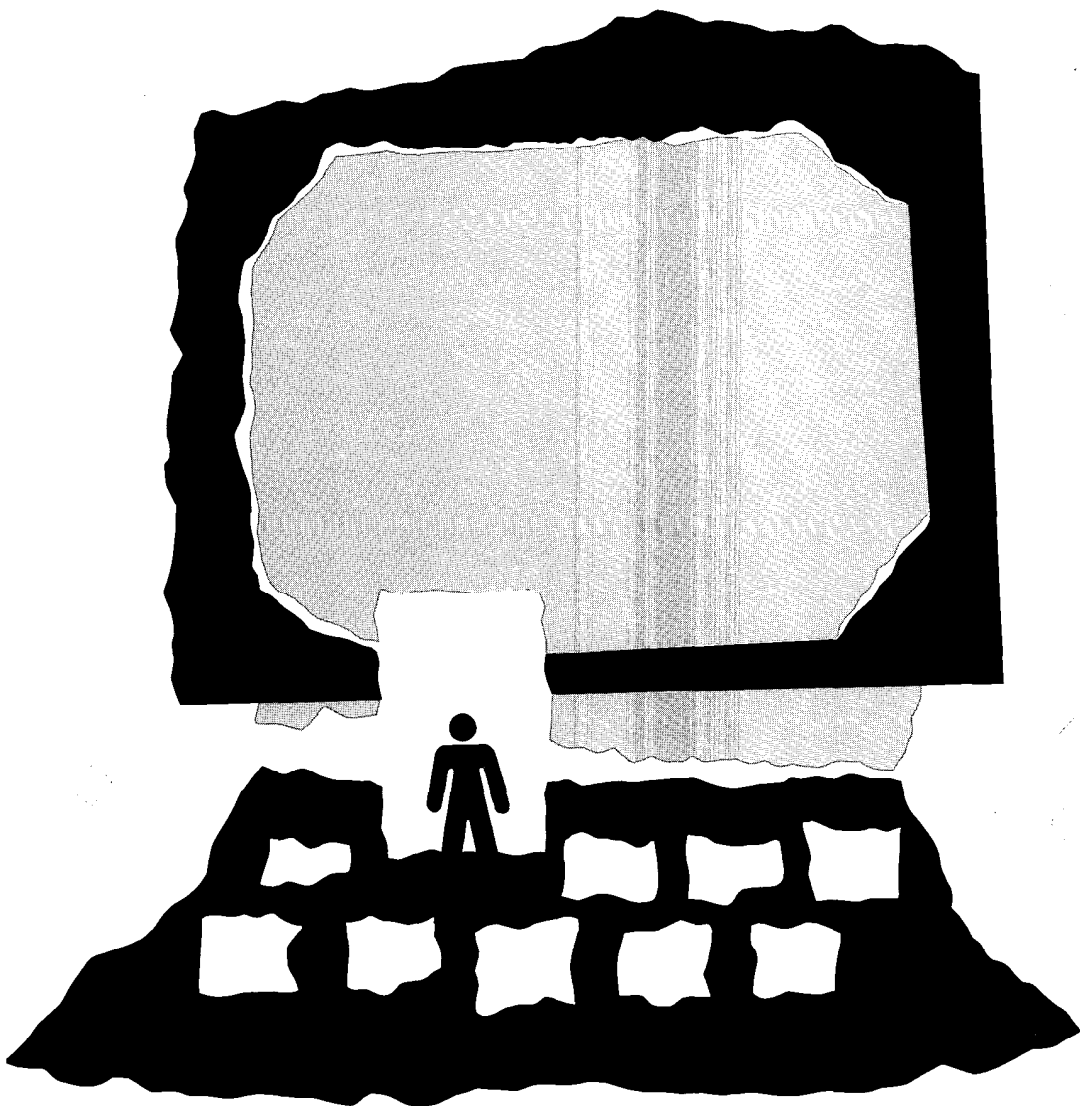




Privacy Commissioner

Annual Report 1988-89



**Annual Report
Privacy Commissioner
1988-89**



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

© Minister of Supply and Services Canada 1989

Cat. No. IP 30-1/1989

ISBN 0-662-56842-7

“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*

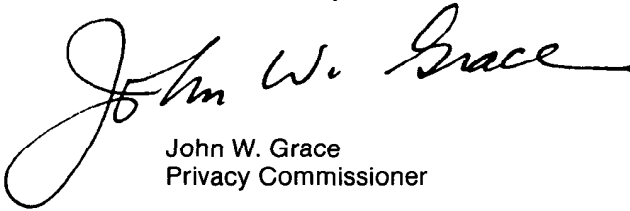
The Honourable Guy Charbonneau
The Speaker
The Senate
Ottawa

June 30, 1989

Dear Mr. Charbonneau:

I have the honour to submit to Parliament my annual report. This report covers the period from April 1, 1988, to March 31, 1989.

Yours sincerely,

A handwritten signature in black ink that reads "John W. Grace". The signature is written in a cursive style with a large, looping initial "J".

John W. Grace
Privacy Commissioner

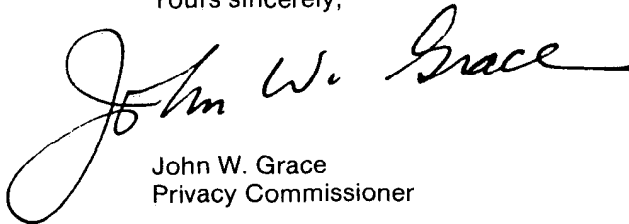
The Honourable John Fraser, P.C., Q.C., M.P.
The Speaker
The House of Commons
Ottawa

June 30, 1989

Dear Mr. Fraser,

I have the honour to submit to Parliament my annual report. This report covers the period from April 1, 1988 to March 31, 1989.

Yours sincerely,

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

John W. Grace
Privacy Commissioner

Contents

Mandate	01
A Mixed Review	02
Who's in Control Here?	10
AIDS and Privacy	14
The Dawn of the Biotechnological Age	16
Computer Security	18
CSIS Files	20
What's with the Cheque?	22
Complaints Directorate	24
Cases	26
Inquiries	38
Compliance Directorate	39
Canada Post	42
Pension Appeals Board	44
Science Council of Canada	44
Department of Finance	45
Ministry of the Solicitor General	46
Employment and Immigration Canada	47
Notifying the Commissioner	50
Spreading the Word	53
Corporate Management	54
Appendices	
I Organization Chart	56
II Government Institutions covered by the Act	57

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

Individuals in Canada 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, using or disposing of personal information in a way which contravenes the *Privacy Act*.

The Privacy Commissioner's 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.

A Mixed Review

The measure of a year's results in the privacy business can be as variable as the standards used for the calculation. It may even be fraudulent to attempt to sum up the privacy state of the nation with catchy generalizations. The subject is now simply too complex to be reduced to neat themes.

Even the Supreme Court of Canada mixed the results. Here was a year in which the court pronounced in *Her Majesty the Queen v. Brandon Roy Dyment* that "privacy is essential for the well-being of the individual" and the "restraints imposed on government to pry into the lives of the citizens go to the essence of a democratic state". The message could not be clearer or the source more definitive.

Here the court was re-inforcing its earlier opinion that the protection of "individuals from unjustified intrusions upon their privacy" is established by section 8 of the Charter of Rights and Freedoms ("everyone has the right to be secure against unreasonable search and seizure"). The judgment in the *Dyment* case, written by Mr. Justice G. V. La Forest, also set forth the following key principle: "If the privacy of the individual is to be protected, we cannot wait to vindicate it only after it has been violated....Invasions of privacy must be prevented and, where privacy is outweighed by other societal claims, there must be clear rules setting forth the condition in which it can be violated."

The *Privacy Act* is precisely a compendium of such rules. In two cases now, the Supreme Court has given the *Privacy Act* the strongest possible constitutional underpinning, making explicit the application of section 8 of the Charter to privacy protection.

Parliament can take some satisfaction in being ahead of both the Charter and the Supreme Court in having established by the *Privacy Act* the rules to control government uses of personal information collected from its citizens. Parliament is not always thus in advance of the courts in these litigious days.

But the privacy news from the legal front does not bring unalloyed joy. The Supreme Court of Canada's decision in *Stewart v. Her Majesty the Queen* appears to set back the cause. In this case, the court ruled that confidential information cannot be stolen because it cannot be considered property for the purpose of the Criminal Code.

In the case, a union, attempting to form a bargaining unit at a hotel, was unable to obtain the names and addresses of some 600 employees because management treated this information as confidential. A consultant hired by the union obtained the list through a security guard who, for a fee, copied the names from a list on the hotel's premises without removing, or in any way altering, the original document. The consultant was charged under the Criminal Code with counselling to commit fraud, theft and mischief to the private property of the hotel and its employees.

The Ontario Court of Appeal's conviction was overturned by the Supreme Court (in a unanimous decision). Mr. Justice Antonio Lamer wrote for the court that "confidential information is not of a nature such that it can be taken because if one appropriates confidential information without taking a physical object, for example by memorizing or copying information...the alleged owner is not deprived of the uses or possession thereof". The judgment went on to observe that "one cannot be deprived of confidentiality because one cannot own confidentiality".

With great respect, as lawyers ritualistically intone, these observations have alarming implications for the information society in general and the *Privacy Act* in particular. If the *Privacy Act* promises anything, it is the promise of protection for the confidentiality of personal information collected by government institutions. That fine legal point of whether one can own confidentiality is simply irrelevant to the important business of keeping sensitive information confidential.

If this non-lawyerly reading of the court's decision is correct, insufficient weight was given to the significant injury which can occur through unauthorized access to huge amounts of sensitive personal information held by both government and the private sector.

While possible commercial harm seemed uppermost, perhaps exclusively, in the mind of the court, terrible personal tragedy could be the result of the unauthorized disclosures of Royal Canadian Mounted Police investigation records, Canadian Security and Intelligence Service surveillance reports, Health and Welfare medical files — to stay with government.

Yet, the court seems to have said that records could be memorized — or copied (or photographed?) — without any criminal sanctions as long as documents are not physically appropriated.

Stewart v. Her Majesty the Queen did not receive the public attention it deserved. Had the information been sensitive health or financial records and not a mere list of names involved in a commonplace labor dispute, the outcry would have been enormous — and deservedly so.

The *Privacy Act* contains no sanctions. Until this Supreme Court decision, a theft conviction under section 298(1) of the *Criminal Code* or a fraud conviction under section 328(1) seemed deterrent enough. Thus it has seemed unnecessary to argue for a sanction provision in the *Privacy Act*. Now the assumed Criminal Code support has been removed.

True, a breach of trust offence remains. It was the charge successfully prosecuted in the case of the Revenue Canada employee who stole the income tax records of some 16 million persons from a Toronto office of Revenue Canada. However, this offence would not be relevant in situations where confidential personal information is taken by a non-public servant or is elicited by deceit from a public official.

Shortly after the decision was delivered in *Stewart v. Her Majesty the Queen*, the Privacy Commissioner raised his concerns with the then Minister of Justice, the Honourable Ray Hnatyshyn. The Minister felt that, despite the Supreme Court's decision, the *Criminal Code* would continue to deter the improper disclosure of information by public officials. He reiterated the government's commitment to amend the *Privacy Act* to provide a statutory basis for the security standards now contained in the Security Policy of the Government of Canada. The Minister noted 1985 amendments to sections 301.2 and 387(1.1) of the *Criminal Code* which created offences dealing with the integrity of computer systems and services and which protect computerized data including personal information.

However, there continues to be a gap in the law which Parliament should close because significant amounts of personal information are held by government in paper files and since compromise of such information by outsiders cannot be ruled out.

The Supreme Court concluded in *Stewart v. Her Majesty the Queen* that Parliament and not the courts should decide what protection be given to confidential information. Parliament needs to act upon that invitation and protect the integrity of the *Privacy Act*.

In passing that Act, Parliament made an explicit commitment to Canadians that the confidentiality of their personal information held by government would be respected. That is the bedrock upon which this legislation rests. If confidential information can be appropriated with no fear of sanction because "one cannot own confidentiality" then the promise Parliament made in the *Privacy Act* has been, at the least, seriously eroded.

"Owning" confidentiality could be enormously more important than owning physical objects. They, after all, can be replaced. But the loss of privacy is non-renewable. Its loss is nothing less than losing control, a diminishing of human dignity.

Hold the Applause

If it was a good news, bad news privacy year from the Supreme Court, so it was from government. The fairest measure of the government's performance is to test it against its own key commitments and timetable set out in *The Steps Ahead*, which was issued in 1987 in response to the unanimous recommendations of the Justice and Solicitor General Committee. That entirely reassuring document was greeted in this report last year with something of the reverence that the Ten Commandments received at Mount Sinai. When put in place, it was said, the new policies and proposed amendments to the *Privacy Act* would make Canada's third-generation privacy legislation "as good as any in the world".

The government's "plan of action" called for achieving all its goals by the end of 1988. Specific commitments were made: "begin immediately" the process of bringing Crown corporations under the *Privacy Act*; establish the Personal Information Index (the guidebook to the government's holdings of personal information) as a data base and to make it available in machine-readable form. The processes may have begun, but more than a year later these commitments had not been realized.

Other target dates were not met. Directives covering consultation with the Privacy Commissioner on issues with data protection implications were to have been issued by spring, 1988. Amendments to the *Privacy Act*, including the promised statutory basis for information security standards, were to be introduced by the fall of 1988. A public education program on behalf of the *Privacy Act* was to be in place by winter, 1988. Not only were the dates missed, nothing had occurred in these matters as of March 31, 1989.

