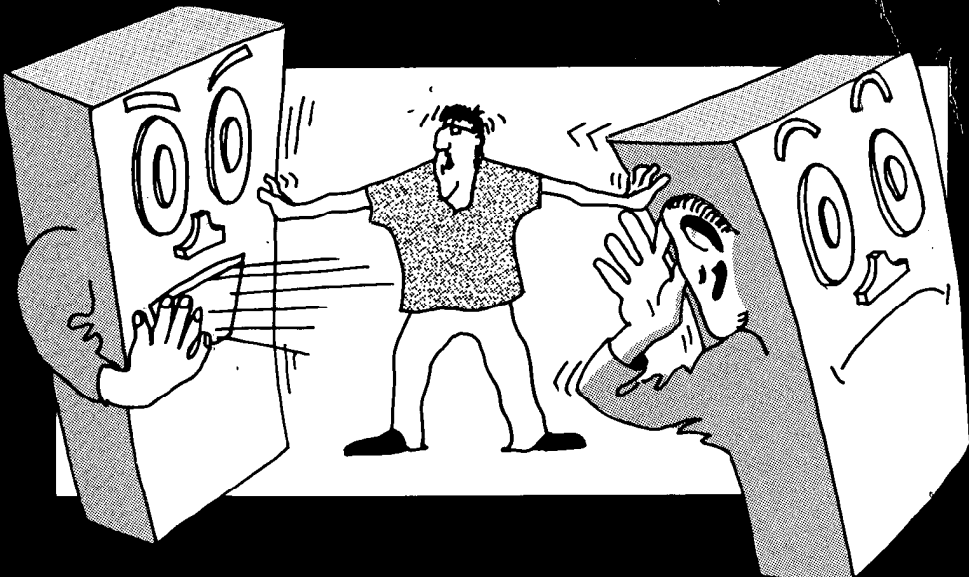


Annual Report Privacy Commissioner 1987-88



**Annual Report
Privacy Commissioner
1987-88**



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

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

© Minister of Supply and Services Canada 1988

Cat. No. IP30-1/1988

ISBN 0-662-55287-3

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

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

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

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

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

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

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

The *Privacy Act*

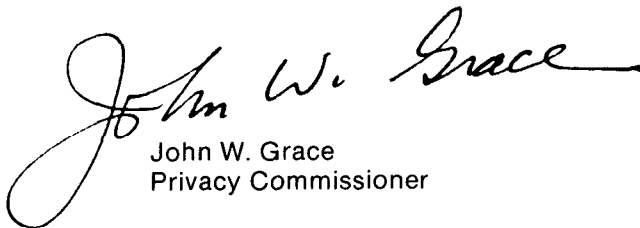
The Honourable Guy Charbonneau
The Speaker
The Senate
Ottawa

June 30, 1988

Dear Mr. Charbonneau:

I have the honour to submit to Parliament my annual report. This report covers the period from April 1, 1987, to March 31, 1988.

Yours sincerely,


John W. Grace
Privacy Commissioner

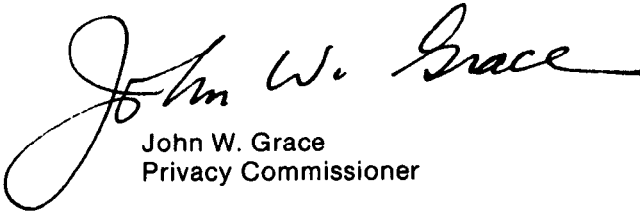
The Honourable John Fraser, P.C., Q.C., M.P.
The Speaker
The House of Commons
Ottawa

June 30, 1988

Dear Mr. Fraser:

I have the honour to submit to Parliament my annual report. This report covers the period from April 1, 1987, to March 31, 1988.

Yours sincerely,

A handwritten signature in cursive script that reads "John W. Grace". The signature is fluid and elegant, with a large initial "J" and a long, sweeping underline.

