sent by messenger from EIC's Hull offices for tabulation in an Ottawa data processing company. The messenger service waybill was signed as complete by the data processing company. The driver said that his route had not taken him near the intersection and the truck had been closed—a company rule.

Privacy investigators searched the area where the documents were found but located no trace of any remaining forms trapped by shrubs or snow.

Although the Commissioner could not determine exactly what went wrong, he concluded that the page with the second person's name and address should have been removed before the forms were sent for data processing. He also recommended that EIC survey data containing personal information be key punched under strict security on EIC premises.

The department told the Commissioner that it will be able to develop surveys in a way which will separate the subjects' identity from their responses. However, limited staff and facilities dictate that survey material be processed on contract outside EIC facilities. EIC now inserts appropriate disclosure clauses in data processing contracts.

## **Postscript:**

### **The unemployment insurance survey.**

A *Montreal Gazette* report on March 5, 1986, said that Employment and Immigration Canada (EIC) had "handed over secret unemployment data to a private company" to survey jobless Canadians. The story alleged that the company, Peat Marwick and Partners, had not sworn to secrecy its employees or about 40 students hired part-time to carry out the survey.

The Privacy Commissioner investigated because the article implied that a federal government department had released personal information improperly, and had misled the respondents about why they had been chosen for the survey.

This survey was intended to determine the job-searching behaviour of unemployed workers and the factors which discourage them so as to help the department plan future policies and programs.



---

The Commissioner's investigators found that EIC first attempted the survey itself, using in-house resources and an 85-part questionnaire that was mailed to 10,000 unemployment insurance recipients listed in the Benefit and Overpayment Master File. The individuals selected had Social Insurance Numbers ending in 5, preceded by an odd number.

It became evident that a telephone survey would be better because this selection method had not produced a geographically balanced sample and many of the respondents had not understood all of the questions. Since the department had insufficient personnel, it contracted with an outside company to conduct the survey.

Peat Marwick and Partners was selected through a Supply and Services bidding process and a contract was signed in which the company and its subcontractors agreed to treat the EIC information "in confidence".

The contract stated in part: "The contractor agrees that it will not use the information provided by EIC for any other purposes than specified in the contract, that it will take the necessary measures to prevent unauthorized individuals from having access to the data, and that all materials obtained from the department or generated from departmental files will be returned." The contract did not mention the *Privacy Act*, nor did it contain express conditions binding the contractor to the Act.

In February 1986 EIC produced two pre-test lists of names and telephone numbers for Peat Marwick. The names were selected by the same method, and from the same data bank, as used in the department's own project. This bank is described in the Personal Information Index as being used, among others, for statistical and evaluation purposes. The bank contains information about UI recipients only.

EIC intended to control future access to the personal data by identifying individuals with a sequential number only, which could be linked to an individual's SIN using protocols kept in secure storage at EIC.

None of the material mentioned the *Privacy Act* and its requirements were not explained to guide the interviewers or inform the respondents.

Peat Marwick hired 32 part-time staff—mostly university students—to conduct the interviews.

These interviewers were to advise respondents at the outset that they were surveying "several thousand Canadians to get their views on the subject of unemployment." At the end of the 27-page survey, interviewers were to tell respondents that the information was strictly confidential, that they had a right to see it and the bank name and number where the information was to be stored.

Following the controversy surrounding the *Gazette* report, EIC asked that all data and forms be returned.

The survey was not completed.

---

The Privacy Commissioner's investigation found several problems with the survey. In particular Supply and Services Canada (DSS) was not asked to bind the contractor to the specific terms and conditions of the *Privacy Act*. However, there was some comfort in the confidentiality clause which bound the contractor to protect the collected information. There was also a requirement to establish a bank in which to store the information (it did not exist), to advise respondents as to exactly why they had been selected, to place all the paper copies from the internal project in the bank (they were destroyed), and to ensure that the information on the computer tapes be made anonymous to avoid the temptation of building profiles of UI recipients.

However, collection of the information was within EIC's mandate, the potential for analytical and statistical use of the information in the bank was clearly stated, and the use of an outside company to conduct a survey is not by itself a contravention of the *Privacy Act*.

Although there had been allegations that relevant documents had been shredded, the Commissioner's investigators found no evidence that any of the personal information had been so destroyed.

#### **Recommendations:**

- \* that EIC instruct DSS to include in any contracts on its behalf with outside suppliers express provisions requiring the company and its staff to comply with the *Privacy Act*;
  - \* that EIC tell respondents to its surveys precisely why they have been selected;
  - \* that EIC ask respondents' permission at the time of the survey to destroy hard copies of the respondents' answers to surveys;
  - \* that EIC establish a bank to contain the survey responses, place the hard copies in that bank and describe the bank in the Index;
  - \* that EIC destroy the key permitting it to link the statistical data to the individual respondent;
  - \* that the department's internal audit bureau audit all information-handling practices in order to satisfy the deputy minister that the department is in compliance with the *Privacy Act*.
- 
- \* that the department follow its own policy of consulting its privacy coordinator whenever projects and programs collect, use, and destroy personal information;

---

## SIN—the Continuing Issue

---

Public concern about the widespread and growing use of Social Insurance Numbers (SIN) as a personal identifier in both the public and private sectors was exacerbated this year by the theft of tax records containing the SIN number of some 16 million Canadians.

Though no legislation now restricts the use of SINs, their collection is given legal authority only by 11 federal statutes. Yet most government departments use the SIN, whether authorized by law or not, and SINs are used widely in the private sector.

SIN's use is particularly disturbing in light of the expanding computerization of information collection, storage, use and transmission. The possibility exists, both inside and outside of government, for building detailed dossiers on individuals by matching information in various databases using the SIN as the link.

Though SIN was never intended to be used as an identifier by the private sector, government facilitated that use by publishing the "last number check digit formula" which enables anyone to determine whether a SIN is valid. While it is more difficult to establish that a valid SIN belongs to a particular individual, it is possible for any employer to verify an individual's SIN from Employment and Immigration Canada's registry. By tendering a valid employer number, employers can verify not only their employees' SINs, but also those of customers, debtors or others. This, too, facilitates the use of SIN as a general private sector identifier.

As a result of the Commissioner's inquiry, Employment and Immigration Canada (EIC) has taken steps to prevent abuses of this nature. EIC told the Privacy Commissioner that a detailed log will be kept of all employer requests for SIN verification and that the requests will be reviewed monthly to detect possible abuses. If it identifies potential abuses, EIC will require employers to apply in writing and be subjected to further controls.

It is small comfort to tell Canadians that, except in those limited situations authorized by law, they are not required to provide their SIN, when refusal may deprive them of a service or benefit. No organization should be able to deny goods, services, benefits or entitlements for failure to provide a SIN unless its collection is specifically required by statute. This principle should apply to both government and the private sector; it should be enshrined in law.

It would be naive to believe that restricting the use of SIN will prevent the use of other numerical identifiers. Canadians may actually benefit from having a unique number to protect them from being confused with others having the same name. However, the identifier used by major government programs, the key to vast amounts of detailed personal information entrusted to government, should be given the greatest possible degree of protection to prevent its use as a *de facto* national identifier.

---

In an ideal world it would be desirable, once the appropriate legislation is in place, to restrict the use of SIN, and to issue new SINs to all Canadians. However, this step would be extremely costly. Based on 1985-86 figures, it costs approximately \$10 to issue a new SIN. The magnitude of the costs involved cannot be completely measured simply by multiplying \$10 by the number of Canadians, some 25 million. As well, there would be significant costs involved in restructuring the millions of government files now referenced by SIN. Not only would this be disruptive to the functioning of many programs, the confusion would inevitably prejudice some Canadians in their dealings with government. In the absence of a comprehensive assessment of the costs and benefits of re-issuing new SINs, an assessment which is beyond his mandate, the Privacy Commissioner does not feel that it is appropriate to recommend that new SINs be issued to all Canadians.

The Privacy Commissioner continues to urge government departments to improve the physical security of SIN information. For example, the SIN Registry itself relies heavily on the use of microfiche. This information is as much at risk as the Revenue Canada microfiche and its security needs to be improved.

In addition, the Privacy Commissioner urges departments to limit the circumstances in which they ask Canadians for their SIN, and to be vigilant in keeping SIN information confidential.

During the past year there have been a number of improvements in federal departments' handling of SIN — the results of concerned individuals or alert employees asking the Privacy Commissioner why the number was being used in a particular way.