Of course, these were self-imposed deadlines. Under-estimating implementation difficulties because of over-enthusiasm should not be too much faulted. Besides, some key commitments were made good, if somewhat later than promised. The will to proceed with the unfinished business appears generally strong.

But the sluggishness and the slippages are disappointing.

The next 12 months will demonstrate whether *The Steps Ahead* will be meaningful or largely an empty metaphor. Will the walk in *The Steps Ahead* turn out to be a stroll in the park? In the privacy business today, the Queen's counsel in Lewis Carroll's *Through the Looking Glass* should be the guide:

"Now, *here*, you see, it takes all the running you can do, to keep in the same place. If you want to get somewhere else, you must run at least twice as fast as that".

Two Steps Forward

In last year's annual report, the government was congratulated for making good on two commitments — a new policy controlling the government's own use of the Social Insurance Number (SIN) and new controls on the matching or linking of unrelated data bases. Alas, the government's pace did not match the Privacy Commissioner's enthusiasm. Though the SIN and data matching policies were announced earlier, final approval was given only in April, 1989 — technically outside this reporting year.

Yet, the cliché "better late than never" is appropriate in this case. A year's delay does not take away from the significance of the accomplishment. The data matching controls were described here extensively last year.

The tough new restrictions on the government's own uses of SIN are worth revisiting; they represent the most significant of the major commitments on which the government has made good. The President of the Treasury Board put the issue precisely:

“Many Canadians feel threatened by the use of the Social Insurance Number as a universal identifier. With the rapid development of computer technology, there is a growing concern that the SIN may be misused for linking personal information in ways that may pose a threat to individual privacy”.

Thus was announced the “first step by the government” to cap its collection and use of the SIN. A large number of existing uses of the number are to be eliminated over five years and from now on any proposed new collection of the SIN for administrative purposes, other than an existing, approved list, is to be sanctioned by Parliament itself.

The new policy stands up against every natural bureaucratic urge in the public and private sector. It is the first time any government has attempted to roll back the use of its own numerical identifier. Omelettes are more easily and less expensively unscrambled (the estimated cost of \$16 million may be low). But it's being done!

No more will the SIN be a public servant's principal employee number; the armed forces lose the SIN as the military service number. Applicants for permanent residence in Canada will not come with a SIN, nor will applicants for citizenship be required to submit to a SIN.

Commercial fishermen seeking permits, taxpayers applying for fuel tax rebates, candidates for grants and fellowships — all these and others are set free from the usages of the SIN.

It is something of a paradox that an age which has all but lost the concept of sin has so come under the sway of SIN. Babies have been given a SIN as a birth registration number in Prince Edward Island and some funeral directors are said to ask for the SIN of the deceased: thus SIN from cradle to grave; SIN even unto death.

In putting its own house in order, the federal government has new moral as well as legal authority to make good on yet another warning issued to other levels of government and the private sector. Continued mindless and insensitive demands for the SIN invite legislation — and that would be deserved.

...A Step Back

Just three months after the announcement of an enormously encouraging policy to control the SIN, Parliament passed amendments to the *Income Tax Act*, among which required Canadians to disclose their SINs to financial institutions where there had been no such compulsion before. Suddenly, even a bank account couldn't be opened without a SIN.

The new policy was designed to facilitate the reporting of interest income to Revenue Canada, an almost noble purpose. Unfortunately, little or no effort was made to notify the public in advance of the purpose of this new collection and use of SIN.

Despite government's promise to consult the Privacy Commissioner in initiatives affecting privacy, no consultation was undertaken before the legislation was introduced. The efficiency of tax collection was accepted by the government as justifying a new use of the SIN without any apparent consideration of the inherent privacy dangers.

In the complexity and detail of the amendments to the *Income Tax Act*, the extension of the SIN and its significance was missed by members of Parliament, the media and, yes, the Privacy Commissioner's Office. One simply did not expect such legislation to contain anything of interest to the business of privacy protection. Of course, the fact that it did demonstrates the vulnerability of privacy to assault from the most unexpected quarters.

The provisions in the new *Income Tax Act* amendments have, for the first time, made it a punishable offence to refuse to provide a SIN. Government institutions have had by statute and regulation the authority to demand SINs, mainly for such social programs as unemployment insurance and pensions. (No number, no coverage, no benefits). Now, no number and a \$100 fine. (What happens for refusing to pay the fine is not clear. Two days in jail?)

Another precedent is established here. Until these income tax amendments, Canadians were required by law to give their SINs only to the federal government. Now they must confess their SINs to banks, trust companies, stock-brokers, credit unions, whenever and wherever they make what looks like an interest-bearing investment. Welcome to the computer society.

Of course, taxes should be paid. There is a relentless consistency in applying the new law once the \$1,000 interest deduction was abolished. But the implications of the new demands for the SIN with the penalty for failure to comply are much more sweeping than anyone appears to have realized. The pity is that no one thought to ask or even to explain.

So soon after announcing the admirable policy to restrict the government's use of the SIN, thousands of private sector institutions (consider the number of bank branches alone!) are authorized to maintain new records systems with the SIN as the identifier. The fact that there is a fine of \$5000 for misusing the SIN is small consolation.

...and Another

In *The Steps Ahead*, the government committed itself to extending the jurisdiction of the *Privacy Act* to cover Crown corporations and their subsidiaries. Such action would almost double the number of institutions covered and, most important, would give visible leadership to the private sector. In implementing the fair information practices, the government was putting its own full house in order.

Since many of these Crown corporations are in direct competition with private sector companies, the coverage by the *Privacy Act* conveys the strong message that the government believes data protection can be a complement, not an obstacle, to good business. Canada Post, after all, has been subject to the legislation for five years and in the face of significant competitive pressures finds that life under the *Privacy Act* does not hinder it commercially.

Though the bulk of the Crown corporations may yet be covered (members of the Privacy Commissioner's Office travelled as part of an awareness task force, meeting representatives of some 21 corporations), two significant omissions, as well as the general delay, have marred the government's initiative. Neither Air Canada nor Petro-Canada were included on the list of institutions to be brought under the *Privacy Act*.

Air Canada has been exempted because it no longer is a wholly-owned government creature — a dubious ground indeed because the government continues to maintain majority ownership, whatever the future may bring. That itself is reason to hold the government to its original pledge. It would be a dangerous precedent in this age of privatization if mixed ownership were enough to exempt Crown corporations from federal legislation. Until now, it has not. Air Canada itself remains subject to the *Official Languages Act* and, presumably, it would even if it were to be completely privatized. Surely the privacy rights of Air Canada's customers and employees are as important as their linguistic rights.

Other western democracies have recognized the need to bring under data protection codes the vast amount of personal information held in the computers of air carriers. If British Airways can live with the United Kingdom's data protection legislation, Air Canada should be able to live with the *Privacy Act*.

With Petro Canada, ownership is not the issue; Petro Canada is a Crown corporation, pure and simple. But corporation's management has resisted the *Privacy Act* because of perceived difficulties with its operations if it had to live within the Act's principles.

Perhaps Petro Canada's life would be made easier if, for example, the credit files of its customers or lessees did not have to be opened up to those customers or lessees, as they would have to under the *Privacy Act*. Being held exempt from the more onerous demands of human rights or employment equity laws would also make Petro Canada's life easier. But there is no chance of such exemptions. The argument for the legal protection of the privacy rights of Petro Canada's employees and customers is at least as strong.

If such high-profile institutions as Air Canada and Petro Canada were both to be excused from the *Privacy Act*, the government would be rightly viewed as undercutting its own commitments. Almost every institution, public or private, can conjure up reasons to be made exempt from oversight legislation — privacy or otherwise.

Via Rail could object to the *Privacy Act*, so could the Canadian Broadcasting Corporation. Yet both of these institutions (the CBC with some special provisions to protect its news gathering activities) are to be covered.

There may seem to be an air of blissful or naive unreality to a plea to bring two Crown corporations under the *Privacy Act* when the entire private sector, including federally-regulated companies, operates outside the Act. Why worry about Air Canada when other Canadian airlines fly the friendly skies unimpeded by the binding rules of fair information practices? Why insist that the customers of Petro Canada be given the benefits of the *Privacy Act* while those of all its competitors are left to fend for themselves?

Two more institutions in or out of the *Privacy Act* will not make much difference to the overall standard of privacy protection in the country. But if government doesn't insist that its own creatures obey the privacy rules of the road, the private sector is not going to be impressed by preachments to adopt codes such as the data protection principles of the Organization for Economic Co-operation and Development (OECD).

Self Regulation?

All of which raises the effectiveness of the government's effort to encourage private sector firms to respect those OECD guidelines to which Canada is signatory. The Minister of External Affairs' request to major companies to implement these guidelines in their organizations does not appear to have brought any discernible results.

The federal government met on two occasions with provincial governments to develop strategies to encourage the private sector to accept and enforce the guidelines. However, no agreement has apparently been reached as to what business sectors are to be targeted or the strategies to be devised.

The government needs a more vigorous approach. That is the least it can do in light of its rejection of the unanimous recommendation of the Standing Committee on Justice and the Solicitor General that the entire federally-regulated private sector be made subject to the *Privacy Act*.

That recommendation was not accepted (a decision which the Privacy Commissioner supported) because self-regulation seemed to be the preferred way to travel in a time when deregulation is in fashion. There have been faint stirrings towards self-regulation and there was no evidence of endemic or widespread abuses. Moreover, could a single privacy law be constructed to cover the diversity of the private sector — from banks to cable television companies? Perhaps not. There are practical limits to enforceable regulation in the age of micro-computers. A swollen Privacy Commissioner's Office with brigades of inspectors would give even privacy a bad name.

Self-regulation will be for most, including the Privacy Commissioner, the preferred option to government regulation. Recent "second generation" data protection laws (Ireland, Australia and Japan all adopted legislation within the past 12 months) have been much closer to Canada's model than to the "first generation" laws of Sweden and France which covered the private sector. Without more evidence of effective self regulation, however, the supporters of voluntary data protection codes will be increasingly hard put to defend their position.

Who's in Control Here?

The demands for personal data continue to grow exponentially and unchecked. Arthur Miller, who teaches law at Harvard University, says that his ability to fly depends not on the fact that he is standing at an airport counter waving a ticket. So far as the airline is concerned, unless the right numbers come up on a computer, "I do not exist. I am a mere three-dimensional version of the two-dimensional screen". Let Mr. Miller continue:

"It's not just an airline reservations system. It has my name. It has my telephone number. It has my credit card number. It has who I'm flying with. Whether I've got hotel reservations or a car rental through the system...that's a dossier, and I know it."

And there are more dossiers. Arrive at a hotel and, he says, "you're not going to lay your head down on a Sheraton pillow unless its computer recognizes you. You put it all together and you realize that your life is controlled by one data bank after another, made possible by the computer."

It is a price for convenience and efficiency. No one is suggesting smashing the computers. But ground rules for the handling of the vast amount of personal information being collected should be put in place and respected. Data collections are available, on command, for making the important decisions about us. Arthur Miller is right:

"We have come to understand that it is impossible to get insurance, to get credit, to get certain jobs, get certain government benefits without going through record clearance and record approbation — that people will be looking through our files. Who they are, we don't know. Where they are, we do not know. What the criteria for decision-making might be, we do not know."

We do know (or should!) that information about us in computers can be wrong. But without privacy legislation or working, effective voluntary codes, there is no opportunity to see and correct one's file. Without privacy legislation or enforced codes, there is nothing to stop the frightening growth industry in the sale and exchange of computerized personal information, of data chronicling personal consumption habits (traced through credit card transactions and direct mail orders) and charitable or political contributions.

Who's in control here? Is it individuals of their own information? Or is it personal information collectors and traders with their marvelous machines? To become a "data subject" should not mean becoming any less a human being. Should that ever be conceded, civilization has become subject to its machines and our information societies will have evolved, as Professor David Flaherty of the University of Western Ontario has warned, into "surveillance societies".

Professor Flaherty, an internationally-recognized authority on privacy and data-protection laws, put it in almost apocalyptic terms:

“The various automated data bases now in existence make possible fairly integrated monitoring of individuals in Western countries. The proliferation of such information banks in both the public and private sectors, rather than the existence of any single one of them, poses the fundamental challenge to privacy interests. We need to think about the implications of such surveillance practices for the protection of human rights. In North America in particular, the application of information technology is galloping ahead of regulation and control”.

Stripped of one's power to control what the world knows about oneself is demeaning and dehumanizing. There is nothing fringe or dilettantish about claiming privacy rights. They go to the heart of human integrity, of dignity and the kind of society we want. This is why privacy matters.

Privacy matters most of all between citizens and governments because the state has enormous power to extract and use personal information.

Yet, a privacy concordat covering the marketplace is becoming almost as important. Even when personal information is voluntarily given (in many transactions there is precious little voluntariness, e.g., an application for credit), well-defined rules have become essential if individuals are to have at least residual control over the uses of such information.

Some privacy experts, including Professor Flaherty, have come to believe that it is now too late for volunteer privacy concordats in the private sector. They argue that only legislation can control the powerful new technologies and give personal information at least a minimal level of protection. Back to battalions of privacy inspectors and very red bureaucratic tape!

Another privacy scholar, Professor James Rule of the State University of New York, advocated recently that the best way to protect informational privacy is by giving individuals a copyright interest in the commercial use of their own personal data. Information could not be sold or exchanged for value without an individual's permission. An ingenious, fascinating, even logical concept, though highly improbable and unenforceable.

These are desperate solutions, born of frightful visions. Surely there exists a middle way.

The voluntary rules of the privacy road such as the OECD guidelines are entirely sensible and, if implemented, offer some reasonable reassurances. But it has become time for government to treat volunteering in this business much as “volunteers” are traditionally found in the armed forces.