John W. Grace
Privacy Commissioner

Contents

Mandate	1
Five Years in a Life	2
Issues - Old and New	14
Data Matching and SIN	14
"Consistent Use"	15
Parolees, Inmates and Privacy	16
Privacy in the Workplace	18
Complaints Branch	22
Complaints	23
Using the Privacy Act	37
Compliance Branch	38
The Audits	39
Environment Canada	39
Transport Canada	40
Agriculture Canada	42
Correctional Service Canada	43
Notifying the Commissioner	44
Spreading the Word	45
Inquiries	46
Corporate Management	47
Appendices	
I Organization Chart	49
II Government Institutions Covered by the Act	50

Mandate

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

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

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

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

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

- an institution is collecting, keeping or disposing of personal information in a way which contravenes the *Privacy Act*.

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, without having to wait for a complaint.

Five Years in a Life

It is now five years of life under the *Privacy Act*, five years of these accountings to Parliament (and the country) on how its legislation is being observed; five years of alarms and preachments over the threats of the new information technologies — usually in their benign guise of efficiency — to precious and vulnerable human values.

Not a long span in the life of a law. Not a long time to show results within a system as multifarious and intractable as the federal government establishment. Yet the conclusion in this fifth year must be that the *Privacy Act* has already proved its value beyond all the early (and often understandable) skepticism. That judgment is not of a privacy partisan such as the Privacy Commissioner but of the government as it responded this past year to the remarkably comprehensive and highly supportive review of the Act by a committee of Parliament.

The issue at this five-year point is not the need for privacy legislation, but whether its sweep and its powers are sufficient for the threat and the challenge.

It is hardly conceivable today that a democratic country would not control the use of personal information which its government collects from individuals in ever-increasing amounts. The new privacy threats are so explosive, so unexpected that a single code probably cannot be written to cover them.

Consider what happened to Robert Bork in the midst of the Senate hearings into his nomination as a Justice of the United States Supreme Court. A Washington newspaper obtained and published a list of the movies that Mr. Bork had rented from a video store. But until this outrageous invasion of personal privacy had occurred, who had worried about protecting the privacy of video store customers? (One U.S. senator was so appalled by the lapse of journalistic standards that he brought copies of his own video records to the committee to show how they can be misconstrued. His list revealed that he had rented something the store called "Cat on a Hot" which was the short form for "Cat on a Hot Tin Roof".)

As the direct result of the abuse of Mr. Bork's privacy, legislation has been proposed in some American states to bar such a repellent practice.

But what will the next law be required to stop? Where will the next scary breach of privacy come from? Are we to worry about public libraries releasing lists of their borrowers' selections to investigators or journalists? Pray not! But record-keepers, be they in a video store, a library, personnel or credit card office, can spill out at the push of a button personal information to damage, to defame or merely to titillate.

Another example of the difficulty of keeping privacy protection ahead of technology (and, sometimes, hysteria) is found in the proliferation of tests of greater or lesser reliability.

Old-fashioned, personal evaluations of suitability, character and experience are giving way to science and pseudo-science. One American privacy specialist, Robert Ellis Smith, has observed that in his country it is becoming commonplace for employees to face fingerprinting, lie detectors, urinalysis, psychological tests, blood tests, computerized criminal record checks, handwriting analysis and, yes, clearance by astrology.

In the *New York Times*, William Safire wrote:

“We are frisking each other. Picture yourself going to work tomorrow, handing over blood and urine samples, taking a quick turn with the house polygraph, turning out your pockets and walking through some new fluoroscope. You object? Whatsamatter, you got something to hide?”

Nothing at all to hide; privacy and dignity to lose.

John Shattuck, who teaches privacy law at Harvard and is a vice-president of that university, has said that there is “a basic unregulated quality” to the new systems and practices which invade the sanctuaries of what once were private places. The new technologies are outside the traditional boundaries of privacy law, Mr. Shattuck says, “either because there is no law, because the law is obsolete, or because a decision has been made simply not to apply the law”.