### **SINs on Envelopes**

The Privacy Commissioner's participation on CBC's Cross Country Check-up generated an entire two hours of calls about the use and abuse of SIN. One caller, a woman from the Maritimes, told the Commissioner that unemployed workers were required to put their SIN on the outside of the envelope in which they send employment reports to EIC.

The Commissioner, concerned about her allegations, inquired about the practice. In fact, the offending envelope had been replaced some time earlier with one that does not ask for SINs. The regional office has been using up its large stock.

EIC instructed all its regions to cross the SIN request off the offending envelopes before sending them out, and advised its Forms Management Division to correct any other departmental forms or envelopes which "needlessly expose personal information".

### **...on Old Age Security Cheques**

An Ottawa woman was one of several callers who told the Commissioner that the pensioner's SIN was visible in the window of the envelope containing Old Age Security cheques.

---

The woman said she had told the department about the problem in 1981 but nothing was done.

While the *Old Age Security Act* is one of the 11 statutes that require the use of SIN, the Commissioner saw no reason why the number should be so visible. An investigator confirmed that the SIN was visible and the Commissioner wrote to Supply and Services Canada which issues all government cheques.

Supply and Services, aware of the problem, began in January 1987 to alter the sequence of SINs on cheques to make them unrecognizable. Recipients who still object to this use of the SIN may apply to Health and Welfare Canada for an account number to replace the SIN.

### **SINs to Cash Money Orders**

A North Bay woman objected to Canada Post's demand that she identify herself with her SIN to cash a money order. The clerk wrote her SIN on the back of the order.

An investigator from the Commissioner's office confirmed that Canada Post requires individuals to identify themselves when cashing money orders and that postal clerks note the identification on the back of the order to demonstrate that the identity was verified.

### **...and Pick Up Registered Mail**

Another caller was upset because Canada Post insisted on a SIN before releasing registered mail. The postal clerk had rejected three other pieces of identification, insisting on the SIN. The clerk relented only when the woman asked that the letter be returned to sender.

Canada Post has now instructed its field offices not to ask for SINs as identification for any purpose and to verify, but not record, any personal information from other forms of identification.

### **Fund Drives and Payroll Deductions**

A number of federal public servants were concerned that the pledge cards issued to departmental canvassers during the 1985 United Appeal Campaign were pre-printed with employees' SINs. They pointed out that the SIN is needed only when an employee authorizes a contribution through payroll deductions. Those who make a one-time cash donation or who choose not to contribute through the federal government, should not have their SIN displayed to those handling the cards.

The Commissioner, while sympathetic to the need for campaign efficiency, suggested that employees who contribute through payroll deductions supply the SIN themselves. The Commissioner had given the same advice to the Bank of Canada during its annual Canada Savings Bond campaign.

This year's pledge cards arrived with the department's and employee's names, the payroll and payroll numbers—but no SINs. Employees who elect to contribute through payroll deduction now supply their own SIN.

### **And Now the Bad News...**

SIN complaints about federal government agencies are only the tip of the iceberg. The Commissioner was powerless to help many of the more than 100 callers who wanted to talk, or complain,

---

about SIN. Individuals wondered why they should give their SINS to landlords, employers, unions, supermarkets, stores, banks, insurance companies, and school tax authorities. One person said an Ontario government department was requiring employees to turn in their SIN cards to have them photocopied.

In response, the Commissioner advises individuals when the law requires them to provide the number and when they can refuse. He points out that there is no law against asking for the number or denying a service if the SIN is refused.

The answer satisfies neither the caller nor the Commissioner.

---

## Exempt Banks

---

The government took a giant step this year in bringing the tortured saga of the so-called "exempt banks" to an effective, if somewhat unheroic, end.

During a court case, it became apparent that files in at least one of the closed banks had not been individually examined in order to be sure that each met the test of exempt bank status. (The whole issue and the Ternette case is described in detail in the Commissioner's 1985-86 report.)

Prior to the revelation that the bank was improperly closed, the Privacy Commissioner had begun a systematic audit of other departments' exempt banks, beginning with Employment and Immigration Canada (EIC). When investigators found that files in these two EIC banks had not been examined individually, as required by the *Privacy Act*, the Commissioner wrote to all departments with exempt banks asking for confirmation that each file in its banks had been examined in accordance with the requirements of the Act.

Responses from many of the departments showed that the banks were being treated as open and departments had begun the process of applying to rescind the exempt bank orders.

Orders in Council P.C. 1987-282 to 295 inclusive, passed on February 19, 1987, rescind the exempt status of 15 closed banks. They are:

### **Canada Employment and Immigration Commission and Department of Employment and Immigration**

- EIC/P-PU-260 - Immigration Security and Intelligence Data Bank  
EIC/P-PU-265 - Enforcement Information Index System

### **Canada Post Corporation**

- CPC/P-PU-085 - Postal Related Crimes/Offences or  
CPC/P-PE-824 - Postal Related Crimes/Offences

### **Correctional Service Canada**

- CPS/P-PU-005 - Institutional Security Threats Records  
CPS/P-PU-010 - Security Enquiries  
CPS/P-PU-065 - Preventive Security Records

### **Canadian Security Intelligence Service**

- SIS/P-PU-010 - Canadian Security Intelligence Service Records

### **Department of National Revenue (Customs and Excise)**

- RCC/P-PU-015 - Customs Interdiction and Intelligence Records

### **Department of National Revenue (Taxation)**

- RCT/P-PU-035 - Tax Avoidance Cases

### **Department of the Solicitor General**

- SGC/P-PU-025 - Security Policy and Operational Records  
SGC/P-PU-030 - Police and Law Enforcement Records Relating to the Security and Safety of Persons or Property in Canada  
SGC/P-PU-035 - Protection of Privacy (as defined in Section 178.1 to 178.23 inclusive of the *Criminal Code*)  
SGC/P-PU-050 - Police and Law Enforcement - RCMP Operational Records  
SGC/P-PU-055 - Commissions of Enquiry

---

The five remaining exempt banks are:

**National Defence**

Military Police Investigation Case Files:  
DND/P-PE-835  
Security and Intelligence Information  
Files: DND/P-PU-040

**Privy Council Office**

Security and Intelligence Information  
Files: PCO/P-PU-005

**Revenue Canada/Taxation**

Tax Evasion Cases: RCT/P-PU-030

**Royal Canadian Mounted Police**

Criminal Operational Intelligence  
Records: CMP/P-PU-015

The Commissioner was unable to examine the submissions to the Privy Council on the basis of which the banks were ordered closed. The submissions are considered confidences of the Queen's Privy Council and not subject to the *Privacy Act*.

The Commissioner's investigators have now examined the material in National Defence's Military Police Investigation Case Files, Privy Council's Security and Intelligence Information Files, and the RCMP's Criminal Operational Intelligence Records and Protection of Personnel and Government Property. The investigation revealed that the criteria for establishing an exempt bank had not been met, for example, files had not been individually examined and, therefore, despite the departments' contentions, they also were improperly closed.

The Commissioner will investigate complaints that individuals have been denied access to information in these banks as if they were open. His investigation into the remaining Revenue Canada/Taxation and National Defence closed banks is nearing completion.

Whatever the status of individual banks, applicants should know that much of the material in these files may be exempt under other sections of the *Privacy Act*. In particular, section 16 allows a department to neither confirm nor deny the very existence of a file if its contents could not be released because of other lawful exemptions.

For example, information could be withheld because its release might injure Canada's defence or that of an allied state, or the conduct of international affairs, or damage law enforcement, legal investigations, or the security of a penal institution. Nevertheless, the irritant of completely closed banks—and the suspicions they aroused—has now been significantly reduced, a step the Commissioner applauds.



---

## Parolees and Inmates

---

Parolees and inmates of federal institutions are a large part of the Office's clientele. Parolees and inmates, regardless of citizenship, are protected under the *Privacy Act*.

Government holds a great deal of personal information about these persons, information that is used to make administrative and quasi-judicial decisions directly affecting them.

### Timely Access

It is important that parolees and inmates get timely access to their files and their personal information be disclosed to third parties only when authorized.

Correctional Service Canada (CSC) has had difficulty complying with the Act's response deadlines. During the past year, a total of 255 delay complaints were made against CSC, of which 218 were justified.

However, new CSC procedures and more staff now provide inmates a much more timely response to their requests. CSC has made an almost heroic effort and cleared its backlog of requests. It is to be commended for having solved the problem.