Federally-regulated firms, which the Parliamentary Committee recommended unanimously should be made subject to the *Privacy Act*, would be the place to start. In addition to pursuing more vigorously a cooperative strategy with the provinces to encourage voluntary compliance with the OECD privacy guidelines, the Government of Canada should take on the federally-regulated private sector in a second front of privacy protection activity. Develop effective privacy codes, within a specified time, they should be told, make them known to your customers and employees (who will be delighted!) or, yes, face legislation.

The proponents of privacy laws for the private sector are right about one thing — gentle exhortation has not much worked. But better first to turn the screw a little than impose the heavy apparatus of legislated privacy protection.

Dial Bell for Data

The Privacy Commissioner has not been merely watching these issues from the sidelines, content simply to grade the government's performance. He stepped into the fray upon learning, last November, that the Canadian Radio-Television and Telecommunications Commission was examining whether, to whom and under what conditions, Bell Canada could sell its telephone directory data base of white and yellow page subscriber listings in machine readable form. The initiative was not Bell Canada's but that of companies who have been eyeing Bell's data base with some envy.

This proposal offers chapter and verse on how real the pressure is for the massive exchanges of computerized personal information. At the same time, it is a textbook example of how a sensitive regulatory agency should be alertly aware of the stakes.

In a nice understatement, the CRTC noted that "the provision of this information in machine-readable form may heighten concerns related to customer privacy". "Heighten", indeed! Though nothing is more public than a telephone book, there are good reasons why phone customers should be worried. The Privacy Commissioner put them forward in a formal intervention which asked the CRTC not to require Bell Canada to offer its directories data base to anyone willing to buy.

The reason is this: a qualitative change takes place when names, addresses and phone numbers are moved from paper listings to electronic data processing disks. Special privacy dangers arise because of the infinitely greater accessibility, transmittability and transformability (even the words are ominous) of data in machine readable form. And nothing is closer to home than a telephone book.

One company has already transferred to a 4.7 laser disk the names, addresses and phone numbers of 7.9 million of Canada's 8.5 million households. It was a slow, expensive (more than \$1 million, and this in Pakistan) job.

The phone book was only the start. The same laser disk includes the coordinates of each household to within one meter on a grid map of Canada, the names of neighbours, electoral districts, the length of time the occupant has been at that address. Information from 12 demographic fields (sold in aggregated form by Statistics Canada) offers census data as to probabilities of income, language, religion and children. All this is information in the public domain. But add credit card or banking information, if such information was to be made available by fair means or foul, and the result is profiling of the population on a mass, systematic scale.

It is a marketer's dream — a privacy nightmare. Machine-readable listings mean that personal information can be manipulated in any number of creative ways for telephone or mail soliciting. Yet, that would be an almost benign use. Such listings also provide a monitoring or tracking tool of interest not only to marketers but to criminals and, yes, law enforcement agencies alike.

Phone subscribers never dreamed of, much less consented to, this degree of privacy invasion just by the fact of being listed in the telephone directory. Technology makes the danger real and present.

AIDS and Privacy

On another front, and as promised in last year's annual report, the Privacy Commissioner developed recommendations to ensure that AIDS-related personal information is handled by the federal government in accordance with the letter and spirit of the *Privacy Act*. The resulting report, entitled *AIDS and the Privacy Act*, confirms that an appropriate national response to AIDS is perhaps the most sensitive and anguished privacy issue of our time. *AIDS and the Privacy Act* seeks an elusive balance between protecting the privacy of those either with AIDS or infected with the HIV (the virus that causes AIDS), and appropriate disclosures which the protection of others demands.

Compassion towards those afflicted demands that they are protected from the further trauma of unnecessarily invading their private lives and disclosing their condition. The diagnosis of AIDS continues to be a sentence to death. In fact, some current opinion suggests that simply carrying the HIV virus also means early death.

Unthinking and extreme public or government responses to the disclosure of AIDS or HIV infection may, and in some cases have, altered the very conditions of an individual's membership in society: access to schools, work, medical care, even family and friends. That is the simple case to be made for the deepest possible respect for the privacy of the victims.

On the other side, however, disclosure is required, though not nearly as often as is sometimes suggested. Scientific and medical communities may need to know who are the AIDS victims and HIV carriers in the quest to slow, stop or treat the disease. These competing concerns often call for conflicting courses of action.

The report concludes that mandatory HIV antibody testing of such groups as public servants, inmates of federal prisons, immigrants and long-term visitors to Canada, would contravene the *Privacy Act*. The *Privacy Act* prohibits the collection of personal information which is not related directly to a program or activity falling within the statutory mandate of a government institution. Such testing is not a necessary element of any present legislated program.

Of course, Parliament has the authority to override the *Privacy Act* and give government the power to subject groups of individuals to mandatory HIV antibody testing. However, any such action would represent an hysterical over-reaction to the AIDS epidemic — at least so it appears in the present state of knowledge about the disease.

Any public health benefits that would be achieved through large-scale testing are dubious at best and would be far outweighed by the devastating invasion of privacy which would result. Fortunately, privacy interests accord with the most informed medical opinion that AIDS testing should always be voluntary with pre-and post-test counselling.

The Government of Canada has an important leadership role to play in ensuring that AIDS is sensitively handled in the workplace. The report urges Treasury Board, as Canada's largest employer, to issue a comprehensive policy on AIDS in the workplace.

Confidentiality is an integral part of the workplace policy suggested by the World Health Organization. The employee should not be obliged to inform the employer about his or her HIV status, nor is there any need to inform co-workers. If AIDS-related personal information is volunteered, it should be accorded a high degree of protection and, prior to employment, there should be no direct HIV screening (testing) or indirect screening (assessment of risk behaviors or questions about previous tests).

One of the reasons most often given for individuals hesitating to undergo voluntary HIV antibody testing is the fear that they will not be able to control the extent to which third parties will be given access to the information. Indeed, the *Privacy Act* itself sets out some 13 circumstances in which government departments may disclose personal information to third parties without consent. In recognition of the particularly sensitive nature of AIDS information, *AIDS and the Privacy Act* recommends that a tightly controlled process be followed before any such disclosures are made.

Most important, the decision of whether to disclose to third parties without consent should be made only by the head of the government institution. The decision should be based on a consideration of:

1. why disclosure is necessary,
2. the potential adverse consequences of the disclosure on the individual(s) to whom it relates,
3. the likelihood that the requestor 'can and will maintain the confidentiality of the information, and
4. the likelihood that the requestor will use it only for the purpose for which it was originally sought.

The onus should always be on the requestor to justify the need to release the information without the consent of the individual(s) to whom it relates.

These recommendations attempt to reflect an appropriate compromise between privacy concerns and the legitimate needs of some government institutions. Changes in the understanding of AIDS, its transmission, in public attitudes may compel re-examination of the recommendations as, of course, would a vaccine or cure. In the words of the report:

"To hope for an early cure or an effective vaccine is a natural human response to this terrible disease. But hoping does not diminish society's responsibilities today. The principles set forth here in responding to the privacy issues in handling the personal information of those affected by HIV infection and AIDS may not give much long term comfort. But at least they make society's response more humane. For the moment, perhaps, that is the best we can do."

The Dawn of the Biotechnological Age

By-and-large, the government collects information about individuals in traditional ways, such as by surveys, forms, letters or direct observation. But even these old-fashioned methods can be abused, resulting in unacceptable invasions of privacy. More ominously, however, intrusive collection techniques are gaining currency.

Such methods (some newer than others) permit information about individuals to be drawn directly from their biochemistry: i.e., the breathalyzer and polygraph. Urine tests, blood tests and genetic mapping are also becoming fashionable as means of finding out a person's hidden (perhaps even from himself or herself) secrets.

While these information collection techniques are best known in the law enforcement environment, they are achieving increasing popularity for screening purposes outside of the criminal justice sphere. Would you be a loyal and trustworthy employee? Would you engage in behaviour likely to put others at risk? Have you broken the rules governing an activity in which you want to engage? Do you have a genetic predisposition to certain diseases or personality styles? Governments and private sector employers are being tempted to seek access to biochemistry to provide answers to these questions.

The Department of National Defence, for example, tests the blood of its employees wishing to attend U.S. defence courses to determine if they are HIV free. The Canadian Security Intelligence Service gives prospective employees a polygraph test to determine whether they are loyal and trustworthy. Transport Canada is considering whether transportation workers should have their urine tested for the presence of illegal drugs.

Sports Canada is urging that the urine of funded athletes be tested for the presence of banned (not necessarily illegal) drugs which could enhance performance and undermine fair sporting competition. The RCMP is using genetic material for identification and a national "genetic fingerprint" inventory will be developed similar to that which now exists for fingerprints. Moreover, research is underway into techniques which would enable detailed physical and behavioural profiles to be developed on individuals based on a DNA test.

One commentator has argued that we are moving from the information age into the biotechnological age. In that transition are privacy dangers the likes of which we have not seen in our history.

If privacy is to have any meaning in the 90s and beyond, great care must be taken to ensure that effective limits are placed on new, more intrusive means of information collection. Yet as we end the 80s there are indicators that the policy-makers may not be so inclined.

Some officials testifying at the Dubin Inquiry strongly advocated mandatory, random and unannounced urine testing of federally-funded athletes. While a strong case can be made for such testing, it is troubling that a government policy, even in a well-defined area and with tacit consent of the athletes, appears to ignore a concept which is fundamental to individual privacy — the presumption of innocence. The need to prevent intrusions into private lives, unless there is a specific and reasonable suspicion of wrongdoing, has been clearly articulated by the Supreme Court as part of Canada's Charter of Rights and Freedoms. It has only been compromised in rare instances to protect life — instances such as random, roadside alcohol tests.

Yet, in the case of athletes, the country's offended national pride seems to be widely accepted as sufficient reason to ignore a fundamental principle of freedom. If we can justify the intrusions necessary to test athletes, and perhaps Mr. Justice Dubin will conclude that we can, will it not become easier for employers to justify intrusions into the bodies of their employees or potential employees? Canada's inquiry into drug use by athletes may have an impact on our philosophy of individual privacy which will not end in the sports arena or at the locker room door.

The principle reason why these annual reports have expressed concern about computer matching — the comparison of unrelated data bases to compile profiles of certain individuals — is because it represents search and seizure of records without reasonable cause. For the same reason, the Privacy Commissioner will continue to monitor developments in biotechnological screening programs in an effort to protect the privacy of innocent individuals.

Computer Security

"...security is concerned with protecting the computer from people; privacy with protecting people from computer"

(Robert P. Bigelow)
Computer Law and Security Report,
March/April 1989

Would it were as simple! In highly automated office environments, good computer security is essential to protecting people from other people — perhaps the ultimate goal of privacy advocates.

A totally secure computer system would appear to be an unattainable ideal in the current decentralized data processing world. Computer security professionals now talk of "trusted" rather than "secure" computer systems. (It's a telling social comment that the term "trust" now implies a measure of distrust!)

We are now in the young adulthood of the age of management information systems (MIS). Since the mid-70s the ability of the computer to perform multi-processing, to manipulate massive files, to pass information over great distances in seconds and to allow many users to share the information resource has proven an integral part of the administration of government.

It is no longer uncommon to enter a government office and find multi-purpose workstations connected to a mainframe computer system or to a network of computers wherein the data and, in some cases, the logic programs are purposefully or unwittingly shared.

Over the past year the Office of the Privacy Commissioner delved into the labyrinth of computer security — a confusing world of specialized terminology and technology. Internal threats to computer systems come in strange forms: salamis, trap doors, logic bombs, Trojan Horses, and worms. External threats are equally exotic: viruses, spoofing, scanning, switcheroo, network weaving and pass through.

And those who seek to counter these threats also "colour" the issue; in the U.S. the Department of Defence security standards are published in the "Orange Book" and explained in the "Yellow Book". The security of networking systems are dealt with in the "Raspberry Book" — and so it goes.

The security challenges which the MIS environment poses are enormous and the Office of the Privacy Commissioner is in its infancy in developing the expertise to pinpoint problems and offer responsible, workable solutions. In the coming year, special emphasis will be placed on the security of EDP systems during our regular privacy audits of government institutions.

Special tribute should be paid to the work of the System Security Centre of the Communications Security Establishment. The Centre was established in August of 1988 to augment the computer security expertise of the RCMP and DND and to provide new capabilities for the evaluation of computer and network security products for the Government of Canada. Part of the impetus driving Canada to develop its own trusted computer security evaluation criteria was the *Privacy Act*. There was a recognition that, although the protection of national security information poses the most difficult technical problems, the most widespread problem was the need to protect the privacy of personal information held by government.

The Privacy Commissioner welcomes this initiative and looks forward to a continuing exchange of information and ideas with the Systems Security Centre.

CSIS Files

Another collection of highly-sensitive personal information continued to be a matter of concern over the past year — the intelligence files inherited by the Canadian Security Intelligence Service (CSIS) from the former Security Service of the RCMP. Much of the information contained in these files does not, at least in the view of the Security Intelligence Review Committee, meet the tests for collection under the *CSIS Act* now that the definition of “threats to the security of Canada” has been more precisely drawn.

Thus, CSIS finds itself in the awkward position of being the custodian of information about individuals which it would not be entitled to collect under the terms of its present mandate.

The solution seems simple — dispose of the old files!

In fact, CSIS has set up a unit to review the files, extract what is of continuing legitimate significance to CSIS and dispose of the rest. But, the process is laboriously slow; — some of these files have been “sequestered”, others have become subject to special rules governing internal access to and use of the files. Consultations are in progress between CSIS and the National Archives to determine what information should be archived and under what conditions.