Not a situation to please anyone, liberal or conservative, left wing or right.

The use of the so-called objective and impersonal tests becoming routine in some places is not yet out of control in Canada but, unless care is taken, we may be seeing our future elsewhere.

Protection Improves

Comfort should be taken where it can be found. It can be said that after five years Canada's *Privacy Act* continues to be applied with increasing sensitivity and rigor. While the application remains uneven, there can be growing, not shrinking, confidence that information which individuals give their federal government — often with no choice — will be used only for the purposes for which it is given and will be seen only by persons with the need or right to know.

These are important principles to defend and enforce. Those who know use their knowledge, a truism, as *The Economist* has observed, applying “to many down the years, from tempted Eve in the Garden of Eden to Ivan Boesky in New York” or, bringing the matter closer to home, to a cabinet minister in Nova Scotia.

Privacy laws exist first of all to protect people. Legislators have brought them forward out of the most benevolent of motives: the conviction that their constituents need to be defended from the misuse of their personal information by the state.

But governments should recognize that they too become beneficiaries of effective data protection, though on occasion it may be a nuisance or an embarrassment. Individuals will be more likely to give their government

better quality information, whether required by law as in a census or in tax returns, or in a voluntary survey, if they know that such personal information is protected by the principles found in the *Privacy Act*.

Moreover, countries with data protection laws are showing an increasing reluctance to allow their citizens' data to flow unrestrained to countries without such laws. Off-shore "data havens" would pose sovereignty and economic as well as privacy threats.

It is not entirely pure benevolence, therefore, that this past year has motivated such diverse countries as the Netherlands, Greece, Ireland, Finland and Japan to bring forward privacy legislation broadly similar to that which has been in place in Canada's *Privacy Act* for five years (three years earlier counting Part IV of the *Canadian Human Rights Act*).

Whatever the motives, the enhancement of privacy protection is on some national agendas, far perhaps from the top, but at least under "other matters".

The good privacy news in Canada last year, the biggest news in the privacy business, was not — let us be grateful — of new privacy Chernobyls, or even of more extravagantly lost documents; that epidemic has apparently passed. No, the central event — entirely reassuring — was the government's commitment to the acceptance of key recommendations of *Open and Shut: Enhancing the Right to Know and the Right to Privacy*, the report of the Committee on Justice and Solicitor General after its review of the *Privacy Act* and the *Access to Information Act*.

"The government agrees that changes can be made to the *Privacy Act* to make it more effective as a data-protection statute. This will allow it to remain on the cutting-edge for matters concerning protection of personal information and the setting of standards for effective controls on the collection, use and disclosure of such information by government institutions."

There it was; a Privacy Commissioner could not have put it better. The words are from the government's policy paper, *The Steps Ahead*, issued in response to the committee's recommendations.

Change Is On

Best of all, the game's afoot: significant changes have begun, none more important than the new data-matching policy being put in place. The new policy gives Canada what may well be the toughest and, from a privacy protector's point of view, the most enlightened data-matching code anywhere in the world.

Five years ago, the term "computer-matching" or "data-matching", if heard at all, was probably associated with some high-tech, lonely-hearts introduction service. In fact it is a technique which, unbridled, would present an Orwellian threat which even Orwell could not have imagined. The invasive, indiscriminate use of the computer in gathering, storing and comparing personal information for purposes either benign or malign, reduces individuals to commodities, subjugates human values to mere efficiency.

It would be foolish and dangerous to claim that the genie has been pushed all the way back into the bottle. But the new data-matching policy, effectively applied, makes it possible to entertain reasonable hope that the age of the transparent citizen can at least be delayed.

Perhaps it is neo-Luddite and unrealistic to argue that under no circumstances should data-matching be allowed. The benefits of the computer are not to be denied. The issue, cited four years ago in the Privacy Commissioner's report, is "the adequacy of safeguards to prevent violations of personal privacy". The notion was expressed that data-matching which uses an individual's personal information without knowledge and consent for purposes other than for which it was given was at least implicitly prohibited by the *Privacy Act*.