Yet, there remains room for improvement. CSC could provide inmates with informal access to their records. The Correctional Investigator brought the desirability of a more informal access process to the Commissioner's attention. The Correctional Investigator said that inmates are required to sign some documents to certify that they have seen them. He felt that it was unnecessary to require them to submit a formal access request to examine the same documents later.

The *Privacy Act* does not require informal access. Nevertheless, the Privacy Commissioner agrees with the Correctional Investigator that, to the extent feasible, CSC should provide such informal access.

### Information to Third Parties

CSC and the National Parole Board (NPB) regularly receive requests for parolees' and inmates' personal information from victims' rights groups, inmates' rights groups, police, the media and Members of Parliament. Releasing personal information without consent to any of these individuals or groups invades the privacy of the parolee or inmate concerned.

Each such request places the CSC or NPB in the unenviable position of balancing the rights accorded third parties by the *Access to Information Act* against the rights accorded to inmates and parolees by the *Privacy Act*. The Privacy Commissioner questioned a decision by CSC and the parole board to release inmate information to third parties (see Notifying the Commissioner) and notified 60 inmates that personal information about them had been released without their consent. It was the first such notification since the *Privacy Act* came into force.

CSC and the parole board are developing a revised Use and Disclosure Code and discussions with the Privacy Commissioner about third-party disclosure are continuing.

---

---

## **Confidentiality of Inmate Correspondence**

CSC has authorized inmates to correspond with the Privacy Commissioner's Office on a "privileged basis". The correspondence, exempt from any form of censorship or inspection, is forwarded unopened by CSC. Correspondence from the Commissioner to inmates receives the same treatment. This is a commendable policy.

However, the same level of confidentiality for responses to inmates' requests for personal information from government institutions is not provided, something which could put inmates at risk. Personal information about other inmates is often a coveted commodity in institutions. Its release can result in serious physical harm to the inmate concerned.

For this reason, the Privacy Commissioner supports the CSC policy of not permitting some inmates to keep copies of their personal files in their cells. But CSC policies should ensure that responses to inmates' *Privacy Act* requests are kept confidential.

---

## Personal Information and Public Servants

---

The *Privacy Act* states that information "that relates to the position or functions" of public servants is not protected from release under the *Privacy Act* and the *Access to Information Act*.

The imprecision of the wording in this section (paragraph 3(j)) has plagued departments trying to respond to individual requests. It has also caused the Privacy Commissioner to be concerned about the confidentiality of information which federal employees are required to provide under the government's conflict of interest code and security policy, as well as for employees who identify themselves in affirmative action programs.

The problem stems from the wording of the exception. It says:

"personal information" does not include

"(j) information about an individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual including,

- (i) the fact that the individual is or was an employee of the government institution,
- (ii) the title, business address and telephone number of the individual,
- (iii) the classification, salary range and responsibilities of the position held by the individual.
- (iv) the name of the individual on a document prepared by the individual in the course of employment; and

- (v) the personal opinions or views of the individual given in the course of employment,".

This explanation does not say, for example, that "only the following information is not personal". Thus, interpretation of the section turns upon what information about public servants "relates to the position or functions of the individual".

It can be argued that an employee's statement of financial holdings, provided under the government's conflict of interest code, "relates" to his or her position or functions. So could medical information that an employee provides to benefit from an affirmative action program for hiring those with physical disabilities, or detailed personal histories government departments gather to check employees' reliability or to grant security clearances.

Although a department may consider this information "personal" and treat it circumspectly, it is not clear whether the department could deny access to an applicant seeking the information under the *Access to Information Act*.

Both the Information and Privacy Commissioners called this problem to the Treasury Board's attention when they were first told to apply the conflict of interest code to their own employees. During the exchange of correspondence, 14 public service bargaining agents, which represent the majority of federal public servants, complained to the Privacy Commissioner.

---

## The Conflict of Interest Code

The new federal conflict of interest code took effect January 1, 1986. It requires all employees to complete a certification document in which they agree to observe the code and state whether they have any assets or liabilities — or are involved in any outside activities — which could give rise to a conflict. Those with assets or activities which could be a conflict of interest must then provide details in a confidential report.

The unions alleged that Treasury Board's collection of such information violated section 4 of the *Privacy Act* because all employees were required to disclose their personal financial affairs, regardless of their position, rank or duties, or whether their holdings could give rise to a conflict. They also alleged that collection of the information did not relate to a Treasury Board program (required by the *Privacy Act*), and the broad range of circumstances covered by the code would oblige "any reasonably prudent employee" to disclose full details even where no reasonable apprehension of conflict existed.

The unions also considered misleading the statement assuring employees of the complete confidentiality of the information. They pointed to what they argued were the weaknesses in the wording of section 3 of the *Privacy Act* and the range of releases of personal information permitted by its section 8. These include release to: investigative bodies, the Attorney General for use in legal proceedings, other governments (including those of foreign countries) if there is a formal agreement between the government, researchers, the Archives, and for any purpose if, in the opinion of the head of the department, the public interest would clearly outweigh the invasion of privacy.

The Privacy Commissioner investigated the unions' complaint, and exercised his discretion under section 37 of the Act to investigate whether the administrative procedures now in place properly protected the information, and whether the code complied with the fair information practices as set out in sections 4 to 8 of the Act.

The Commissioner used an outside investigator to examine department's collection, storage, use and disposal of the information. He did this because his own investigators, employees of Treasury Board, the object of the complaint, are represented by one of the bargaining agents which complained.

The investigator found that departments were collecting the information directly from the individuals concerned, explaining why it was being collected, using it only for that purpose, and keeping it in locked cabinets.

However, there were some deficiencies. The Commissioner recommended that files be sealed in separate envelopes within the locked cabinets, that the cabinets be kept in controlled areas and that files be logged in or out, and counted regularly.

Insufficient time has elapsed to ascertain whether departments are disposing of documents according to the Treasury Board requirement that they be kept for two years after termination of employment.

Since the *Privacy Act* requires that records be as accurate, up-to-date and complete as possible, the Commissioner asked that departments remind employees each year of their responsibility to review their statements, and to certify the accuracy of previously submitted information.

---

The legal issues are more complex and are discussed under two questions that follow.

**Does Treasury Board have authority to collect the information required by the code?**

The Commissioner found that the *Financial Administration Act* gives Treasury Board authority over general administrative policy and personnel management in the public service, including establishment of terms and conditions of employment, and standards of discipline. As the government's personnel manager, it is legitimate that Treasury Board require public servants to conduct themselves so as to avoid conflicts of interest, and to implement appropriate reporting and monitoring systems.

Thus, he concluded that, with the exception of section 26 of the code, Treasury Board could lawfully collect the information.

Section 26, however, requires employees to report "any outside activity that is directly or indirectly related to" their official duties and responsibilities. The Commissioner concluded that "directly or indirectly" puts conscientious employees in a difficult position as they might think they should declare everything rather than risk contravening the code. Since such reporting requirements were too broad to relate directly to an operating program of Treasury Board, he found that collecting that type of information contravened section 4 of the *Privacy Act*. He suggested that Treasury Board narrow these reporting requirements.

**Can Treasury Board protect the confidentiality of the reports?**

The Commissioner considered the uncertainty inherent in section 3(j) of the *Privacy Act*, and the releases permitted under section 8. The principal justification for collecting the information is to ensure that employees carry out their duties and responsibilities while avoiding a conflict of interest. If the information did not "relate to the position or functions" of the employees, Treasury Board could not collect it under section 4 of the *Privacy Act*. Thus, section 3(j) may be interpreted as meaning that the *Privacy Act* cannot protect the information from disclosure to third parties who may request it under the *Access to Information Act*.

While the Commissioner believes that information collected under the code should be protected by the *Privacy Act*, the view of the courts may be different. In the absence of that certainty, the Commissioner found it misleading to assure employees of "complete confidentiality".

The Commissioner also noted that section 8(2) of the *Privacy Act* authorizes the release of personal information without consent in 13 situations, such as to the RCMP, to researchers and auditors.

The Privacy Commissioner recommended that section 3(j) be amended to make clear which information about public servants is personal and which is not. He also recommended that employees be informed about the possibilities for third party disclosure specifically contained in the *Privacy Act*.