Yet, the shredders do get used! Since the lifting of the file destruction moratorium imposed in 1985 (after concerns were expressed by the Deschênes Commission on war criminals), some 120,000 security service files have been disposed of. This includes 67,000 which had previously been scheduled for destruction by the RCMP, and 53,000 reviewed prior to disposal by CSIS. It is comforting that the review has resulted in CSIS keeping fewer than 100 files. There remain, however, many thousands of files whose appointment with the shredder is years away.

These old RCMP files create a further complication for CSIS. As authorized under the *Privacy Act*, CSIS will neither confirm nor deny the existence of information which is of continuing intelligence value. Such information is contained in bank SIS/P-PU-010. Neither will it confirm nor deny the fact that no information exists when a *Privacy Act* request is made to that bank. Both the Privacy Commissioner and the Federal Court of Canada have accepted that the so-called “mosaic effect” requires CSIS to take this approach.

However, CSIS will confirm the existence of certain personal information which was gathered by the former RCMP Security Service. Dated, less sensitive information of this type is maintained in bank SIS/P-PU-015. Its existence will be confirmed and the information will be released to a requestor subject to any of the specific exemptions which are set out in the *Privacy Act*. It has not proved possible to reach agreement with CSIS on a set of guidelines which would define what constitutes “less sensitive” information, this despite a genuinely good faith effort on the part of CSIS to respond to the concerns raised by the Privacy Commissioner in his last annual report.

As requests are received, CSIS decides where to allocate (bank 010 or 015) the former RCMP Security Service intelligence information. This appears to be the only practical approach until all records are disposed of which do not meet the CSIS Act's collection requirements.

The Privacy Commissioner is pleased to report that CSIS plans to accelerate its review and disposal of files. In the next two years it intends to review for disposal twice as many as during the past five years. The Privacy Commissioner applauds the initiative but considers the process should be independently monitored to ensure that all information which does not meet the "strictly necessary" requirement of section 12 of the CSIS Act, is actually disposed of and not merely recycled into other formats.

The Inspector General (under sections 30 and 31 of the CSIS Act), the Security Intelligence Review Committee (under section 40 of the CSIS Act) and the Privacy Commissioner (under section 37 of the Privacy Act) all appear to have the power and mandate to provide such independent inspection.

The Privacy Commissioner will, in the coming months, consult with the relevant parties to determine how this file disposal monitoring can be carried out without unnecessary duplication of effort.

What's with the Cheque?

Mailing lists are a private sector privacy issue which everyone understands. But few in the private or public sector have mailing lists as up-to-date and complete as the federal government.

Consider just three.

- the government's own employees (including the armed forces and the RCMP) 350,000;
- family allowance/old age pension/Canada Pension Plan recipients' list, (approximately 5.5 million names and addresses);
- and the income tax list (about 17 million).

These three lists would be a veritable gold mine for direct mailing. Some brazen requests for them have already been made.

Item: A publishing house asked Health and Welfare for the list of all Canada Pension Plan recipients and applicants. The reason? To send an advertising brochure offering legal services to anyone with a pension problem.

The federal government is prohibited from selling (or giving away) its mailing lists. But what about the government's own use of its lists. Government departments and agencies have recognized government cheque envelopes as a cost-efficient method of communicating with their clients. The cost of enclosures with regular government mailings pales beneath that of an advertising campaign and targets more successfully. It would even be an excellent way of advertising the blessings of the *Privacy Act!* ("Do you know your privacy rights?")

Family allowances and pension recipients are accustomed to finding information notices with their monthly cheques. Privacy violations or not?

No violation providing the information relates directly to the mandate of the department on whose behalf the cheque is issued. Thus, Health and Welfare Canada can appropriately inform pensioners of changes in benefits or remind parents to keep their children's inoculations up-to-date.

But there is potential for abuse. To its credit, this has not escaped the attention of the Treasury Board. As a result, the board now requires departments to obtain its permission to enclose material with a regular government mailing. The record is generally good. However, in spite of the closer monitoring, some five of the 50 mailings last year were unrelated to the original purpose of the mailing list.

Examples: Information on the Canada-U.S. Free Trade Agreement was offered in one enclosure which was sent to all nine million recipients of Family allowance, Old Age Security and Canada Pension Plan. Pension and salary cheques to past and present public servants were accompanied by appeals to purchase Canada Savings Bonds and to contribute to United Way campaigns.

Clearly, there are conflicting goods here. The government's own communication policy sensibly obliges departments and agencies to tell the public about their activities. Canada Savings Bonds are essential to the government's financing and individuals wanting to buy undoubtedly value knowing about the bonds and the procedures for automatic deductions. As well, the United Way depends heavily upon public servant's contributions, which are greatly facilitated by payroll deductions.

Yet, the principle in the *Privacy Act* is clear. Information collected for one purpose cannot be used for another purpose.

There will be some difficult applications of the law, some hard judgment calls. The Privacy Commissioner seeks not to be the Grinch who stole the Christmases which United Way agencies provide. But the Privacy Commissioner very much wants to stop government mailings being used for distributing political statements. Government junk mail is still junk mail.

What accompanies a government cheque bears some close watching.

Consultations are underway with Treasury Board to set guidelines to ensure government mass mailings conform with the *Privacy Act*.

Complaints Directorate

This year's startling 20 per cent increase in new complaints (1,050 compared to 691 in 1987/88) is difficult to explain. It may simply reflect a return to the pattern of a 10 per cent annual increase evident since the program began, making last year's drop an aberration for which this year's case-load compensated with a vengeance. This can be said: there is no reason to attribute the increase to growing resistance to either the letter or spirit of the *Privacy Act*.

The return to the larger numbers was accompanied by more complaints about the length of time departments took to respond to requests. This is disappointing. The Commissioner had hoped that the delay problem would resolve itself as departments gained experience. In fact, the office investigated 414 delay complaints, 243 of which were against the Correctional Service of Canada (CSC) — the result of a marked increase in applications.

Despite the substantial rise in new complaints, the Commissioner and his staff whittled away the 296 cases carried over from last year. Only four of these now remain.

Overall, investigators completed 1,028 cases during the year, an increase of 56 per cent over the preceding year. The directorate continues to reduce the time required to complete an investigation. The new performance standard for an investigation is three months (on average), with no complaints outstanding for longer than six months. At the end of the reporting year, 94 per cent of the complaints were less than six months old.

The acceleration can be partially explained by the addition of three staff positions to the directorate, given in anticipation of Crown corporations being made subject to the *Privacy Act*. By the end of the year these corporations were still not covered so the additional investigators allowed the office to keep pace with the large increase in complaints. With the directorate now fully staffed, the office is confident of continuing to meet the new performance standard — at least until the Crown corporations come on stream.

Statistics — “a rose by any other name”

The terminology in this report describing the disposition of complaints is a little different from previous years. The change makes consistent the terminology used by the departments in reporting their statistics to the Treasury Board and that of the Privacy Commissioner's office. Discussions with the board and all other parties resulted in the following:

Not well-founded
(formerly “dismissed”)

Well-founded, resolved (formerly “justified”). This means that negotiations led to what the Commissioner considered a reasonable resolution of the problem. It does not always mean that the complainant was completely satisfied.

Well-founded. This signifies that there was some breach of the *Privacy Act* which was not resolved, either because material could not be found, had already been destroyed, or time limits had been exceeded. This term is also used when access has been denied and the Commissioner has threatened to take court action in order to have the information released.

Abandoned. This indicates that the complainant has withdrawn the complaint (often because the problem has been solved before the investigation begins), or has not responded to follow-up calls or letters.

Origin of Completed Complaints by Province and Territory	
Newfoundland	3
Prince Edward Island	35
Nova Scotia	17
New Brunswick	165
Quebec	240
National Capital Region Quebec	4
National Capital Region Ontario	53
Ontario	200
Manitoba	21
Saskatchewan	96
Alberta	57
British Columbia	134
Northwest Territories	1
Yukon	0
Outside Canada	2
TOTAL	1028

Cases

CEIC can seek UI medical claim details

An Ontario man objected to the amount of medical information the Canada Employment and Immigration Commission (CEIC) collected when he claimed unemployment insurance medical benefits.

The man was on modified duties at the time of his layoff because of an injury. He gave CEIC information from his doctor that stated the recuperation period and his claim was accepted. A week later, a specialist extended the recuperation period because the injury was not healing well. Later, the period was extended again. Each time he informed CEIC.

Following the second extension, CEIC asked for and received a completed form from the doctor. However, the commission found the information to be insufficient and asked for more detail. The doctor completed the form reluctantly because he considered the details privileged information.

During investigation it became apparent that the two doctors had supplied conflicting information. When this happens, CEIC requires, and is authorized to get, a diagnosis to settle the claim. The Commissioner concluded that CEIC officials were exercising prudent judgment as set out by the Unemployment Insurance regulations, by corroborating the information. He considered the complaint not well-founded.

Marriage data needed for passport

An Ottawa man complained that he had had to reveal his past and current marital status to the individual who guaranteed his passport application. He also worried that External Affairs collected too much information in his application.

Passport applications ask "if you are or have been married". The form explains that the details are needed for "identity, citizenship and/or custody of children." However, investigation revealed that the information is required in only three instances when:

- *the surname on the passport was assumed after marriage (either the spouse's surname or a combination of birth surname and spouse's surname);

- *when children are to be included on the passport (the details help determine legal custody);

- *a female applicant was married to a non-British subject prior to January 1, 1947. She may have ceased to be a British subject because of the marriage and, according to the laws at that time, not a Canadian citizen.

In all other cases, passport examiners may waive the marriage data requirement.

The Commissioner agreed that External Affairs needed the information but questioned whether the application form made it clear that it was limited to the three circumstances. External Affairs agreed to explain this on a new form.

The Commissioner rejected the position that requiring the guarantor to know marriage details was an invasion of privacy. A guarantor is not simply a witness to the applicant's signature, but attests, to the best of his or her knowledge, that the information is correct.

"Since a Canadian passport allows the bearer to enter Canada ... as a matter of right, I believe that disclosure of the information to the person attesting... cannot be viewed as an unreasonable requirement", the Commissioner said.

He considered the complaint not well-founded.

RCMP may release subpoenaed information

A lawyer involved in a lawsuit with an insurance company complained that the RCMP had, without consent, given the company's lawyer a copy of his client's statement to police.

The RCMP explained that it had discussed that portion of the file with the company's lawyer but had neither provided a copy nor allowed her to see one. However, all the information had been subpoenaed at an earlier criminal trial of another man. The RCMP produced the information in response to the subpoena and it was now part of court records. Thus, the RCMP discussed nothing which had not already been disclosed at the trial.

The complaint was dismissed because the *Privacy Act* allows government institutions to release personal information in response to a subpoena.

No charge to use *Privacy Act*

A senior citizen complained when charged \$25 to use the *Privacy Act*. He had seen information about using the Act in the *Seniors Guide to Federal Programs and Services*, a Health and Welfare Canada publication. He applied to National Archives for his employment file and to Canada Employment and Immigration Commission (CEIC) for his immigration file.

National Archives redirected his application to his former employer and shortly thereafter he received the information. However, CEIC charged him \$25 for his immigration documents. Because the guide had not mentioned a charge, he wrote to Health and Welfare suggesting it include such information.

An investigator found that CEIC staff had misunderstood the man's request. Seniors often need certified copies of landing documents to support pension applications, a service for which CEIC charges. Once CEIC realized the request was not for certified copies but simply to see the file under the *Privacy Act*, it refunded the \$25.

The complaint was well-founded/resolved.

Keep performance appraisals five years

A complaint that a department was keeping employees' performance appraisals too long ended up involving Revenue Canada/Customs and Excise, National Archives, the Treasury Board and the *Privacy Commissioner*.

The complainant told the Commissioner that Customs and Excise was retaining annual appraisals longer than the three years described in the *Personal Information Index*. The length of time that appraisals are held (the retention schedule) is established by National Archives in consultation with the Treasury Board. Customs and Excise considered the schedules as policy, not law, and not subject to complaint. Treasury Board, however, considers the schedules to be the law.

The Commissioner agreed to study the matter. The investigator confirmed that Customs and Excise was keeping the man's appraisal (and all appraisals) beyond three years. Through consultations involving the department, Treasury Board and National Archives, he discovered that Treasury Board had changed the retention period to five years but the department had not been made aware.

After discussion, Customs and Excise concluded that the intent of Treasury Board's policy was clear and agreed to comply with the five year period.

Test scores need expert interpretation

A lawyer preparing an appeal sought information about her client from two Correctional Service of Canada (CSC) banks. She complained when CSC withheld information.

Investigation revealed that much material in the Offender Health Care Record bank was supplied in confidence by a province, and thus CSC was obligated not to release it under the *Privacy Act*. The investigator suggested that the lawyer apply using the provincial privacy legislation.

CSC had also exempted raw psychological test data from a Psychology bank, maintaining that releasing medical information would not be in the inmate's best interests. CSC argued that releasing test results in raw form would make it subject to misinterpretation by laymen.

According to a CSC psychologist, the test is copyright and psychologists are not free to provide copies. He also argued that revealing test questions, individual responses and scores would render the test invalid — particularly in a closed population like a prison. Further, test results can vary daily according to the subject's health or mood. Again, a layman might misinterpret such variations and one-time scores.

The doctor suggested that the lawyer hire a registered psychologist as an expert witness to whom the doctor could release the documents.

The Commissioner found compelling the doctor's arguments against releasing this type of information in a prison environment and considered the complaint not well-founded.

Applicant gets reference comments only

Several potential and former RCMP members applied for information from their security clearance records and complained when the Force withheld the names of persons interviewed during the security clearance process and their comments.

The RCMP argued that it must take extraordinary care in screening police officers. For example, police officers have the power to arrest and carry firearms. Temperament and moral character are therefore of special importance. The RCMP argued that it must protect its sources to ensure candor.