It was reassuring to have in *The Steps Ahead* the government's view that "the current *Privacy Act* provides sufficient authority to regulate data-matching and data linkage". The question then is one of the effectiveness of the regulation.

This can be said: if the new data-matching and linkage policy is observed in letter and spirit, Canadians for the first time have a reasonable assurance that their privacy will not be systematically breached as the custodians of enormous federal government data banks allow their whirring computers to run free. In fact, the gleam has been taken out of the eyes of some data processors.

Even if the *Privacy Act* had accomplished nothing else in the past year — or the past five years — it has justified its existence by being the instrument of control over data-matching. The significance of the accomplishment cannot be over-stated.

Two years ago, Professor Kenneth C. Laudon, an American authority on computer systems, wrote a book called *Dossier Society*, such a society being the dark side of the information economy. The strength of the new technology lies, Professor Laudon observes, "in its ability to move data efficiently across organizational boundaries and combine it with data from entirely different programs and files".

Here is Professor Laudon's description of the most significant characteristic of the "dossier society" from the individual's point of view:

"...decisions made about us as citizens, employees, consumers, debtors and supplicants rely less and less on personal face-to-face contact, on what we say or even what we do. Instead, decisions are based on information that is held in national systems, and interpreted by bureaucrats and clerical workers in distant locations ... decisions based on a comprehensive 'data image' drawn from diverse files."

The *Privacy Act* is the only mechanism Canada has standing in the way of unchecked federal government surveillance by computer. And, as has been acknowledged in previous reports, the justification for information sharing, so far, has been unflinchingly good — tracking down those who refuse to pay court-ordered support to children and former spouses, catching welfare cheats and debtors, establishing centralized police information systems.

It is precisely the goodness of the cause which makes matching both so attractive and so hard to stop. Yet, Professor Laudon maintains that unrestrained matching bestows upon a central government an “aggregation of power” over its citizens without precedent in peacetime and without constitutional consent. Whenever bureaucrats meet to design national information systems, it is Professor Laudon’s startling conclusion that “a small constitutional convention is in progress”. Though this may be an exaggeration, the consequences for computer centralization and sharing of personal information on a national scale could be much more serious than generally realized in this country.

That is why the federal government’s commitment to control its own computers, using the authority of the *Privacy Act*, is the best privacy news of the year — or many years. The challenge now for the Privacy Commissioner’s office is to monitor the policy effectively. The dawning of the age of the dossier society need not be upon us.

Saying no to SIN

The year produced additional encouraging privacy news as the government formally acknowledged that Canadians do not want the Social Insurance Number (SIN) to become a universal identifier. *The Steps Ahead* makes the commitment, so far as the federal government is concerned, that “no right, benefit or privilege will be withheld from and no penalty be imposed on” any individual who refuses to disclose his or her SIN except where its provision is required by law.

That policy falls short of the recommendation, made in this report last year, that no organization, government or otherwise, should be able to deny goods, services or benefits for failure to produce a SIN — unless, of course, it was specifically demanded by statute. Yet a good start has been made. The legal obstacles to launching a broader attack on the tyranny of the SIN are undoubtedly formidable.

Even so, the iron fist is almost showing through the velvet glove. The government has said that if the public sector and the private sector do not bring the use of SIN under control “legislative alternatives” will be explored “including, if necessary, an amendment to the Criminal Code to prohibit a request for the number unless authorized by law”.

In setting forth tough controls against the proliferation of abuses of the SIN within its own establishment, the government puts itself in a much stronger moral position to preach on the wages of SIN both to other public jurisdictions and the private sector.

On To Crown Corps

The third piece of good news in the privacy year was the promise to extend the mandate of the *Privacy Act* to cover federal Crown corporations and their wholly-owned subsidiaries. This was the recommendation of the parliamentary review committee. The government did not accept the committee's much broader recommendation that the federally-regulated private sector (banks, some telephone and trucking companies, for example) also be brought under the sway of the *Privacy Act*. Since this recommendation was one of the few made by the committee and not concurred with by the Privacy Commissioner, some explanation is in order, though the essential argument was made in an earlier report.