---

## Consulting the Privacy Commissioner

---

The Privacy Commissioner maintains a watch to assess the privacy implications of legislative and regulatory proposals. He has tried to have this "consultative" role better defined and strengthened. However, during the past year such consultations with the Commissioner continued to depend on the courtesy of departments. For example, the Department of Justice consulted with the Commissioner's Office on the privacy implications of four proposals during the year.

The Commissioner was also invited before the Standing Committee on Communications and Culture concerning the *Archives of Canada Act* (Bill C-7) which received third reading December 19, 1986. The privacy principles in the *Privacy Act* are a code of fair information practices and the new duties and powers given the Archives of Canada will strengthen government-wide attention to these principles.

There were a number of instances during the year when the Commissioner was not consulted on initiatives with privacy implications. The most significant cases were the government's new security policy, its conflict of interest and post-employment code, and the new *Employment Equity Act*. (The conflict of interest code is discussed above.)

### The New Security Policy

A new federal government security policy came into force on June 18, 1986. It was issued by Treasury Board, under the authority of the *Financial Administration Act* and of Cabinet decision 3-042485 RD.

This policy replaced both the policy on security of information, in force since 1956, and the policy on security screening, in force since 1963.

The new policy has privacy implications because it specifies physical security of personal information and requires the government to collect such information about public servants to ensure that "all persons engaged by the government meet the standards of reliability, trustworthiness and loyalty required by the nature of their duties or tasks."

In response to concerns expressed to him by public servants and their representatives, the Privacy Commissioner has been reviewing the privacy implications of the security policy. He has concluded that the Treasury Board has the authority, indeed the responsibility, to ensure that government information and assets receive adequate security. This authority includes the legal power to collect information about public servants to assess their reliability, trustworthiness and loyalty. However, he has raised with the Treasury Board a number of concerns associated with the implementation and administration of the code. In particular he has questioned the government's ability to protect the information collected under the code from disclosure, pursuant to an Access to Information request (see above).

---

As well, he has suggested that there be more flexibility in determining when credit and fingerprints checks will be required and more guidance in determining the basis on which employment can be denied. Discussions on these matters are ongoing.

### **Employment Equity Act**

The *Employment Equity Act* came into force September 9, 1985, to improve equality in the federally-regulated workplace. The Act requires employers to report publicly on the make-up of their workforces and their employment practices. The legislation does not require the identification of individuals.

The statistical information contained in the reports can be used, albeit in rare circumstances, to identify personal information about specialized staff in small regional offices. Care should be taken to inform fully employees in designated groups before they agree to be identified. In order that consent be freely given, employers should not require prospective employees to self-identify prior to hiring. As well, employees should be able to withdraw consent at any time.

While the employers' annual public reports do not directly identify individuals, employees may have to complete detailed background questionnaires as part of the self-identification process. Since some employers covered by the *Employment Equity Act* are also subject to the *Access to Information Act* and the *Privacy Act*, the information may, in some circumstances, be accessible to third parties. These employers should collect only minimum personal information about their employees and make sure that the employees are aware of the possibilities for third party disclosure.

The Privacy Commissioner would have welcomed an opportunity to provide advice on both the new security policy and the *Employment Equity Act*.

---

## Commissions of Inquiry

---

Mr. Justice Deschênes pointed out in the Report of the Commission of Inquiry on War Criminals (December 30, 1986) that the *Privacy Act* and the *Access to Information Act* were among the statutes which had prevented his Commission from accessing certain information held on pensioners.

During its inquiry the Commission (which had been designated an investigative body under the *Privacy Act*), had applied to Health and Welfare Canada for information about a particular individual. The department supplied the material but denied a second request for details about several suspects because section 19 of the *Old Age Security Act* prohibits the department from disclosing any information it obtains under the act about individual applicants.

The Commission complained to the Privacy Commissioner that it had been denied the information and asked the Commissioner to recommend that Health and Welfare Canada provide the information "forthwith".

The Privacy Commissioner dismissed the complaint because

- \* the *Privacy Act* grants rights of access (and the right to complain) only to the "individual" who is the subject of the information;
- \* disclosure of information under the *Privacy Act* is subject to limitations contained in other acts of Parliament;
- \* subsection 8(2) of the *Privacy Act* permits but does not require disclosure;

\* section 19 of the *Old Age Security Act* prohibits release of the information.

The Privacy Commissioner concluded that a dispute about Health and Welfare Canada's obligation to provide the information to the Deschênes Commission involved an interpretation of section 19 of the *Old Age Security Act*, which might better be resolved by a court of law.

As a remedy, Mr. Justice Deschênes recommended legislative changes that would require Health and Welfare to disclose personal information to commissions of inquiry, the RCMP and other investigative bodies.

The Privacy Commissioner would question legislative changes which could weaken existing protections for personal information in Canada. This is especially so when it involves commissions of inquiry. These commissions are not subject to the provisions of the *Privacy Act* which establish standards for the collection, retention, use, disclosure, and disposal of personal information. Once a government institution discloses personal information to an inquiry commission, the information loses the protection of the *Privacy Act*. Yet the RCMP or other investigative bodies must abide, of course, by the provisions of the *Privacy Act*.

At present, paragraph 8(2)(e) of the *Privacy Act* permits investigative bodies to have access on written request to personal information held by departments, "if the request specifies the purpose and describes the information to be disclosed".



---

---

This provision gives the departments discretion whether to disclose and thus provides a check on possible abuses by investigative bodies. As well, it ensures an audit trail which can be reviewed by the Privacy Commissioner.

Should the government adopt the recommendations of Mr. Justice Deschênes to increase access to pension information, the Privacy Commissioner urges that access be discretionary, not mandatory; that the safeguards contained in paragraph 8(2)(e) of the *Privacy Act* to be maintained; and that the inquiry commissions themselves be subject to the data protection provisions of the Act.

---

## Notifying the Commissioner

---

The *Privacy Act* requires government departments to notify the Privacy Commissioner when they intend to release personal information "in the public interest" and when they use it in a way that is consistent with the reason for its collection, but for a use not described in the Personal Information Index.

### In the Public Interest

The head of a department may release 'personal information' if, in the opinion of the head of the department,

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

"disclosure would clearly benefit the individual to whom the information relates."

By notifying the Commissioner of the release he can advise any individuals he considers appropriate that release is forthcoming. If he considers the release improper he may initiate his own complaint.

There were several such notifications during the year.

In December 1986 the National Parole Board told the Privacy Commissioner that it had released information about 60 inmates to a member of the Parliamentary Committee reviewing Bill C-67 (an act to amend the *Parole Act* and the *Penitentiary Act*). The 60 inmates were affected by the Bill's detention regulation.

The released information included the inmates' fingerprint section numbers, names, home regions, the institutions where they were being held, the dates they would be released under mandatory supervision, their warrant expiry dates, and the dates of hearing or detention orders.

The Commissioner believed that the Committee could have been satisfied with depersonalized statistics and that personal information should be released in the public interest only in "exceptional circumstances". He did not agree that this was such a case.

The Parole Board supplied the names and addresses of the 60 inmates and the Commissioner notified each of them of the release.

In another case, the Commissioner questioned a Solicitor General notice that it proposed to release a National Parole Board investigation to an MP, solely because of his status. The subject of the investigation was not in the MP's constituency.

After receiving the Commissioner's letter, the department reversed its decision.

In yet another incident, Statistics Canada advised the Commissioner that it had received 23 requests from a legal firm representing a foreign government to search 1940 National Registration records for information about persons recently deceased. Statistics Canada, having located some of the information, advised the Commissioner that it would be releasing under paragraph 8(2)(m) of the Act.

---

The Commissioner told Statistics Canada that he saw nothing in this application which served the public interest and that should the department decide to deny release and the matter went to the Federal Court, he would ask to be a party to the action so as to express his views about breaching the privacy of the deceased.

The test set out in sub-paragraph 8(2)(m)(i) is an onerous one. The head of the institution must be satisfied not only that the public interest outweighs any invasion of privacy that may result from the disclosure, but that it does so "clearly".

Some fears were expressed when the legislation was proposed to Parliament that this section could undermine the purposes of the *Privacy Act*. Experience has shown that fear to have been unfounded. At the same time, experience has also shown that the section has been used occasionally to authorize disclosure of personal information without adequate regard for privacy rights.

CSC and NPB are sensitive to privacy concerns. However, the legislation itself has no "fail safe" mechanism to permit independent review of an institution's decision to disclose personal information in the public interest. The Commissioner has no power to substitute his judgment for that of the institution. In fact, information may be disclosed to third parties before the Commissioner is told of the release.