After discussing the complaints with the investigator, the RCMP staff agreed to review the material. It concluded that the sources' comments could be released, but it withheld their names (or other identifying details) to protect the integrity of the inquiry.

The Commissioner agreed with the resolution and considered the complaints well-founded but resolved.

World War II hospital records gone

Despite a thorough effort by National Archives, a British Columbia man did not receive all the information he wanted from the Archives' Medical Records World War II bank.

He told the Commissioner that the material Archives sent excluded documents from his stay in a particular hospital in the 1940s. This included a form he had been required to sign stating that he would not apply for a military pension.

At the request of an investigator, Archives searched other banks but with no success. Archives found the records of the hospital (which no longer exists), but lacked those of the period covering the complainant's treatment.

The investigators then asked the Department of Veterans Affairs who also searched, without success, for the missing files.

The Commissioner concluded that the files cannot be found and that Archives had responded to the best of its ability. The complaint was not well-founded.

Informant's name withheld in tax case

A woman complained to the Manitoba Institute of Chartered Accountants that her former chartered accountant had acted unprofessionally. The institute began an investigation and applied to Revenue Canada, Taxation on the woman's behalf for her individual income tax return file.

Revenue Canada withheld some information because it either concerned another person or its release could "be injurious to the enforcement of the *Income Tax Act*".

The lawyer complained to the Commissioner.

The investigation confirmed that some of the information was about someone else and was thus properly exempt. The rest concerned a confidential source. The Commissioner agreed that release of the material could threaten enforcement of the *Income Tax Act*. However, he added that a strong argument could be made that the public good would be best served by releasing the information. Nevertheless, the *Privacy Act* gives the department discretion to decide and he did not believe that Revenue Canada had exercised the discretion improperly.

The complaint was not well-founded.

Grounds of Complaints and Investigation Results

Grounds	Aband.	Well-founded	Well-founded. Res.	Not Well-founded	Total
Access	16	8	69	410	503
Use & Disclosure	6	8	7	29	50
Correction/Notation	0	1	6	10	17
Time Limits	4	317	14	79	414
Language	0	1	0	23	24
Index	0	0	0	0	0
Collection	2	1	2	12	17
Retention/Disposal	0	0	0	3	3
TOTAL	28	336	98	566	1028

Employer compares sick leave records

A woman asked the Commissioner's Office whether Canada Post, which employed both her and her husband, could use her attendance records to investigate her husband's attendance problems. Her file had been given to a supervisor to whom she does not report and her husband found one of her attendance cards in his own file.

The investigation had to determine whether it was proper to match the couple's attendance records to verify her husband's attendance.

Canada Post considered the use consistent with the purpose for its collection—to ensure that employees respect their leave entitlements in the collective agreement. Canada Post held that when management suspects abuse, it was "natural" to review attendance records "including those of two or more individuals where warranted".

The Commissioner advised Canada Post that, while he understood the motivation, the practice appeared to contravene the *Privacy Act*. He invited Canada Post to respond before he made a final decision:

Canada Post replied that matching "supported the attendance and leave function" when management suspects employees are colluding to abuse leave. Canada Post maintained that the only option to matching records to confirm fraudulent leave claims would be an even more intrusive investigation.

The Commissioner was unconvinced. He had difficulty accepting that unregulated comparisons between the attendance records of spouses, other family members and golfing buddies were integral to attendance management. He concluded that accepting the position was tantamount to discrimination against employees whose relatives or friends also worked for the post office. He recommended that Canada Post stop the comparisons.

Canada Post did not agree but was prepared to discuss a resolution. After further negotiations, Canada Post adopted guidelines to control the practice. Under the new guidelines, individuals' attendance records will continue to be reviewed but will only be matched with those of others to generate depersonalized information or, if necessary, to confirm or disprove a pattern of common absenteeism already observed among employees.

The guidelines also restrict who may see and compare the information and to whom it may be disclosed.

Can't use tax files for discipline

A tax auditor, fired for falsifying her income tax returns, complained to the Privacy Commissioner that Revenue Canada, Taxation had breached both the *Income Tax Act* and the *Privacy Act* when it used her tax returns for disciplinary purposes.

A week prior to filing the complaint, the woman had asked the Federal Court to declare that Revenue Canada could not use the tax return information, except as allowed by the *Income Tax Act*. In particular, she argued that her tax returns should not be used as evidence in a hearing about her discharge.

The Commissioner postponed his finding until the court ruled. The judge agreed that when Revenue Canada is acting as an employer, it is not entitled to use individual tax returns for personnel purposes.

The *Privacy Act* allows the department to use personal information only for the purpose for which it was collected, "subject to any other act of Parliament". Since the use was not one for which it was gathered, nor was it a correct use under the *Income Tax Act* according to the court, the Commissioner concluded that the complaint was well-founded.

This does not mean that Revenue Canada may not discipline employees who evade taxes. It does mean that the department should treat the employee as it would anyone else it suspects of tax evasion, then take appropriate disciplinary action if he or she is found guilty.

Ham radio operators' data released

An amateur radio operator complained because the Department of Communications (DOC) releases amateur broadcasters personal information to amateur radio societies and publishers to print directories (call books) of licensed operators. DOC maintains a database of the licensees which includes names and addresses.

The operator opposed release of his personal data because he did not want to become the target for "junk" mail or thieves seeking expensive radio equipment.

The complaint influenced DOC to put on hold release of the information pending the Privacy Commissioner's decision. This prompted a barrage of calls and letters from operators to both DOC and the Commissioner's office.

The investigation found that DOC release of the information is a complicated issue. DOC officials told the Commissioner why the department considers the release “consistent with” the purpose for its collection.

DOC explained that it is responsible for managing the radio spectrum, a limited public resource. Individuals who pass the examinations are assigned a call signal and are licensed to use a portion of the public air waves. Publicly identifying these operators allows them to police themselves since misuse by amateurs can interfere with other radio transmission. As radio saturation and electro-magnetic interference grows, DOC considers this policing an important part of spectrum management. DOC also argued that it was not sound public policy to allow individuals to enjoy a shared resource with anonymity.

As a member of the International Telecommunication Union, DOC is obligated to provide public access to names, addresses and call signs under two articles of international regulations which deal with investigating interference, communication amongst operators and their self-training.

As well, DOC discloses licensing information to permit communication amongst amateurs, including verifying signals and technical details. This helps operators who are required by the radio regulations to confirm that a contact is a licensed amateur. DOC is also required to release the names and licence status of amateurs using shared systems (such as satellites) which are funded and maintained by the amateur community.

DOC agreed that not all operators want to join clubs, volunteer for emergency communications services or be listed in call books. However, it considered that amateurs may not opt out of their responsibility to make public their use of the airwaves.

The Commissioner accepted DOC’s strong case for disclosure and noted that operators may ask private call book publishers not to list their information. He considered the complaint not well-founded.

Solicitor-client privilege widely drawn

A woman involved in a wrongful dismissal suit against Transport Canada applied for her information in its 20 standard employee banks. Her complaint alleged slow response and the withholding of material.

The investigation found that there was no information about the woman in 14 of the banks. It was also evident that information had been withheld from the grievance file, some because it concerned another person and some because the department considered that it was protected by solicitor-client privilege.

The investigator found that Transport Canada had exempted the request for its lawyer’s opinion, the opinion itself, and all the background material. This material — part of the regular grievance file — was withheld in order to seek a legal opinion. The department held that once this information was attached to the request for legal advice, it became privileged.

However, legal precedents are clear that solicitor-client privilege covers communications between the parties and materials created or obtained specifically for litigation. All documents given by a client to a legal adviser are not privileged. For example, when facts are obtained from other sources, not for or by legal counsel, they are not privileged.

The Commissioner advised Transport Canada that he considered its view "extends unacceptably the concept of privilege". His recommendation to release the grievance file material prompted the department into partial release of the information. The Commissioner proposed to the complainant that she take her case to the Federal Court. She agreed and the Commissioner notified the department. In the meantime, Transport Canada had received advice from the Department of Justice and decided to release the material. The Commissioner considers the complaint well-founded.

Completed Complaints by Department, Type and Result

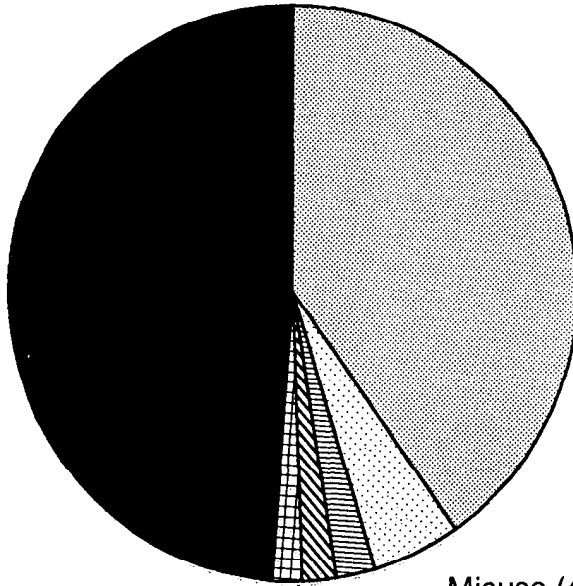
Department	Total	Well- founded	Well- founded - Resolved	Not Well- founded	Dis- continued
Agriculture Canada	5	0	2	3	0
Canada Labour Relations Board	1	0	0	1	0
Canada Mortgage and Housing Corporation	1	0	1	0	0
Canada Ports Corporation	4	0	4	0	0
Canada Post Corporation	12	2	2	7	1
Canadian Human Rights Commission	11	0	2	9	0
Canadian Security Intelligence Service	49	3	6	40	0
Communications, Department of	2	1	1	0	0
Consumer and Corporate Affairs Canada	1	0	0	1	0
Correctional Service Canada	404	203	29	168	4
Employment and Immigration Canada	68	24	13	28	3
Energy, Mines and Resources Canada	2	1	1	0	0
Environment Canada	3	0	0	0	3
External Affairs Canada	14	3	1	10	0
Health and Welfare Canada	18	3	5	8	2
Indian and Northern Affairs Canada	1	0	1	0	0
Justice Canada	5	0	0	5	0
Labour Canada	5	0	0	5	0

Department	Total	Well-founded	Well-founded - Resolved	Not Well-founded	Dis-continued
National Archives of Canada	15	1	0	14	0
National Defence	85	32	4	46	3
National Parole Board	30	3	11	15	1
Office of the Chief Electoral Officer	1	0	0	1	0
Office of the Commissioner of Official Languages	3	0	0	3	0
Office of the Correctional Investigator	1	0	1	0	0
Office of the Inspector General of the Canadian Security Intelligence Service	4	0	0	4	0
Privy Council Office	6	0	1	5	0
Public Service Commission	8	0	4	3	1
Public Works Canada	2	0	0	2	0
Revenue Canada - Customs and Excise	15	5	1	9	0
Revenue Canada - Taxation	37	11	0	21	5
Royal Canadian Mounted Police	109	13	6	86	4
Security Intelligence Review Committee	4	0	0	4	0
Solicitor General Canada	22	0	0	22	0
Transport Canada	77	31	2	43	1
Veterans' Affairs Canada	3	0	0	3	0
TOTAL	1028	336	98	566	28

Caseload by grounds 1988-89

Access (48.93%)

Delay (40.27%)



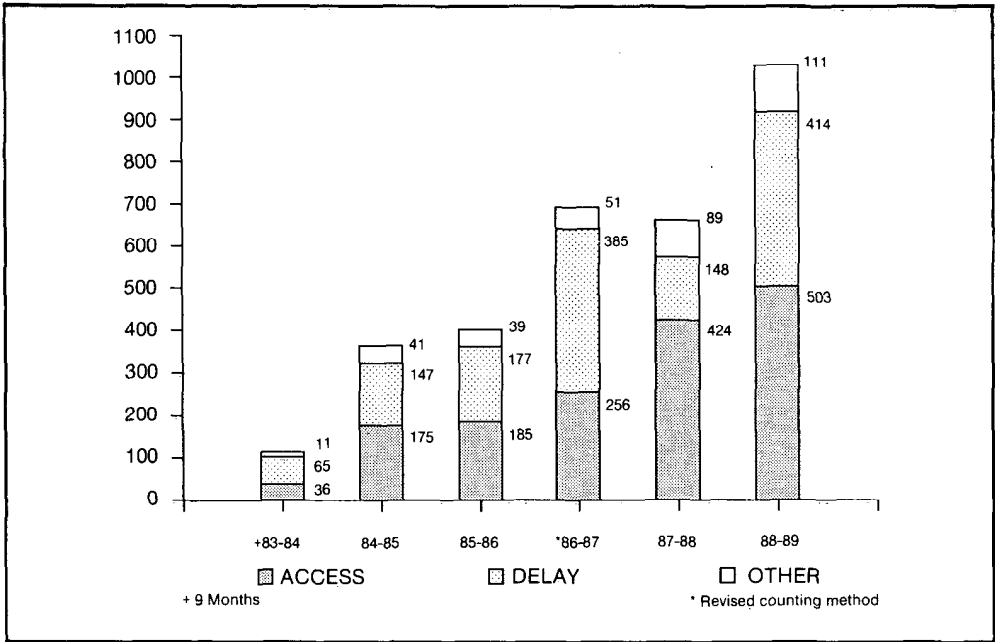
Misuse (4.86%)

Language (2.33%)