A broadening of the *Privacy Act's* universe beyond government would, of course, be justified by demonstrable and endemic abuses of privacy.

Indeed, there have been inquiries as to whether banks, telephone and cable television companies are covered by the *Privacy Act*. Sometimes anxious inquiries and public apprehension focus on the adequacy of privacy protection of credit card transactions.

The possibilities of violation are enormous and such nervousness is entirely prudent. Yet, while the dangers are real, the heavy hand of regulation should only be imposed if the private sector does not voluntarily take steps to address them.

Banks and their credit card associates, for example, have recognized that a high standard of privacy protection is simply basic good business. Thus, along

with other businesses, they are developing, albeit slowly, their own codes of fair information practice. Privacy codes have also been adopted by the cable television, insurance, direct marketing and information processing industries.

In another business sector, at the initiative of the Canadian Radio-Television and Telecommunications Commission, privacy protection provisions have been written into new telephone company regulations. The CRTC's action provides a model for other regulators.

A sectoral approach is being increasingly advocated and practiced. It is becoming recognized as the model for the next generation of privacy laws. It is consistent with the fashion, perhaps the trend, towards decentralization and self-regulation.

One international indicator of the new trend is the Netherlands' new Data Protection Bill which allows organizations or business sectors to draw up privacy codes and submit them to the data protection authority for review. The authority can give the code a "declaration" — in effect, a seal of approval — if it finds the code conforms with the legislation. Needs and, as noted earlier, dangers differ.

Won't Suit All

The general principles enunciated in broadly-applied legislation may not well serve diverse groups. For example, it is highly doubtful that the *Privacy Act*, however ingeniously (or monstrously) elaborated, can be an effective code of fair information practice at the same time for, not only video stores, but the direct mail industry, credit bureaus and cable television.

Thus do arguments for extending the *Privacy Act's* domain to the private sector at this time go against the grain. They seem more doctrinaire than based upon hard evidence of abuses. To push privacy legislation where it is not necessary would cause it to be held cheap, to make it a burden rather than something valuable.

It would also require a greatly expanded Office of the Privacy Commissioner. Were the Act to cover all federally-regulated private sector firms, some 25,000 new institutions would be included. Even if the Act were to be applicable only to firms with 500 or more employees, 800 or 900 firms would be affected. Such an extension, by conservative estimate, would require a three to four-fold increase in human and financial resources in the Commissioner's office. Privacy protection would become big and expensive business. No one would gain from that.

Thus, there is no disappointment on the part of the Privacy Commissioner that the Crown corporations and no more have been brought under the *Privacy Act's* sway at this time. But the close call for the banks and the others in the federally-regulated category should be taken as notice. The handwriting in the parliamentary committee's report is a powerful incentive for the private sector to put its privacy house in order if it does not want legislation.

Assuming the private sector prefers a regime of voluntary to compulsory privacy regulation, scrupulous compliance with the data protection principles set forth in the guidelines of the Organization for Economic Co-operation and Development (OECD) would be a good place to start. Canada has endorsed the OECD's guidelines. The principles comprise essentially the same code of fair information practices as set forth in the *Privacy Act*. The minister of external affairs has called Canada's endorsement to the attention of major Canadian companies and urged that the OECD guidelines be put into practice. So far, the impact of this request is not discernible.

A few more steps

Though it risks turning too much of this report into a gloss of *The Steps Ahead*, a few more significant initiatives should be noted.

The government's statement, "Individuals cannot assert their rights under the *Privacy Act* unless they are aware of them", is a tautology which needs saying. The promised public awareness program will fill a long-felt need.