The Act does not permit the Commissioner or an individual to ask the Federal Court to review whether a proposed release should be permitted under sub-paragraph 8(2)(m)(i). The Commissioner's sole recourse is to notify the individual whose information has been released, but by then the release has occurred.

It is an anomaly that individuals denied access to their personal information may go to court for review of the decision, but they cannot seek a review of a department's decision to disclose their personal information to third parties.

#### Other Notifications

Department	Information
Canada Post	Last known address of an individual to police to notify the individual of an inheritance
Correctional Service	Information confirming the transfer of an inmate's funds to his spouse, supplied to Provincial Compensation Board to settle estate
	Last known address of an individual required by a law firm in a claim arising out of a motor vehicle accident in which the individual was named defendant
	Personal information of a deceased inmate requested by deceased's son

	Addresses to a law firm of several inmates who were potential witnesses in a murder trial		pursuant to paragraph 8(2)(m). It was taken to be "... to a member of Parliament for the purpose of assisting the individual to whom the information relates in resolving a problem", pursuant to 8(2)(g).
External Affairs	Register of Measures taken by Canadians against Apartheid containing the names of individuals and organizations and cities of residence, presented to the Secretary General of the United Nations	Northern Canada Power Commission	Information on superannuation benefits released to Canadian Utilities Ltd. to carry out reciprocating pension agreement
	Personal information concerning a deceased Soviet scientist who had defected to Canada, released to a Canadian journalist	Public Archives	Blood type of ex-armed forces member released to company trying to establish a safe blood bank while providing medical services to Canadians employed on oil drilling operations in Kenya
Dept. of Justice	Information regarding Canadian government funding of the Allan Memorial Institute in the 1950's and 1960's		
Health & Welfare	Personal information requested by a provincial Physicians and Surgeons Board	RCMP	Last-known address of deceased RCMP member for pension claim of widow
National Parole Board	Parole information to media on an inmate released by the Parole Board to justify its decision to release the inmate on parole	Secretary of State	Date an individual obtained Canadian citizenship released to Dutch authorities to help individual's daughter obtain Dutch citizenship
	Personal information contained in results of a Parole Board investigation into the early release of an inmate requested by an MP. The Board was advised that this release was not considered to be		Personal information to help an individual apply for Canada Pension benefits

	Citizenship status of a producer released to Department of Communications so that investors in Canadian films and videotapes benefit from tax deductions	After discussions with Correctional Service Canada, the Commissioner determined that these releases were a consistent use of information.
Solicitor General	Status of security clearance of official in Solicitor General's office released to an MP anticipating questions in House of Commons	<b>Inmate data to victims</b>  In a similar case, Correctional Service Canada advised the Privacy Commissioner that it considered the release of certain personal information to an inmate's victim(s) conformed with the provisions of paragraph 8(2)(a), "for the purpose for which the information was obtained ... or for a use consistent with that purpose".
	Seniority roll of RCMP officers requested by Joint House and Senate Committee on official languages. Personal information about official language capacity, dates of retirement and years of continuous service was removed	Thus, CSC believes it could reveal to a victim an inmate's release date, the conditions of the release and the released person's destination. As previously indicated, the use and disclosure policies of CSC and the parole board are under discussion.
Statistics Canada	Eleven notifications concerning personal information released to help individuals obtain Canadian or American citizenship, or pension benefits	<b>Native persons' list to Health and Welfare</b>  In September 1986 the Department of Indian Affairs and Northern Development (DIAND) advised the Privacy Commissioner that it had entered into a formal agreement with Health and Welfare "in respect to the exchange of personal information pursuant to the <i>Privacy Act</i> ".
Veterans' Affairs	Medical information on deceased veteran to daughter	Health and Welfare, which provides medical services to Native people, asked DIAND to provide a list of status Indians. This use is consistent with the original collection purpose and was to be added to the statement of consistent uses in the next issue of the Personal Information Index.

### Consistent Uses

Solicitor General Perrin Beatty advised the Commissioner in March 1986 that parole information on an inmate being freed on mandatory supervision had been released to the Attorney General of British Columbia and a victim of the inmate.

---

---

### **Aircraft accident data to public**

The Canadian Aviation Safety Board asked the Privacy Commissioner for an "authorization for class disclosure of personal information" under paragraph 8(2)(m) of the *Privacy Act*. The board told the Commissioner that it receives many requests for information it obtains during aircraft accident investigations. It often considers release of such information to be "in the public interest".

While the Treasury Board's Interim Policy Guide mentions "class disclosures" under paragraph 8(2)(m), there is no such provision in the *Privacy Act*. The Commissioner concluded that for the most part this type of disclosure was consistent with the purpose for which the information was compiled.

### **Intelligence to third parties**

The Solicitor General notified the Commissioner that information collected by the Canadian Security Intelligence Service, under section 12 of the *Canadian Security Intelligence Service Act*, was being provided to third parties to offset potential threats to the security of this country. The Commissioner considered the use consistent with the purpose for which the information was compiled. It will be described in the next issue of the Personal Information Index.

---

## Complaints Branch

---

The office received 767 complaints during the year, completed 692 investigations, and carried forward a case load of 271. The Commissioner considered justified 53 per cent of the completed complaints and dismissed 45 per cent. Two per cent were abandoned.

Those following the complaint investigations from year to year may be startled by this year's statistics. While there have been more complaints, the increase results partly from a new method of statistical reporting.

The office now records complaints against information banks. Thus a complaint that access was denied to two banks shows as two complaints, even though both are controlled by the same department. The change acknowledges that investigators may have to review material in several different information banks and examine several claims for exemptions on a number of different grounds. It also identifies problem banks.

In real terms, however, there has been a 10 per cent increase in complaints this year.

The Privacy Commissioner's success in complaint investigation is based on negotiation. Investigators have been able to persuade departments to release hundreds of pages of documents by discussion and clarification of the law. While more time-consuming, the non-confrontational approach ultimately benefits the complainant more than early recourse to the courts.

### Delays

Departments are steadily ironing out their administrative difficulties and most are responding to requests within the 30 days (or maximum 60 days with an extension) permitted by the *Privacy Act*. However, two departments continued to be the subject of a large number of delay complaints: Correctional Service Canada (CSC) with 255, and National Defence (DND) with 49. As mentioned earlier, CSC has refined its procedures and added more staff to handle inmate requests. It has already cleared a large backlog and, according to the latest Treasury Board statistics, appears to be processing applications faster.

DND receives the largest number of quarterly applications of any government institution: 5,169 during the period from October 1 to December 31, 1986 (compared with CSC's 1,696 for the same period). However, the department is largely the architect of its own workload since it continues to require armed forces members to apply formally to see their annual performance evaluations. The Commissioner has recommended in past annual reports (and during complaint investigations) that DND provide members routine access to their performance appraisals. Until it does so, DND can expect to continue being number 1 on the list of applications received.

---



---

**Origin of Completed  
Complaints by Province and  
Territory**

The following cases give life to the statistics.

**Only His Own Conversations (1372)**

An individual sought access to two wire-tap tapes containing personal information about him. He was given the two tapes with portions exempted because the information was obtained in the course of lawful investigations. He complained to the Privacy Commissioner.

Because the personal information was contained on audio tapes, the RCMP had difficulty in processing the request. Eventually it decided to give him access to his own communications on the tapes, exempting those between other persons.

The Privacy Commissioner was satisfied that the RCMP released to the applicant all portions of the tapes on which his voice appeared.

**Exemptions Not Explained (1303)**

A man objected to National Parole Board's exemptions to material released to him from the board case files. The board had withheld material because it was received "in confidence" from another government (section 19), and because some were medical records. While medical records are generally accessible, section 28 allows government institutions to withhold medical information it believes "would be contrary to the best interest of the individual".

The Privacy Commissioner's investigator disagreed with the exemption for medical records. The Parole Board did not explain why examining the information would be contrary to the applicant's best interests. After discussions between the investigator and the coordinator's office, NPB dropped this exemption.