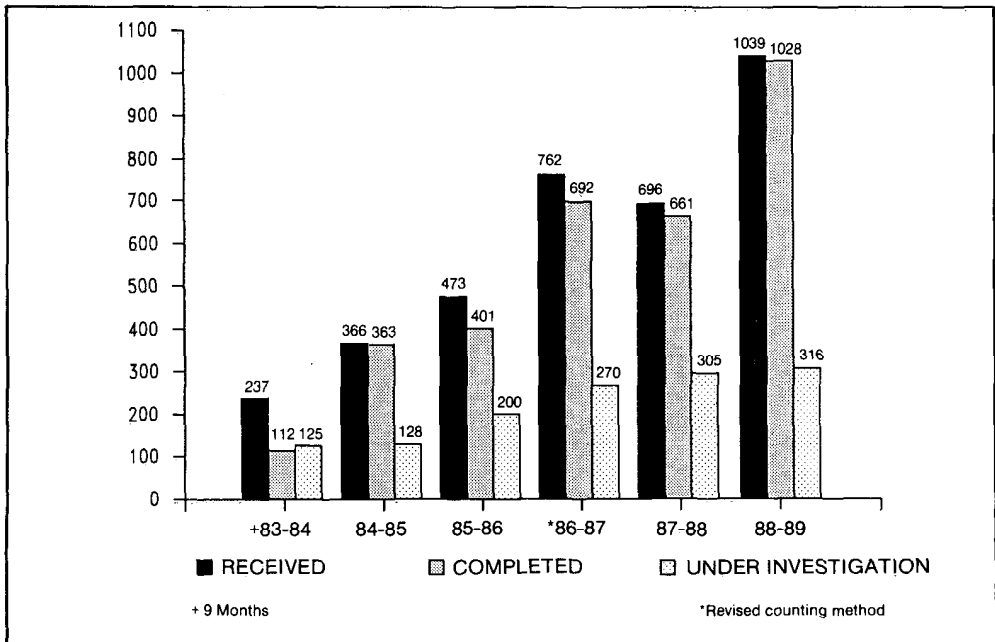
Collection etc. (1.95%)

Correction (1.65%)

Completed complaints and grounds 1983-89



Completed complaints 1983-89



Inquiries

Inquiries to the Privacy Commissioner's office almost doubled in this fiscal year as the staff dealt with 2,041 compared to 1,248 in the previous year. The office now has a full-time inquiries officer who handles the majority of the calls. Her improved system of logging all inquiries makes the increase appear greater than it actually is. Before this, many calls were simply not included as staff members fielded them but lacked the time to officially record them.

Queries cover a broad range. They can be as simple as forwarding an application to see personal information to the proper department (approximately eight per cent of inquiries).

They can also be as time-consuming (but ultimately satisfying) as following up an MP's call about a detailed questionnaire which temporary helpers at Canada Post had to complete before they were hired to deliver advertising mail. Canada Post, after discussion with this office, stopped using the questionnaire. Calls about using and interpreting the *Privacy Act* make up 46 per cent of the inquiries.

Questions and complaints about the use of social insurance numbers climbed to 21 per cent of all inquiries during the year, due in large part to an amendment to the *Income Tax Act* which requires everyone to give their SIN to their financial institutions. Some callers were incensed at the apparent contradiction between the government's newly-announced policy on restricting the number and a requirement to put the SIN in the hands of their bank, trust company, credit union, *caisse populaire* and stockbroker. Callers were also being told they had to give it to real estate agents (who were banking deposit cheques) and to insurance agents.

Other callers were disturbed at what they considered the "secrecy" with which the new requirement was introduced. In fact, as noted earlier, the amendments to the *Income Tax Act* went through normal Parliamentary procedures. MPs did not query the new SIN requirements and the media did not report them. Most callers discovered the new law, which imposes a fine for failure to produce the SIN, when they bought the new series of Canada Savings Bonds or went to the bank. They were not amused.

About ten per cent of callers are concerned about federal agencies that are not subject to the *Privacy Act*, often Crown corporations such as Air Canada and Canadian National Railways. Some Crown corporations are expected to be covered by the Act in 1989.

Fifteen per cent of the calls concerned privacy issues in either the provincial or private sector and thus were beyond the authority of this office. For example, an Ontario woman called to determine whether the *Privacy Act* would prevent her municipality from selling its voters list to companies or individuals. The office was unable to investigate since municipalities are not covered by the *Privacy Act* and will not be subject to the Ontario legislation until 1991. (Federal enumeration lists, by comparison, may not be sold.)

Compliance Directorate

Who Was Audited

The Commissioner's office again selected audit candidates nominating targets according to overall level of risk measured as objectively as possible.

Selected were Canada Post Corporation, the Secretariat of the Ministry of the Solicitor General and Employment and Immigration Canada. In addition to these major institutions, audits were done on several smaller institutions: the Department of Finance, the Pension Appeals Board, and the Science Council of Canada.

Small agency audits are being concluded in the Law Reform Commission, International Development Research Centre, the Canadian Cultural Property Export Review Board, Export Development Corporation and Canadian Patents and Development Limited.

How and What was Audited

Audits are conducted by teams of two to four investigators who visit selected headquarters units and a number of regional offices. Investigators review a random sample of files from selected information banks and interview managers and staff who use and control the files.

The auditors examine:

- * the institution's collection, use, disclosure, retention, disposal and security of personal information;
- * the adequacy of internal policies and compliance with central agency policy and guidelines on personal information;

- * the accuracy and completeness of listings in the Personal Information Index;

- * staff awareness of the *Privacy Act* and its implications for handling personal information;

- * individuals' access to their personal information;

- * delegation of powers by the department head.

Once the audit is completed, the auditors discuss it with the managers, focussing on any areas of non-compliance. The department first receives summaries of findings, then an audit report. In line with accepted audit practice, the reports address only those areas requiring correction.

Auditing the Auditors

Six auditors cannot in a short time cover all government agencies under the *Privacy Act's* authority. Thus, the Privacy Commissioner has always urged departments' internal auditors to audit for privacy. The year provided encouraging evidence of this happening.

The Canada Employment and Immigration Commission responded. After consulting the Commissioner's office, its internal audit bureau began a review of CEIC's personal information handling. Privacy staff then examined the auditors' working papers to determine the level of reliance they could place on the audit. That review disclosed a thoroughly professional audit which the Privacy Commissioner could accept with as much confidence as if it had been done by his own auditors. (The findings are summarized elsewhere in this section.)

What Was Found

Some findings apply to all of the agencies audited. For example, few employees outside of the access to information and privacy units know about their rights under the *Privacy Act* or understand their responsibilities for the proper collection, retention, use, disclosure and disposal of personal information.

Inadequate protection of personal information is another common finding. Operational (and even some security) staff do not yet fully understand the new government security policy, particularly those sections which deal with the protection of personal information. Nevertheless, auditors found no indications that personal information had been compromised.

Auditors again found personal information holdings that had not been identified or properly described in the *Personal Information Index*. Similarly, some uses of personal information which the institution considered "consistent" with the purpose for the original collection, were not included in the Index descriptions.

The audits underscored the need for a government-wide policy covering who may see personnel files. Such policy should consider the subtleties of the *Privacy Act* and limit the amount of personnel information managers need for discharging the legitimate demands of their positions. The current organization of most personnel files precludes segregating the information according to the "need to know" principle.

Security and Privacy

Most staff treat information security as the domain of security officers or management information specialists. Both of these groups are trained to think of security in terms of classification in the "national interest", not individual privacy. They are often not prepared to deal with the designation "protected", which now applies to all information which is personal but not in the national interest.

Treasury Board, the Communications Security Establishment, the RCMP and the Privacy Commissioner's staff have taken major steps toward creating staff awareness about the protection of personal information. Until now, this information has often not been considered as security sensitive.

Continuing consultation among these organizations has produced levels of protection that match the sensitivity of the personal information. These levels will be included in the government's security policy statement. The publication and application of this new policy should help departments realize security standards for all designated information.

Incident investigations

The office investigated one lost document incident during the year and maintained a watching brief over another department's investigation of missing records. The investigation concerned the loss of tax microfiche from the Calgary district office of Revenue Canada, Taxation. Revenue Canada told the Privacy Commissioner in October 1988 that it had lost 38 sheets out of a set of microfiche. The sheets identified employers (by code number only) and their employees by surname, initials, social insurance number, earnings, pension, unemployment insurance contributions and other deductions. Each fiche (or sheet) could contain data on more than 8,000 individuals.

The investigation began at the Ottawa Head Office. Investigators followed the procedure for producing and shipping microfiche sets and were convinced that the set would have arrived intact at its destination.

Investigators followed the fiche's trail at the Calgary District Office. Once the fiche had been opened and counted, they were put in a holding tray where they were available during the day to approximately 150 staff. At night they were locked in a cabinet, but the keys were kept in an unlocked desk drawer. The first employee who needed the set in the morning could unlock the cabinet and put the fiche in the tray. It was never determined who put out the set on the day the loss was discovered. The 38 fiche were never recovered.

It became apparent that employees could remove fiche from the set and take them to other parts of the floor without completing a log. Only employees from outside that work area were required to log out fiche.

The investigators considered that Revenue Canada's security was adequate for the production and distribution of the microfiche and that staff are highly security conscious. However, once inside a secure area, employees appeared to overlook the need to protect personal information as evidenced by the cabinet key in an unlocked desk drawer. Employees also knew little or nothing about the *Privacy Act* and the obligations it imposes on employees handling personal information.

Following the incident, the office instituted new strict procedures. The set of fiche and readers are now kept and used in a secure room which is staffed while open. Sheets must be logged as used and the set then returned to a locking cabinet. Stringent controls are now in place for destruction of old fiche.

These new controls make redundant any recommendations to increase security in the Calgary unit. However, the Commissioner recommended that other locations review their storage and microfiche handling to ensure compliance with both the *Privacy Act* and the new government security policy. As well, several recommendations made after the previous microfiche theft (Annual Report 1986-87) from the Toronto office were repeated:

- * employees should be made aware of their obligations to protect personal information under the *Privacy Act*;
- * microfiche should be given even more stringent protection than paper files and
- * staff should have access to microfiche only as they need to know.

In the second incident, Correctional Service Canada lost more than 30 boxes of outdated inmate files which were being shipped to the National Archives Records Centre in British Columbia. After almost two weeks of searching, the trucking company found the boxes in its warehouse. There was no evidence that the boxes had been opened. However, standard security precautions could have prevented the incident.

The Audits

Two of this year's audits revealed a potential glitch which generated discussion between the Commissioner's office and the organizations being audited. Canada Post and the Export Development Corporation (both Crown corporations) are subject to the *Privacy Act* but technically are not bound by the federal government security policy. Both corporations have opted into the national interest provisions of the policy, but objected to the office using it as a standard against which to measure their physical security.

The Commissioner does not believe that Crown corporations should be bound necessarily by the policy but considers the government standards a reasonable measurement against which to assess the corporations' security.

Canada Post

The auditors travelled to Ottawa Head Office and divisional headquarters in Edmonton, London, and Quebec City.

Findings

Staff Awareness: As in most government institutions audited, the staff did not understand their own or others' privacy rights, nor their responsibilities under the *Privacy Act*. Canada Post publishes periodic reminders in its internal bulletins, but most staff could not recall such material. Thus, either the information is not distributed widely enough or it is simply having little impact.

Canada Post plans a communications program to support its corporate policy on the protection of personal information.

Personal Information Index Descriptions:

- 1.) The description of two Human Rights banks (CPC/P-PU-096 and P-PE-809) contained no reference to personal harassment cases found in the files. The bank description will be changed to incorporate a reference to the material.
- 2.) Change of address cards are now described as being a "class" of personal information. However, the *Privacy Act* requires that personal information used for an administrative purpose be included in an information "bank". Since the cards are used to redirect customers' mail (an administrative purpose) Canada Post will create a new bank to contain address change notices. A second bank has been established (CPC/P-PU-120) for requests from other departments to find individuals who owe Crown debts.

Protection of personal information:

Divisional headquarters employees who want to review their personnel files must apply through their supervisors and then examine the files in their presence. This means supervisors have access to all personal information in an employee's file—including such details as medical history, charitable contributions and marriages. This information is unnecessary to supervision. Canada Post will review and correct its access procedures.

Some headquarters personnel files contained limited information on other employees, usually in lists containing names and social insurance numbers. Information about third parties will be removed as the files are drawn and used.

In Edmonton, auditors found waste paper containing personal information being sent for disposal to a private company where it was stored outside and unsecured. Canada Post will ask National Archives to provide secure disposal of sensitive waste wherever possible. Elsewhere it will dispose of its own material.

The auditors also found problems with disposal of other waste materials and control of cabinets or rooms containing personal files. Canada Post is committed to correcting these problems when it implements its new privacy and security policies.

At Ottawa and Edmonton, personal information from the Risk Management Claims bank is shared with private insurance adjusters. However, no formal agreement exists with the company to ensure protection of information according to the *Privacy Act*. Canada Post will obtain insurance adjusters' undertakings to meet both

the spirit and intent of the act. It will also determine whether Canada Post should incorporate privacy and security provisions in contracts with all agents collecting or receiving personal information on its behalf.

Improper use of personal information:

Investigators found a human rights training manual which included actual grievance files, complaints and investigation reports. The documents have now been made anonymous.

Improper disclosure of personal information:

Canada Post shared on one occasion its mailing list of stamp collecting customers with the Royal Canadian Mint "and other reputable mailers". Canada Post considered this a "consistent use" of the information. The Commissioner did not see a reasonable connection between collecting stamps and collecting coins or other items. The exchange has already been stopped.

Retention and Disposal Schedules:

Auditors made several recommendations about storage or disposal of personal records that were being kept either too long, or not long enough (the act requires personal information be kept at least two years). Canada Post will take action on each of the recommendations.