Almost five years after coming into effect, the *Privacy Act* probably still remains more unknown than known to Canadians. Yet, even with this general state of unknowing, some 170,000 individuals have applied formally under the Act to receive their personal information. These impressive figures immediately demonstrate the use-

fulness of the Act. What will the numbers be following a vigorous publicity campaign? (Will privacy be advertised as effectively as "Participaction"?)

A little background to another useful initiative announced in *The Steps Ahead*. Section 37(1) of the *Privacy Act* says that "the Privacy Commissioner may, from time to time" at his discretion, "carry out investigations ...to ensure compliance" with the Act's broad principles.

The Steps Ahead says "such audits are desirable" arguing that the *Privacy Act* does not "expressly authorize the Privacy Commissioner to conduct compliance audits on a regular and ongoing basis". The Act leaves compliance auditing to the Commissioner's discretion. The report announced that the Act will be amended to make the authorization explicit.

Such an amendment will be welcome, not because any institution has even slightly questioned the authority to carry out an audit. Nor has the Privacy Commissioner felt at all inhibited about initiating audits. (Why would the Act give the discretionary authority if it were not to be exercised?)

No, an explicit injunction to audit regularly sends the message that the Privacy Commissioner's compliance auditors will be coming. That message is important because regular, systematic auditing is the wave of the future for privacy protection. It offers the greatest source of privacy comfort —inside and outside of government.

However, privacy audits in federal institutions conducted by internal, departmental auditors have not developed as quickly as they should. Most departments have still to accept the argument that privacy audits should be as routine and necessary as financial or management audits. Yet without privacy audits it is difficult to understand how the heads of the institutions, who are responsible for implementing the *Privacy Act*, can be sure that their departments are complying.

Only a handful of departments are known to be conducting some internal privacy auditing: Environment Canada, the Bank of Canada and, in the last year, Employment and Immigration Canada (EIC). If an organization as large as EIC, and which handles as much personal information as EIC can take on the daunting task of critically examining its own privacy practices, what excuse can there be for others? Sadly, they appear content to await the coming (for some, it will be a long wait!) of auditors from the Privacy Commissioner's office for their privacy check-up. That may be flattering. But these specialist auditors should not be doing basic departmental tasks; they should be auditing the internal auditors.

The essential role of privacy coordinators to the effective functioning of the *Privacy Act* is clearly asserted in *The Steps Ahead*. That is welcome support for they are the privacy professionals, the privacy consciences of their institutions. They are sometimes pulled by a conflicting loyalty to their

colleagues and institutions on one side and to the abstraction called data protection on the other. That is why they should be persons of strength and status. They should have direct access to senior officials. Now the government too says that this should happen. Score at least two for the privacy coordinators!

These admirable fresh privacy initiatives set out in *The Steps Ahead* would be only posturing without the will and resources to carry them forward. It is too early to give out final grades, but the action plan for putting the new policies into effect has about it an encouraging look of rigor.

The tougher SIN and data-matching policies have been produced as promised. Others seem to be under way: for example, strengthening personal data protection provisions in the new security policy; a training regime so that federal public servants, notably privacy coordinators, may better discharge their responsibilities under the *Privacy Act*; putting in place by the Treasury Board of a new public awareness program. The Privacy Commissioner's staff is participating with Justice and Treasury Board officials in orientation sessions across the country at head offices of the Crown corporations coming under the mandate of the *Privacy Act*.

Other commitments will require more time. These include important *Privacy Act* amendments that will give unequivocal privacy protection to the

personal information of public servants; provide a specific public education mandate for the Privacy Commissioner's office; facilitate the extension of the *Privacy Act* to some Crown corporations, such as Petro Canada.

When all these policies and amendments are finally in place, Canada's third-generation privacy legislation will continue to be as good as any in the world. No apologies needed.