---

Newfoundland	2
Prince Edward Island	4
Nova Scotia	21
New Brunswick	20
Quebec	238
National Capital Region Quebec	3
National Capital Region Ontario	36
Ontario	178
Manitoba	43
Saskatchewan	33
Alberta	43
British Columbia	66
Northwest Territories	0
Yukon	3
Outside Canada	2
<b>Total</b>	<b>692</b>

---



---



---

**Grounds of Complaints and Investigation Results**

<b>Grounds</b>	<b>Abandoned</b>	<b>Justified</b>	<b>Dismissed</b>	<b>Total</b>
Misuse	—	6	20	26
Access	13	65	178	256
Correction	—	—	7	7
Language	—	3	3	6
Index	—	1	—	1
Collection/ retention/disposal	—	3	8	11
Delay	3	288	94	385
<b>TOTALS</b>	<b>16</b>	<b>366</b>	<b>310</b>	<b>692</b>

This case was one of a number of exemptions under section 19 referred to the Solicitor General for discussion. As a result of negotiations with the province, more information was released to the complainant. The Privacy Commissioner considered the complaint justified.

**Can Non-Citizen Transfer Rights?**  
(1137)

Can an individual with no application rights under the *Privacy Act* ask someone who does to apply on his or her behalf?

This was the issue when a prospective immigrant was denied entry into Canada. With the women's permission, her sponsor applied for access to the file.

The issue was resolved at the Federal Court where the sponsor obtained the material under the *Access to Information Act* (Goldstein vs Employment and Immigration Canada). Once access was obtained, the sponsor withdrew the complaints under the *Privacy Act*.

**No Access to Fiancee's Information**  
(1618)

A man scheduled to appear at an immigration hearing asked to examine information in two Employment and Immigration (EIC) banks. EIC removed some information before sending material to the applicant because it concerned another person—his fiancée.

The documents in question concerned his alleged marriage to a Canadian citizen overseas, a ceremony the fiancée said never took place.

The man's lawyer complained to the Commissioner that all the information in the files concerned his client, including others' "views or opinions about him" and, since the material concerned his client's marital status and right to stay in Canada, the lawyer maintained it was his client's personal information.

---

The investigator found that the information about the client and his fiancée was so entwined that severing was impossible without rendering the documents meaningless.

The Commissioner found that EIC had done all that it could to satisfy the man's application, and dismissed the complaint.

**Staffing Board Members' Notes Lost (1665)**

A Winnipeg woman asked Employment and Immigration Canada for copies of all material from her job interview in the Winnipeg Regional Office. EIC provided the material, without the interviewers' notes. When EIC told her the notes were lost she complained to the Commissioner.

The investigator found that once the hiring process was completed, the staffing officer sent all the material, including the notes, to personnel for filing. A search of the office files by the board chairman and personnel staff found nothing. EIC believes the notes may have been destroyed when the documents were filed because notes are not considered part of the administrative documents needed to establish a job eligibility list.

The Commissioner concluded that EIC had made notes part of the competition file. By destroying them it had denied her access. He considered the complaint justified.

**Exemptions on Security File Reduced (1673)**

An External Affairs employee asked to see her security clearance file and complained to the Commissioner about information it withheld. External Affairs exempted material because it would identify an information source, jeopardize a lawful investigation, and injure crime detection and prevention.

The investigator asked the department to substantiate each exemption. During the discussion the investigator convinced the department to exempt only part, not all, of a three-page letter. The department agreed.

The Commissioner regarded the remaining exemptions as reasonable but justified the complaint.

**Advise Review Committee (1625)**

The Privacy Commissioner received a complaint from an inmate of a federal penitentiary that information had been improperly released to his family without his consent. The investigation disclosed that this was indeed the case, and the Commissioner found the case justified. The Solicitor General, acknowledging the Commissioner's adverse finding, said that the problem with such releases had been brought to the attention of the Parliamentary review committee.

**Completed complaints by department, type, and result**

Department	Complaint Type	Number (Total)	Justified (Total)	Dismissed (Total)	Abandoned (Total)
Agriculture Canada	Access	1 (1)	—	1 (1)	—
Canada Mortgage and Housing Corporation	Access	1 (1)	1 (1)	—	—
Canada Post	Access	1	—	1	—
	Misuse	2	2	—	—
	Delay	19	16	3	—
	Col/Ret/Dis	2 (24)	— (18)	2 (6)	—
Canadian Aviation Safety Board	Access	1 (1)	—	1 (1)	—
Canadian Human Rights Commission	Access	1 (1)	—	1 (1)	—
Canadian International Development Agency	Misuse	1	—	1	—
	Col/Ret/Dis	1 (2)	—	1 (2)	—
Canadian Security Intelligence Service	Access	6 (6)	—	6 (6)	—
Communications	Access	1 (1)	—	1 (1)	—
Correctional Service Canada	Access	102	33	66	3
	Misuse	7	1	6	—
	Correction	3	—	3	—
	Delay	255	218	35	2
	Language	6	3	3	—
	Index	1	1	—	—
	Col/Ret/Dis	1 (375)	1 (257)	— (113)	— (5)
Employment and Immigration Canada	Access	34	6	27	1
	Misuse	8	2	6	—
	Delay	10	4	6	—
	Col/Ret/Dis	4 (56)	1 (13)	3 (42)	— (1)
External Affairs	Access	5	1	3	1
	Delay	9 (14)	8 (9)	1 (4)	— (1)
Farm Credit Corporation	Access	1 (1)	—	1 (1)	—
Health and Welfare Canada	Access	6	2	4	—
	Misuse	1	—	1	—
	Delay	3	2	1	—
	Correction	1 (11)	— (4)	1 (7)	—
Indian and Northern Affairs	Access	1	—	—	1
	Misuse	1 (2)	1 (1)	—	— (1)
Immigration Appeal Board	Access	1	—	1	—
	Delay	1 (2)	—	1 (2)	—
Justice	Access	2	—	2	—
	Delay	1 (3)	1 (1)	— (2)	—

Department	Complaint Type	Number (Total)	Justified (Total)	Abandoned (Total)	Dismissed (Total)
National Defence	Access	13	2	10	1
	Misuse	1	—	1	—
	Correction	1	—	1	—
	Delay	49 (64)	28 (30)	20 (32)	1 (2)
National Parole Board	Access	9	2	7	—
	Delay	3 (12)	— (2)	3 (10)	—
National Sciences and Engineering Research Council Canada	Access	1 (1)	—	—	1 (1)
Public Archives Canada	Access	2	1	1	—
	Correction	2	—	2	—
	Delay	1 (5)	1 (2)	— (3)	—
Public Service Commission	Access	2 (2)	1 (1)	—	1 (1)
Public Works Commission	Access	1 (1)	—	1 (1)	—
RCMP	Access	18	4	12	2
	Misuse	3	—	3	—
	Delay	16 (37)	2 (6)	14 (29)	— (2)
Revenue Canada Customs and Excise	Access	2	2	—	—
	Misuse	1	—	1	—
	Delay	8	6	2	—
	Col/Ret/Dis	1 (12)	— (8)	1 (4)	—
Revenue Canada Taxation	Access	14	6	7	1
	Delay	5	1	4	—
	Col/Ret/Dis	1 (20)	— (7)	1 (12)	— (1)
Regional Industrial Expansion	Access	1	—	1	—
	Delay	1 (2)	1 (1)	— (1)	—
Solicitor General Canada	Access	11	—	11	—
	Delay	1 (12)	—	1 (12)	—
Statistics Canada	Access	1 (1)	—	1 (1)	—
Supply and Services Canada	Access	2	1	1	—
	Delay	2 (4)	— (1)	2 (3)	—
Transport Canada	Access	2 (2)	1 (1)	1 (1)	—
Treasury Board	Access	4	—	4	—
	Col/Ret/Dis	1 (5)	1 (1)	— (4)	—
Veterans Affairs Canada	Access	9	2	6	1
	Misuse	1	—	1	—
	Delay	1 (11)	— (2)	1 (8)	— (1)
<b>TOTAL</b>		<b>692</b>	<b>366</b>	<b>310</b>	<b>16</b>

---

### **Information Posted (1588)**

A list of names, ages, telephone numbers, and SINS of job applicants was posted near the office manager's desk at a Canada Post office. The list was clearly visible to anyone using the post office. One person whose name appeared on the list complained that this contravened the *Privacy Act*.

The privacy coordinator's office at Canada Post confirmed that the list had been posted and immediately advised the manager that such personal information should not be displayed where it could be seen by other persons not needing to know. Canada Post also issued guidelines explaining the steps to be followed when posting personal information. The Commissioner considered the complaint justified.

### **Realized Error (1780)**

The Privacy Commissioner received a complaint that Employment and Immigration Canada personnel had improperly disclosed personal information to an American newspaper reporter. The information concerned an application for refugee status. These applications are made during *in camera* immigration inquiries and, therefore, are not publicly available.