Finally, auditors found fingerprints in personnel files in each division they visited. Apparently Canada Post once took fingerprints routinely from all employees. The Commissioner suggested that prints no longer needed should be returned to the individuals. Those still needed might better be stored in security clearance or reliability check files.

Pension Appeals Board

The Pension Appeals Board hears appeals against decisions of the Canada Pension Plan and the Quebec Pension Plan. All the files are held in Ottawa and all personal information is on paper. There are no EDP files.

Findings

Awareness: Board staff knew little about the *Privacy Act*. Management will provide the necessary training.

Personal Information Index Descriptions: The Index incorrectly says that the *Privacy Act* does not apply to any material the board holds about appeals under the Quebec Pension Plan. All personal information under the board's control is subject to the *Privacy Act* and the board will remove the statement from the listing.

Auditors found that the Employee Records bank (PAB/P-PE-801) is held and controlled by Health and Welfare Canada (HWC), and not the board. The description will be moved to HWC's listing and a statement included under the board's listing directing employees to Health and Welfare. The board also intends to create a bank called "Staff Matters" in which it will hold routine staff material.

Protection of Personal Information: During the audit investigators found keys left in the locks of cabinets containing completed files. The cabinets are in the main office and accessible to cleaning staff during the evening. The Board will ensure that keys are removed. Investigators also recommended new destruction procedures for sensitive waste.

Retention and Disposal: There is no retention and disposal schedule for appeals files, some of which date from 1967. The Board will seek National Archives advice on establishing a proper schedule.

Collection of Personal Information: Investigators found that the board receives all Canada Pension Plan Review Committee decisions and supporting evidence, whether or not an appeal has been filed. When there is no appeal, the board returns the evidence, but retains the decision. The Commissioner considers this to be collection of information outside the mandate of the board. The board will change its process for examining review committee files.

Science Council of Canada

The Science Council of Canada assesses Canada's scientific and technological resources, needs and potential and has a mandate to increase public awareness about science and technology.

All files are kept in the Council's office in Ottawa. No personal information is stored electronically or on microfiche.

Findings

Awareness: Science Council staff were generally aware of privacy principles — a rare finding among government institutions. In fact, the Council has conducted research into privacy-related matters.

Security of Personal Information: Auditors found staff members who handle personal information have not been checked for reliability, as required by the government security policy. The Council undertook to screen all employees who use protected information.

Cleaning staff is allowed into the personnel office unescorted after hours. No one checks to ensure that the door is locked after cleaners leave. The Council will instruct commissioners to make such checks.

Index Bank Descriptions: Two groups of files containing personal information about contract personnel and Council members are not described in the Personal Information Index. The Council will describe these holdings in the next edition of the Index.

Department of Finance

The department implements financial and economic policies and programs. Its offices and some 800 employees are in Ottawa.

Findings

Awareness: Once again, employees interviewed demonstrated little knowledge of the *Privacy Act*, though the department developed procedures on the Act in 1983 and has since provided periodic briefings. Management is developing new procedures and guidelines which will be distributed to the administrative branch and the office of each assistant deputy minister.

Protection of Personal Information: Auditors found that both supervisors and official languages training staff who had no real need to know were

able to review complete personnel files. Moreover, some files contained limited information about other employees. One of the files examined contained a derogatory assessment of another employee.

The department is determining how it could sever sensitive information from these files without hindering supervisors and language staff from discharging their responsibilities.

Keys to cabinets were kept in unlocked drawers in nearby desks and waste personal information was found in regular garbage cans or recyclable-paper bins.

The keys will now be kept personally by the responsible staff member and "burn" bags will be provided for disposal of personal information.

Investigators suggested that the cabinet and room containing records of requests under the *Access to Information Act* and *Privacy Act* be locked when unattended. The department agreed.

Personal Information Index Descriptions: The department maintains records from reliability checks on its employees but does not list the information in the *Personal Information Index*. This effectively prevents employees from asking to see the information since they may not realize it is available.

Treasury Board has amended the description of this bank (one of the standard banks kept by all departments). The department will use Treasury Board's description.

Ministry of the Solicitor General—Secretariat

The Secretariat supports the Solicitor General whose responsibilities include the Royal Canadian Mounted Police, Canadian Security Intelligence Service, Correctional Service of Canada and the National Parole Board. Auditors visited the Secretariat's head office in Ottawa.

Findings

Protection of Personal Information: Auditors found many of the same deficiencies identified in other agencies: detailed personnel files available to supervisors; lists of employees, some with social insurance numbers, in others' personnel files; files in locked cabinets—but keys in nearby unlocked desk drawers; personal information in regular garbage and cabinets left unlocked when offices are not staffed. As well, file covers for records in the Employee Personnel Record bank had neither a security classification nor "Protected" designation.

The Secretariat agreed to examine the problem of limiting access to personnel files. It will also remind staff about their security responsibilities. "Protected" folders are now used for new personnel files (or when requested) though the secretariat does not consider it feasible to convert all existing files.

Personnel files containing sensitive personal information should be marked appropriately because the investigation found that some information had been revealed "outside the organization that created or collected it".

Although the Secretariat has an adequate security procedure, investigators witnessed the offices left open and unstaffed.

Improper Use of Personal Information: A human resources desk manual uses, as examples, copies of actual completed forms and memoranda. The material identifies individuals. Management agreed to remove the identifying information.

Retention and Disposal of Personal Information: Employee personnel records and RCMP personnel and administrative records were retained beyond the approved period. The National Security Records bank (P-PU-026) had no disposal schedule. The Secretariat agreed to review personnel files annually and consult with National Archives and the Canadian Security Intelligence Service on disposal of the other files.

Personal Information Index Descriptions: Records of employee reliability checks are included in the secretariat's Security Clearances bank (P-SE-909) but are not described. Several banks have a National Archives approval number without the listing describing how long information is kept. Reliability checks will be included in the new standard bank created by Treasury Board. This bank, and disposal schedules for other banks, will be described in the next edition of the Index.

An Old Issue: In 1986 the deputy solicitor general agreed to purge personal information from the files in one of the secretariat's banks, Protection of Privacy (P-PU-035). The bank was then to be removed from the Index. During the audit, investigators found that the bank continues to be listed and only 200 of the 600 files have been purged. The Secretariat has assured the Commissioner that the task will be completed by September 1989.

Employment and Immigration Canada (EIC)

The Internal Audit

This audit was divided into two parts. The first was done by EIC's own internal audit bureau and focussed on protection of personal information about EIC clients. The Privacy Commissioner's role was to "audit the auditors". During the next two years the internal audit bureau will examine its personnel information banks and information in EDP files.

The second part, conducted by the Privacy Commissioner's office, was of EIC's Employee Assistance Program (EAP) files.

The internal audit's objective was broader in scope than those done by privacy auditors because EIC assessed the effectiveness of its internal administration and structures in dealing with both the *Privacy Act* and the *Access to Information Act*.

In an internal audit the Commissioner provides overall advice, when needed, and comments or makes recommendations on the department's compliance with the *Privacy Act's* rules concerning collecting, using, maintaining, disclosing and disposing of personal information.

Employment and Immigration, one of the largest federal government departments, provides employment counselling, training and referrals to millions of Canadians, administering the Unemployment Insurance Plan and screening and providing services to immigrants.

"The need for privacy protection is obvious. The whole of EIC, with its 800 offices, is a veritable repository of personal information". EIC runs on personal information", concluded the internal audit report. The Privacy Commissioner couldn't have put it better.

Findings

Staff Awareness: EIC auditors found privacy coordinators knowledgeable about the *Privacy Act* but other staff were not as well informed. As a result, there were inconsistencies in handling informal requests or requests from third parties such as provincial governments or advocacy groups. EIC has given priority to producing operational manuals for staff and will supplement these with training throughout the department.

Collection and Use of Information: The auditors found that a number of forms which collect personal information contain incomplete references to the *Privacy Act*. They suggested improving the privacy notice on the forms by adding descriptions of the data and listing the ways it is used, the bank in which it is kept and the organizations with which it is shared. They also recommended improving the description of the Unemployment Insurance Claim File bank in the Personal Information Index because it may not adequately describe all of the data in the files.

To ensure that its forms comply with the *Privacy Act*, EIC will ask program staff to refer forms which collect personal information to the Public Rights Administration Directorate for advice.

Data Matching: EIC shares (or matches) more information with other agencies than perhaps any other federal department. Matches include comparisons with Revenue Canada, Taxation data to ensure that individuals are reporting earnings and that those collecting unemployment insurance are not also working. The matches are carried out under the *Unemployment Insurance Act* and the *Immigration Act*.

The *Privacy Act* also allows matching by "an agreement or arrangement" between government agencies and with other governments, whether Canadian or international, in order to administer or enforce a law or carry out an investigation.

The internal auditors found that not all matches are governed by written agreements and that a portion of the agreements have been in effect too long to reflect current legislation. Without formal agreements, staff have insufficient guidance on what information can be shared and how it can be used. The auditors recommended providing summaries of agreements to operational staff, completing all pending agreements and then conducting a follow-up audit to ensure that EIC complies with the new Treasury Board data matching policy.

EIC will review all agreements and complete those still being considered. As well, it will report all current data matches to the Privacy Commissioner and ensure that they all are listed in the *Personal Information Index*. (The new Treasury Board matching policy requires all departments to advise the Privacy Commissioner's office 60 days ahead of any new matches.)

Security: EIC auditors found that some service contracts with private companies do not contain privacy or security clauses, meaning that the companies may not always treat personal data in confidence. Auditors cited examples of companies or individuals providing services such as transportation, document shredding, office cleaning (particularly in offices with open shelving), interpretation, transcription, EDP and psychological diagnosis.

Auditors recommended revising regional contracts to include clauses to protect personal information according to the requirements of the *Privacy Act*, the security policy and EIC's own regulations.

Disposal of personal information:

Clearly there was no consistent disposal of waste personal documents among EIC offices. Auditors found that some sorted waste for shredding or regular garbage; others simply put it out with disposable material from other building tenants. Since local office staff estimate that as much as 90 per cent of waste is personal information, auditors questioned the need to sort. The auditors also found that no single unit ensures that all microfiche are accounted for and eventually destroyed. The procedures varied from sending old fiche to regional offices, regional computer centres or to National Archives. The auditors suggested a standard procedure for eventual destruction of out-of-date fiche.

EIC's Security Task Force will address both the incorporation of security clauses in service contracts and the control and destruction of microfiche in its workplan.

Employee Assistance Files (EAP)

These files are among the most sensitive personal files kept by government, recording personal information of individuals undergoing counselling for health or behavioural problems. The files are seen only by the employee and the counsellor. Theft or unauthorized release could cause the employee irreparable harm.

As a result, auditing EAP files poses its own problems for both the department and the Privacy Commissioner. The Commissioner is torn between needing to ensure that the information is seen by as few as possible but requiring evidence that it is appropriately collected and protected. Thus, the auditor examines randomly selected anonymous files to determine whether the information meets privacy standards for collection, use, retention, disclosure and disposal.

In EIC's case there were no EAP files in the Ottawa office. EIC's policy is to maintain as little information as possible, passing necessary details on to outside counsellors. The decision not to maintain files is understandable, even commendable, as a method of ensuring client confidentiality. But the practice means there is no documentary evidence of uses of the information, nor that the client has consented to its release.

The Commissioner observed that the department has to make a trade-off between restricting the amount of sensitive personal information in files and the need for operational controls. He proposed that EIC re-examine its current procedures.

Auditors made several suggestions for improving physical security of the unit's records and disposal of waste containing personal data. The Commissioner recommended that EIC also make the improvements in the regional offices that kept files.

Notifying the Commissioner

Generally, the *Privacy Act* prohibits federal government agencies from releasing personal information to anyone other than the individual concerned. As with most rules, there are exceptions. In fact, the Act has 13 — from releases to comply with a warrant or subpoena, to helping validate aboriginal peoples' claims or grievances.

Among those exceptions are two which require the government agency to notify the Privacy Commissioner. The first covers releasing information "in the public interest" or to benefit the individual concerned. The notification gives the Commissioner an opportunity to advise the individual of the release if that is considered necessary. The second exception deals with releases for a use "consistent" with the purpose for which it was originally collected (but not described in the *Personal Information Index*).

The *Privacy Act* does not provide a means for the Commissioner or the individual to block release. The *Access to Information Act* gives third parties the right to court action to prevent the release of corporate information. The Privacy Commissioner believes that individuals too should be able to prevent the release of what they consider to be unwarranted and damaging release.

There were early suspicions that these exceptions to the general rule prohibiting the disclosure of personal information to third parties would prove to be the *Privacy Act* "Mack truck" clause. It was feared that there would be a full-scale release of personal information based on broad interpretations of "public interest" and "consistent" use. To prevent such abuse, the Commissioner itemized all uses of these releases in his annual report.

So far no abuse has been evident. While the office continues to examine each notification, beginning this year, only global statistics and select examples for illustrative purposes are reported. A detailed breakdown of the 24 notifications can be obtained from the Privacy Commissioner's office.

The MPs — again

Once again Employment and Immigration Canada (EIC) advised the Privacy Commissioner how it would handle MPs' requests for personal information about constituents during the federal election campaign.

The *Privacy Act* allows government agencies to release personal information to an MP who is trying to help solve a constituent's problem. Once Parliament is dissolved, however, MPs have only the status of ordinary citizens. This means, according to the letter of the law, that MPs may no longer (without the individual's consent) inquire on behalf of a constituent about foul-ups with a government agency since this would require them to see personal information.