What didn't happen

Yet a few more changes which the government's response did not address could make the good better. The greatest disappointment is that no commitment was made to provide a mechanism in the *Privacy Act* for an individual to prevent the release of personal information pending resolution of any dispute over the appropriateness of the release. The point is this, as made in last year's report:

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

From anomaly to incongruity: the *Access to Information Act* provides a mechanism for notice to and comment by corporations whose sensitive commercial information may be released. Yet, the *Privacy Act* accords no similar rights to individuals whose sensitive personal information may be disclosed. Personal information deserves protection from abuse that at least equals that afforded corporate information. Amendments to the *Privacy Act* should end the incongruity.

Now back to the old vexation of section 19 of the *Privacy Act*, somewhat less vexatious than when first raised four years ago, but still an untidy, unsatisfactory business. Under section 19, federal government institutions *must* refuse release of any personal information received in confidence from a province. In 1983, most provinces, nervous and defensive, claimed confidentiality over all information already supplied to federal departments as well as information to be supplied in the future.

These blanket claims of confidentiality were a standing rebuke to the spirit of the *Privacy Act*. They have proved particularly troublesome in the parole and corrections field. Applicants are routinely refused information from their files at Correctional Services Canada (CSC) and the National Parole Board (NPB) only because it has been supplied by a provincial or municipal police force or a provincial parole or correctional service. CSC and NPB cannot release even the most innocuous information, which would be routinely released had it originated federally.

Rather than simply dismiss many complaints because federal departments have no choice but to withhold information, the Privacy Commissioner encouraged CSC and NPB to seek provincial agreements that would permit information to be processed under the *Privacy Act* as if it were federal information.

It Worked... sort of

The strategy produced some encouraging results: arrangements have now been made with Quebec, New Brunswick, Nova Scotia, Prince Edward Island and the Yukon. However, other provinces have not agreed. Ontario's case is particularly disappointing and curious because as of January 1, 1988, it proclaimed its own legislation to provide rights of access to personal information. The Ontario bill gives the province discretion to provide access to confidential federal information, as if it were its own — a curious double standard.

Unfortunately, no longer is there any reasonable expectation that the Commissioner can resolve complaints on information from Ontario, Manitoba, Saskatchewan, Alberta or British Columbia. Cases have too long been delayed already out of that hope. Now, there is no choice but to allow the use of section 19. It means geography will determine privacy rights. Some individuals will be granted access to personal information supplied by certain provinces; others will be denied access to similar information supplied by other provinces. That is essentially wrong.

There is a last hope — the political level. An agreement among the minister of justice, the solicitor general of Canada and all provinces could yet end this arbitrary discrimination. The cause is worth another effort.

As the finishing touches are applied to Canada's third generation of data protection rules, the focus shifts to new pressing privacy issues.

Towards an AIDS Policy

Perhaps the most sensitive and anguished privacy issue arises from our national response to acquired immune deficiency syndrome (AIDS). In what situations, if indeed any, is compulsory AIDS testing to be permitted? How should government use AIDS-related personal information which it holds? To whom and in what circumstances may AIDS-related personal information be disclosed? Does the stigma of AIDS require that it be treated differently than other communicable diseases? What level of physical security should AIDS-related information receive? These are fundamental questions to the development of a federal privacy policy on AIDS information.

Such policy should be developed by government, by legislators, not by the Privacy Commissioner. He will press the privacy interest — vigorously. But many competing concerns must be considered by those with over-reaching responsibilities.

Based on the assumption that a lack of information should not prevent development of a coherent, sensitive privacy policy on AIDS, the Privacy Commission has initiated a study of AIDS from the privacy perspective so as to provide the best and latest advice. Key government departments gave full cooperation to this study.

The federal umbrella confronts the issue of AIDS on many fronts — in its dealings with prisoners, immigrants, its own employees (be they foreign service officers, members of the armed forces, prison guards or nurses). While Health and Welfare Canada encourages employers to establish AIDS policies, the country's largest employer — the federal government — has as yet no such policy of its own.

Absence of a general policy does not mean that AIDS testing programs have not been implemented. For example, National Defence has begun an AIDS-testing program to meet a requirement established by the U.S. Defence Department. This American policy requires all foreigners attending U.S. defence training courses to certify that they do not carry the AIDS antibody. More than 1,000 military and civilian employees of Canada's National Defence department attend these courses annually.