The department realized its error before the complaint was made.

EIC has taken steps to advise personnel of proper procedures to be followed to prevent further improper releases of personal information.

### **No Jurisdiction (1502)**

In a September 9, 1985, letter a man complained that Canada Post "maintains computer files of the public's Envoypost correspondence". He was concerned that users of the service do not have access to the database and cannot purge their correspondence from the system.

The problem surfaced when his Envoypost message was received, then misplaced at the Toronto post office. Canada Post subsequently printed and delivered a copy of the original.

On investigation, it was found that Canada Post does not keep copies of the correspondence. It simply prints out the electronic message, transmitted by Envoypost, and delivers the printed copy.

Telecom Canada keeps the message in its main computer memory for 10 days for the very reason the man complained; in case it has to retransmit lost messages. After 10 days the message is purged automatically. Although Envoypost is a joint service between Canada Post and Telecom Canada, the customers, service and computers are Telecom Canada's. Telecom Canada is not covered by the *Privacy Act*. The Commissioner dismissed the complaint.

### **Ensuring Medical Confidentiality (1392)**

A Revenue Canada employee complained that questions on an application form for disability insurance contravened the *Privacy Act*.

He had told the department he could not return to work and submitted his doctor's certification. The department advised that he was eligible for disabili-

---

lity insurance (provided by a private insurance company), and sent him the disability insurance form to complete and return. He felt the information asked for was too personal and confidential to return to the personnel office where it could become common knowledge.

When the office called to remind him to complete and return the form he refused, calling the questions "outrageous". The department warned him that the company would not pay his claim without the form, and the man complained to the Commissioner.

The investigator discussed the case with Revenue Canada's privacy coordinator who called Supply and Services (which prints the form), and Treasury Board (the employer for most federal public servants). It was agreed that the claim could proceed if the man would complete two copies of the form, one copy for the department containing only his identifying information, and the second, with the detailed responses, to be sent directly to the insurance company.

Although satisfied with the outcome, the man asked that his complaint not be closed until a solution was reached which would prevent the same thing happening to others. The investigator met staff from Treasury Board's insurance section to explain the problem and was told later that the board was considering new procedures for handling medical information. The Office's Compliance Branch will monitor the new procedures.

This was the first time anyone had complained about returning the form to a personnel office. Most employees pre-

fer to have personnel staff handle such applications, considering they have the expertise and sensitivity.

The Commissioner found that Revenue Canada was following established Treasury Board procedures and had not contravened the *Privacy Act*. Both the department and the board had been sensitive enough to accommodate the man's concerns and still process his claim.

#### **After Hours Misbehaviour (1134)**

An employee of the Canadian International Development Agency (CIDA), accompanied a consultant under contract to CIDA to a bar where they were involved in an altercation. Another employee told CIDA's security director about the incident and he made informal inquiries, noted it in the employee's file and referred the matter to management.

The information was used in the employee's performance evaluation and he was rejected later on probation. He complained to the Commissioner that CIDA had misused his personal information.

CIDA's security director had been given unsolicited information suggesting the employee was a potential security problem. The director's inquiries did not conflict with the *Privacy Act*. He had the authority to inquire into the incident and to advise senior management because it was a security matter. The incident had a bearing on the employer-employee relationship, and the employee's behaviour as a representative of the agency.

The Commissioner dismissed the complaint.

---

### **Exemptions withdrawn (1167, 1172)**

After two RCMP members were transferred out of a section against their wishes, they applied under the *Privacy Act* to see an audit report which led to their transfer. Both applied later for any personal information in the file under the *Access to Information Act*.

The RCMP told the members that using the Information Act would preclude release of any material since it maintained that audit reports can be exempt under that act. The RCMP processed both requests under the *Privacy Act*, giving the members some personal information but ignoring the preponderance of the material, calling it "non-personal". It also exempted some material as resulting from investigations. Both members complained to the Commissioner.

The investigator suggested that the RCMP reconsider the latter exemptions because the report was the result more of an administrative inquiry than an "investigation".

During discussions, the RCMP reviewed the entire file and agreed to release portions of the "non-personal" information in the audit report that were pertinent to the complainants. Information that was not pertinent; concerned other individuals; would identify a confidential information source, or would injure international affairs or defence, was exempt.

The Commissioner agreed with the later exemptions but found the original complaint justified.

---

## Compliance Branch

---

Section 37 of the *Privacy Act* authorizes the Privacy Commissioner to carry out investigations to ensure that government institutions are complying with the fair information principles embodied in the Act. Under this authority, a compliance branch has been established to "audit" federal government record-keeping. During 1986-87, an audit plan and procedures have been developed to establish the systematic approach to the 147 organizations under the jurisdiction of the *Privacy Act*.

These organizations range from the three person staff of the Pension Appeals Board to the approximately 120,000 employees of the Department of National Defence. The size of the organization is not the only determining factor in assessing "audit risk". The Commissioner must also consider the type of personal information collected, the number of individuals in the data banks, the mechanisms for collecting, storing and disposing of the information.

### Analyzing the Audit Population

The branch developed a computer model by extracting information from a profile questionnaire sent to all departments in 1986. The questionnaire asked departments to describe their organizations in some detail, including their personal information handling policies and procedures, internal audit capabilities, and both data processing and site security requirements.

The computer model, containing 27 elements, assesses the relative risk of each department's personal information handling. With this risk ranking,

the branch organized the departments into those with high, mean, and low audit risk. Those with high audit risk will be the prime targets for the branch's own investigators. For the others, the Commissioner will seek the support of their internal auditors to ensure that personal information handling requirements are met.

Without this approach, the existing compliance staff would take about 12 years to do complete audits of all of the institutions - by any measure an unacceptable audit cycle.

During the past year the branch developed a sampling program to enable investigators to examine vast data banks with a high degree of accuracy. The program does not demand a sophisticated knowledge of data processing or statistics but ensures an accurate investigation based on a minimum sample size.

### Outside the Plan

In addition to planned audits, the Compliance Branch is frequently called on to investigate incidents of unauthorized disclosure such as those previously described in this report. During the year the Compliance Branch completed the following investigations:

#### Statistics Canada:

- lost census forms, Winnipeg
- Urban Forward Sortation Postal Code

#### Employment and Immigration Canada:

- lost surveys, Ottawa
- Grand Forks dump find
- Kitchener microfiche
- Peat Marwick survey



---

National Parole Board:  
theft from member's car

Regional Industrial Expansion:  
files on Ottawa street

**Exempt banks:**

Staff also investigated the following  
exempt banks:

Royal Canadian Mounted Police:  
Criminal Operational Intelligence  
Records, CMP/P-PU-015

National Defence:  
Military Police Investigation Case  
Files, DND/P-PE-835  
Security and Intelligence Information  
Files, DND/P-PU-040

Privy Council Office:  
Security and Intelligence Informa-  
tion Files, PCO/P-PU-005

Revenue Canada/Taxation:  
Tax Evasion Cases, RCT/P-PU-030

---

# The Privacy Act in Court

---

Applicants who believe they have been wrongly denied access to their personal information may ask the Federal Court to review the decision, providing the Privacy Commissioner has already investigated the case. If the Commissioner considers the applicant's complaint to be justified, and he is dissatisfied with the government's response to his recommendations, he may, with the complainant's consent, take the case to court.

There have been no circumstances during the past year in which the Commissioner has not been satisfied with a department's response to his adverse finding.

Few complainants ask for a court review, in part because 87 per cent of applicants receive all or most of their requested information. The Privacy Commissioner is participating in the cases which follow. Other case reviews under the *Privacy Act* are now described in the Treasury Board's bi-annual Bulletin.

The court only reviews a complaint that a department has denied access to personal information. It does not review the Commissioner's investigation or decision. However, the Commissioner may ask the court to review a file that he believes is improperly contained in an exempt bank.

## **Ternette v. Solicitor General of Canada**

The application of Nick Ternette to see his personal information in an exempt bank is still before the courts. The case was described in detail in the 1985-86 annual report.

## **Mary Bland v. the National Capital Commission**

This complaint was lodged under the *Access to Information Act* after the National Capital Commission (NCC) refused the applicant's request to see its list of tenants and the amounts of rents the tenants paid. The Information Commissioner recommended that the NCC release the addresses and amounts of rent of the residential tenants "in the public interest". The Privacy Commissioner is an intervening party to the case in order to give his interpretation of the relevant sections of the *Privacy Act*.