It seems doctrinaire to impede MPs seeking to help constituents while in the legal limbo of an election period. On the other hand, other candidates may feel unfairly disadvantaged due to the incumbent's special access to government information. EIC — the department most affected — advised the Privacy Commissioner that during the election period it would once again release information without consent to former MPs since it “would clearly benefit” the person concerned [paragraph 8(2)(m)(ii)].

The Privacy Commissioner agreed to the solution — the same one used during the 1984 election. But he repeated his concern that delegating the discretion to disclose personal information to “any” EIC officer or employee increased the opportunity for abuse. Privacy staff reviewed 1479 such notifications during the election campaign.

The *Privacy Act* should be amended before the next election to clarify whether, during an election period, incumbent MPs should maintain their special access to government information when helping a constituent.

Breach of dog's quarantine period

Canada Post advised the Privacy Commissioner that it had given an Agriculture Canada veterinarian the address change of a woman who appeared to have breached her dog's six-month quarantine period. The dog had been in contact with a rabid animal and had not completed the required treatment.

The post office reached the woman directly but she did not cooperate. Although the *Animal Disease and Protection Act* does not authorize release of the information, Canada Post concluded the disclosure was in the public interest. The Commissioner did not question the release.

Inmates' names and addresses to Chief Electoral Officer

Following a Manitoba Court decision that inmates had the right to vote in the federal election, Correctional Service Canada advised the Commissioner that it would give the names and addresses of all federal inmates in Manitoba to the Chief Electoral Officer of Canada.

The list was to be used by returns officers to organize the voting in penitentiaries and was not to be given to anyone else. However, since the court decision was appealed, the inmates were not enumerated and the list was not sent.

Soviet government alerted to visitor with TB

External Affairs advised the Privacy Commissioner that it had notified Soviet public health authorities about a Canadian visitor with an infectious disease.

Health and Welfare Canada had warned External Affairs that a woman with pulmonary tuberculosis had refused medication and checked herself out of the hospital. She then travelled to the Soviet Union to visit relatives. After calling the Privacy Commissioner's office, External informed the Canadian embassy in Moscow which, in turn, notified the Soviets.

The notification was considered "in the public interest".

Spreading the Word

It has been said that if there were a privacy constituency in Canada — a group of knowledgeable, committed privacy activists — it would fit in the Privacy Commissioner's boardroom (a snug fit even for the Commissioner's own staff).

The job is no longer so lonely. In fact, two recent conferences on privacy (and access to information) filled large meeting rooms in Toronto and Ottawa hotels. A loose network of federal, provincial and unaligned privacy advocates is emerging, allied with committed records and EDP systems managers to spread the word.

The public may still be puzzled when told of a *Privacy Act* (and find it faintly hilarious that there is a Privacy Commissioner). Nevertheless, people understand the issues and find them deadly serious.

The Commissioner and his staff welcome opportunities to discuss the Act and the issues. During the year the Commissioner completed a series of some 20 speeches to Canadian Clubs across the country, spoke to (among others) trainee intelligence officers, data processors, heads of federal government agencies and middle level financial managers. He also participated in a Canadian Chamber of Commerce briefing on the implications for the private sector of privacy legislation and the OECD guidelines; and on AIDS at a National Parole Board seminar.

The Commissioner began a series of visits to federal penitentiaries to discuss the *Privacy Act* with staff and inmates. So far he has visited the Prison for Women in Kingston and the medium security institution at Springhill, Nova Scotia.

The Commissioner's staff continues to brief participants on the government's management training courses and spoke to Coast Guard staff in Halifax, a race relations seminar in Montreal, and college classes in Toronto and Ottawa.

The office produced an information package entitled "Do you need help using the *Privacy Act*?" It includes a poster, bookmark and an explanatory brochure describing the Commissioner's role and how to use the office's services.

Corporate Management

Corporate Management provides both the Information and Privacy Commissioners with financial, personnel, administrative, data processing and library services.

Finance

The Offices' total resources for the 1988-89 fiscal year were \$5,074,000 and 69 person-years, an increase of \$1,152,000 and 11 person-years over 1987-88. Personnel costs of \$3,837,201 and professional and special services expenditures of \$702,567 accounted for more than 88 per cent of expenditures. The remaining \$603,137 covered all other expenses.

Personnel

A substantial increase in person-years for the Privacy Commissioner produced a very active personnel program. New positions were classified and there were 42 staffing actions including two senior management appointments. In addition, the offices underwent a biennial classification audit by Treasury Board and the PM (program management) and IS (information services) positions were reviewed in line with the new classification standards.

The following are the Offices' expenditures for the period of April 1, 1988, to March 31, 1989.

	Information	Privacy	Corporate Management	Total
Salaries	\$ 1,268,673	\$1,469,048	\$568,480	\$3,306,201
Employee Benefit Plan Contributions	202,500	246,600	81,900	531,000
Transportation and Communication	29,363	66,204	118,094	213,661
Information	57,681	38,815	1,526	98,022
Professional and Special Services	506,936	144,959	50,672	702,567
Rentals	2,898	64	5,294	18,256
Purchased Repair and Maintenance	1,337	5,112	21,940	28,389
Utilities, Materials and Supplies	9,957	14,738	37,264	61,959
Acquisition of Machinery and Equipment	43,232	85,986	48,464	177,682
Other Payments	1,630	1,569	1,969	5,168
TOTAL	\$2,124,207	\$2,073,095	\$ 945,603	\$5,142,905

Administration

The offices moved to the 3rd and 4th floors of Tower B, Place de Ville. Improved security measures were implemented for the new premises and a security manual was prepared. In addition, National Archives completed a records management audit.

Informatics

A review of informatics was undertaken with the assistance of outside consultants. The office will implement the major recommendations of the study concerning renewal of the case management system and expansion of report and text production facilities.

Library

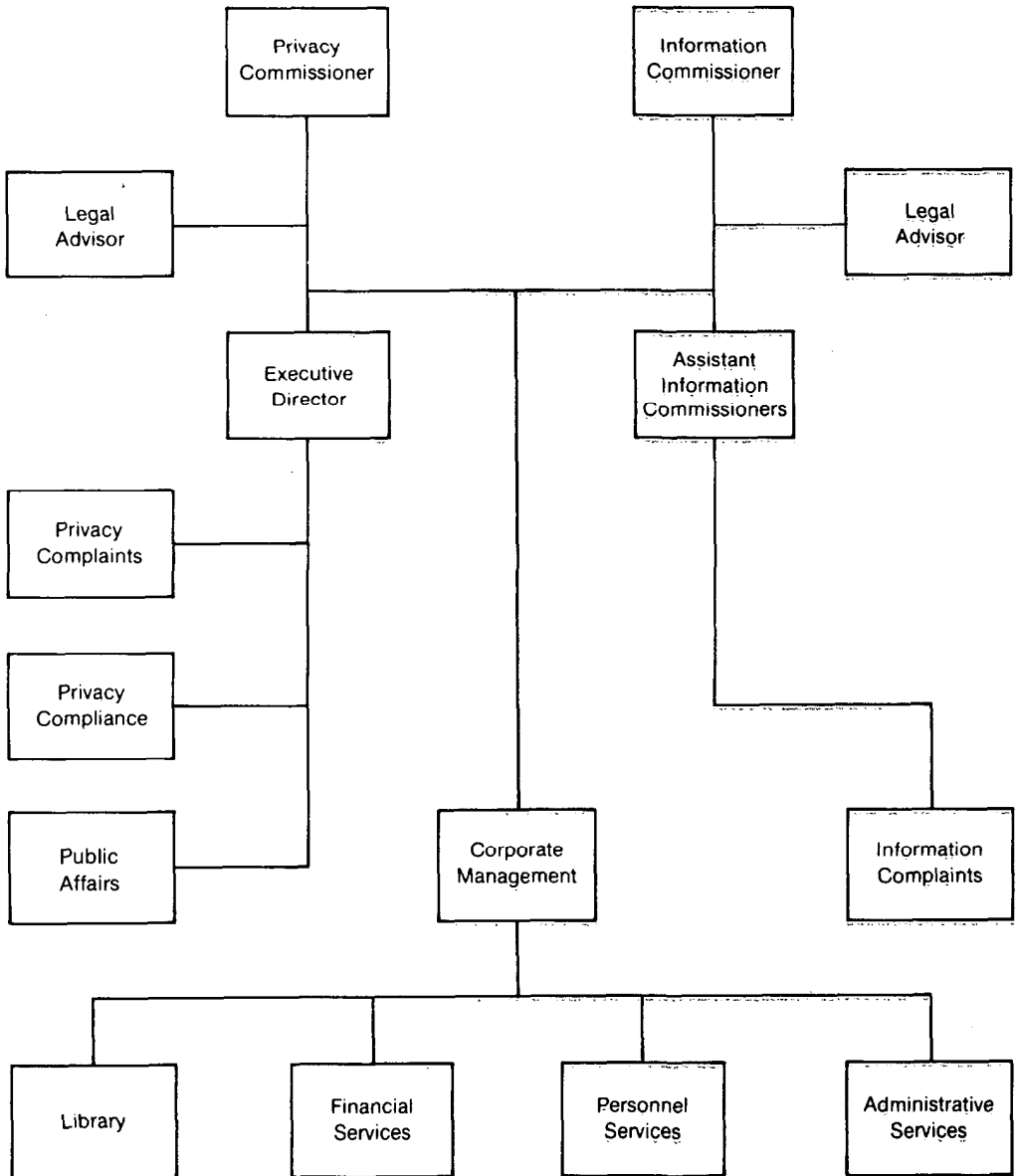
The library continues to provide an information and referral service for both Commissioners. It offers a full range of library services, including interlibrary loan, automated reference, and literature searches.

Last year, approximately 500 publications about access to information, the protection of privacy and the ombudsman function were added to the library's inventory. The public is welcome to consult our collection, which also includes newspaper clipping files, periodicals, and annual reports.

Appendix I



Offices of the
Information and Privacy
Commissioners of Canada



Appendix II

Government Institutions Covered by the Act

Advisory Council on the Status of
Women

Agricultural Products Board

Agricultural Stabilization Board

Agriculture Canada

Atlantic Development Council

Atlantic Pilotage Authority

Atomic Energy Control Board

Bank of Canada

Bilingual Districts Advisory Board

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

Bureau of Pension Advocates

Canada Council

Canada Deposit Insurance
Corporation

Canada Employment and Immigration
Commission

Canada Labour Relations Board

Canada Lands Company Limited

Canada Mortgage and Housing
Corporation

Canada-Newfoundland Offshore
Petroleum Board

Canada-Nova Scotia Offshore
Petroleum Board

Canada Ports Corporation

Canada Post Corporation

Canadian Aviation Safety Board

Canadian Centre for Occupational
Health and Safety

Canadian Commercial Corporation

Canadian Cultural Property Export
Review Board

Canadian Dairy Commission

Canadian Film Development
Corporation

Canadian Government Specifications
Board

Canadian Grain Commission

Canadian Human Rights Commission

Canadian Institute for International
Peace and Security

Canadian International Development
Agency

Canadian International Trade Tribunal

Canadian Livestock Feed Board

Canadian Patents and Development
Limited

Canadian Penitentiary Service

Canadian Pension Commission

Canadian Radio-television and
Telecommunications Commission

Canadian Saltfish Corporation

Canadian Security Intelligence Service	Freshwater Fish Marketing Corporation
Canadian Unity Information Office	Grain Transportation Agency Administrator
The Canadian Wheat Board	Great Lakes Pilotage Authority, Ltd.
Communications, Department of	Hazardous Materials Information Review Commission
Consumer and Corporate Affairs Canada	Health and Welfare Canada
Defence Construction (1951) Limited	Historic Sites and Monuments Board of Canada
The Director of Soldier Settlement	Immigration and Refugee Board
The Director, The Veterans' Land Act	Indian and Northern Affairs Canada
Economic Council of Canada	International Development Research Centre
Employment and Immigration Canada	Investment Canada
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 of Canada
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 Canada	

National Defence	Office of the Custodian of Enemy Property
National Design Council	
National Energy Board	Office of the Director of Investigation and Research
National Farm Products Marketing Council	Office of the Inspector General of the Canadian Security Intelligence Service
National Film Board	Office of Privatization and Regulatory Affairs
National Library	
National Museums of Canada	Office of the Superintendent of Financial Institutions Canada
National Parole Board	Pacific Pilotage Authority
National Parole Service	Pension Appeals Board
National Research Council of Canada	Pension Review Board
National Transportation Agency (formerly Canadian Transport Commission)	Petroleum Compensation Board
	Petroleum Monitoring Agency
Natural Sciences and Engineering Research Council	Prairie Farm Assistance Administration
	Prairie Farm Rehabilitation Administration
Northern Canada Power Commission	Privy Council Office
Northern Pipeline Agency	Public Service Commission
Northwest Territories Water Board	Public Service Staff Relations Board
Office of the Auditor General	Public Works Canada
Office of the Chief Electoral Officer	Public Works Land Company Ltd.
Office of the Commissioner of Official Languages	Regional Development Incentives Board
Office of the Comptroller General	Regional Industrial Expansion
Office of the Coordinator, Status of Women	Revenue Canada
Office of the Correctional Investigator	Royal Canadian Mint

Royal Canadian Mounted Police	Solicitor General Canada
Royal Canadian Mounted Police External Review Committee	Standards Council of Canada
RCMP Public Complaints Commissioner	Statistics Canada
The St. Lawrence Seaway Authority	Statute Revision Commission
Science and Technology Canada	Supply and Services Canada
Science Council of Canada	Tax Review Board
The Seaway International Bridge Corporation, Ltd.	Transport Canada
Secretary of State	Treasury Board Secretariat
Security Intelligence Review Committee	Veterans' Affairs Canada
Social Science and Humanities Research Council	War Veterans Allowance Board
	Yukon Territory Water Board