# Corporate Management

Corporate Management provides both the Information and Privacy Commissioners with financial, personnel, administrative, data processing and library services. During the year responsibility for public affairs was transferred to the respective Commissioners.

## Finance

The Offices' total resources approved by Parliament for the 1986-87 fiscal year were \$3,624,730 and 56 person years, an increase of approximately \$400,000 over the 1985-86 expenditures. Personnel costs of \$2,783,000 and professional and special services expenditures of \$393,000 accounted for more than 88 per cent of expenditures. The remaining \$438,000 covered all other expenses.

## Personnel

Staff increased by two during the fiscal year, to a total of 53 on March 31, 1987. There were 11 staffing actions during the year, including appointments to three senior management positions: assistant Information Commissioner, director of Privacy Compliance, and director general of Corporate Management.

## Administration

During the year, Treasury Board authorized additional office space to relieve a serious shortage of accommodation. The Office upgraded its telephone system and added a second toll-free telephone line to help out-of-town callers reach the Offices.

The following are the Offices' expenditures for the period April 1, 1986 to March 31, 1987.

	Information	Privacy	Administration	Total
Salaries	\$ 906,344	\$ 975,118	\$ 546,389	\$2,427,851
Employee benefit plan contributions	135,300	129,950	89,750	355,000
Transportation and Communications	44,585	43,984	82,598	171,167
Information	84,274	38,567	4,816	127,657
Professional and special services	335,093	37,970	20,323	393,386
Rentals	—	75	14,697	14,772
Purchased repair and maintenance	—	322	5,103	5,425
Utilities, material and supplies	1,779	3,694	36,695	42,168
Construction and equipment acquisition	3,220	7,642	64,753	75,615
All other	46	753	12	811
<b>TOTAL</b>	<b>\$1,510,641</b>	<b>\$1,238,075</b>	<b>\$ 865,136</b>	<b>\$3,613,852</b>

---

---

## **Data Processing**

The Office continued to convert data it previously gathered manually to electronic systems. This improved efficiency and the Offices' ability to handle an ever-increasing workload without increasing personnel.

## **Library**

This special library provides an information and referral service for both Commissioners. Its collection is open to the public for reference and research, and interlibrary loans may be arranged. The collection includes books, magazines and government reports, newspaper clipping files and periodical articles on privacy, access to information, and the ombudsman function. The library also has access to several automated bibliographic data bases. During the past year, the library acquired approximately 440 books and answered 512 reference questions.

---

## Inquiries

---

Word is getting out about using the *Privacy Act*. There was a noticeable drop this year in the number of requests for the Privacy Commissioner to "send me all the information in my file". Inquiries about using the Act, misdirected applications, and questions of interpreting particular sections of the Act accounted for 58 per cent of the 1,062 inquiries this year, compared to 69 per cent a year ago. Twelve per cent of the inquiries concerned Social Insurance Numbers and another 12 per cent were about personal information held by organizations not subject to the *Privacy Act*.

In the "other" category (18 per cent of the total—up from six per cent last year), callers wanted to know, for example, whether they had to buy car insurance, how to get a student visa to enter the United States, how to transfer a pension from one employer to another, and inevitably—how adopted children could track down their natural parents.

An additional 185 inquiries concerned both the Access to Information and *Privacy Acts*. These were divided between privacy investigators and the Information Commissioner's staff with whom the Privacy Commissioner shares offices.

A second toll-free line was installed in October to handle the increasing volume of out-of-town calls. Since the Commissioners do not have regional offices, this toll-free number is listed in telephone directories across the country. There were 2,532 calls on these lines during the year.

The offices received 650 requests for information material, many for more than 100 copies.

---

## Spreading the Word

---

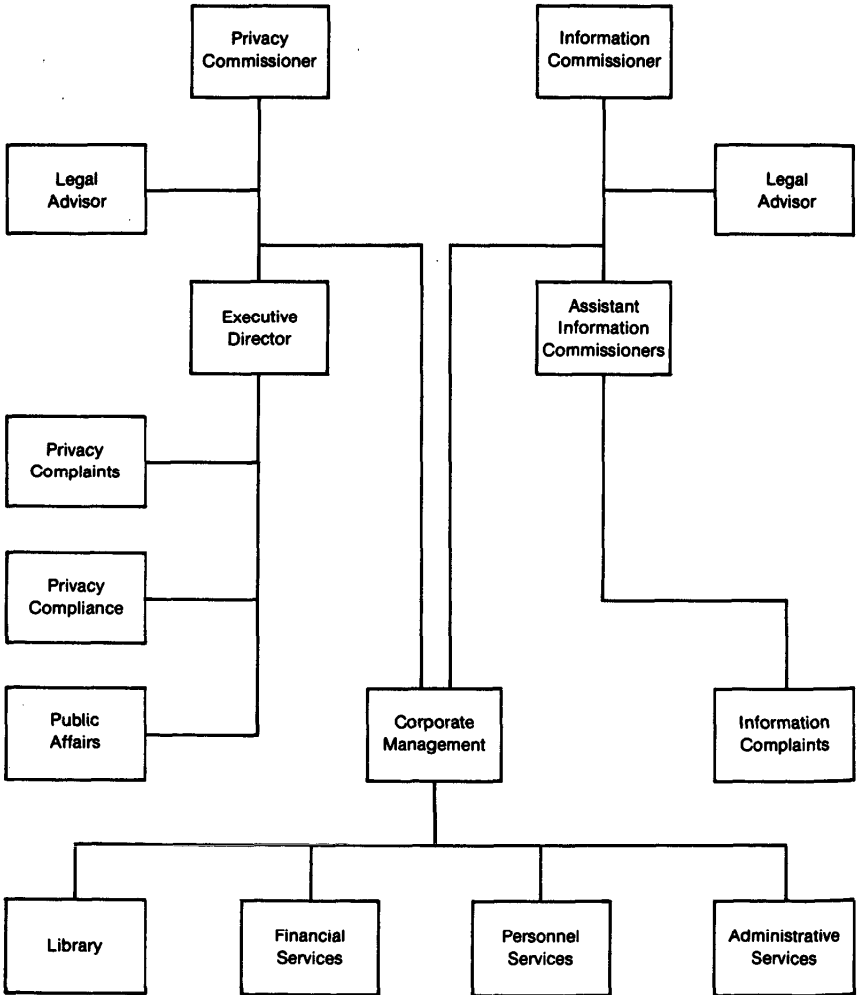
The Commissioner welcomes opportunities to inform Canadians of privacy issues and to tell them about the *Privacy Act*. During the year he spoke to 22 diverse organizations including Canadian Clubs from Kelowna, B.C., to Shawinigan, Quebec, the National Conference on Management in the Public Sector in Victoria, the Institute of Public Administration in Vancouver, the Association of Records Managers and Administrators in Ottawa, the Canadian Public Personnel Management Association in Charlottetown, Computer Professionals for Social Responsibility in Toronto, the International Bar Association in New York, and public administration students at Dalhousie University in Halifax.

The Commissioner's staff regularly briefs participants of the federal public service senior management course and speaks to professional associations and federal public servants. During the year privacy investigators presented seminars to a national ombudsman's workshop in Victoria.

# Appendix I



Offices of the  
Information and Privacy  
Commissioners of Canada



# Appendix II



Government of Canada / Gouvernement du Canada

Privacy Act

## Personal Information Request Form

For official use only

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

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

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

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

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

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

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

Federal Government Institution

Registration Number and Personal Information Bank or Class of Personal Information

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

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

Method of access preferred

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

Identification of applicant

Name (or previous name)

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

Street address, apartment

City or town

Province, territory, or other

Postal Code

Telephone number(s)

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

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

Signature

Date

Canada

Français au verso

TBC 350-58 (Rev. 85/8)



---

## Appendix III

---

### **Government Institutions Covered by the Act**

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

---

---

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

---

---

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

---

---

Social Development, Ministry of  
State for

Social Sciences and Humanities  
Research Council

Solicitor General Canada

Standards Council of Canada

Statistics Canada

Statute Revision Commission

Supply and Services Canada

Tariff Board

Tax Review Board

*Textile and Clothing Board*

Transport Canada

Treasury Board Secretariat

Veterans' Affairs Canada

War Veterans Allowance Board

Yukon Territory Water Board