It is open to serious question whether U.S. policy on AIDS testing should drive Canadian policy. But the fall-out cannot be avoided. For example, should Canada reject mandatory AIDS testing, what would be the impact on the careers of employees denied access to U.S. defence training courses because either they refused to be tested or they tested positive?

If Canadian policy encourages only voluntary AIDS testing, then a clearly defined policy should be issued indicating how such information will be used and the circumstances under which it may be disclosed to third parties.

CSIS Files

Another unresolved issue of much discussion this past year is the balance to be struck between accessibility and secrecy in security and intelligence. The Canadian Security Intelligence Service (CSIS) is subject to the *Privacy Act*. However, few applicants have been given access to their files or have ever received confirmation whether a file on them exists. This should come as no real surprise to anyone; silence is in the nature of CSIS's business. There has been no pattern of non-compliance by CSIS with the *Privacy Act* and Parliament specifically provided exemptions for disclosure requirements, recognizing the special circumstances of security and intelligence work.

But there comes a point, either as time diminishes the sensitivity of information or because of its seemingly innocuous nature, where it becomes difficult to explain how the release injures CSIS.

This issue is being explored, with the co-operation of CSIS, with the aim of achieving a clearly defined and acceptable policy.

Welcome to the Club

Important Canadian privacy news of the year was not confined to the federal domain.

The coming into force of Ontario's *Freedom of Information and Protection of Privacy Act* advances significantly the quality of data protection in Canada. Covering provincial institutions as it does, Ontario's new law confers important privacy rights upon millions of individuals.

Cordial, close working cooperation has already been established between the office of the Ontario Commissioner, Sidney Linden, and that of the federal commissioner. Visits have been exchanged and useful consultations have taken place.

Strong provincial data protection statutes (Quebec's comprehensive law came into force in 1984) will be mutually re-inforcing both for the provincial and federal laws. Privacy, like freedom, should not be divisible.

ISSUES — Old and New

DATA MATCHING AND SIN

At the beginning of this report, the government's important commitment to establish controls on data matching and on the use of the SIN was included among the good privacy news of the past year.

The power, versatility and omnipresence of information processing technology are perhaps the greatest challenge to the effectiveness of the *Privacy Act* in the decade ahead.

A prime goal of the *Privacy Act* was to erase the possibility of the government establishing one central, comprehensive information file on any single individual. The central file possibility has reached technical feasibility as government holds more information in machine readable form. By using the Social Insurance Number (SIN), the government's personal identifier, computer matching techniques would accomplish what previously was felt — perhaps too smugly — to be most unlikely.

The government's commitment is therefore timely. The Privacy Commissioner's office has worked closely with Treasury Board officials responsible for drafting a detailed control policy. Canada could very well have the world's most rigorous controls on the use of computer technology to compare and compile information extracted from records contained in unrelated data bases.

Data Matching Policy

The major features of the new data matching policy are:

- * no data matching shall be undertaken except with the written approval of the head of the government institution involved, which, ordinarily, is the minister;
- * all proposed data matches will be appropriately documented including:
 - a preliminary assessment of a match's compliance with the *Privacy Act*, and
 - a further assessment of the costs and benefits of the proposed match against an analysis of the potential threat to the privacy of individuals;
- * all data matching will be described in the Index of Personal Information;
- * proposed data matches must be submitted to the Privacy Commissioner 60 days before the match is to begin;
- * any information generated from data matching must be subjected to independent verification before being used in a decision-making process that directly affects an individual; and
- * an individual must be given the opportunity to refute the information resulting from data matching before any action concerning the individual is initiated.

SIN policy

The government's commitment to return the SIN to its intended role as a specialized identifier for selected social programs is critical to data matching control. Only those programs authorized by Parliament to do so will use SIN. Gradually, other programs will replace SIN with unique identifiers, reducing the possibility of matching information from unrelated data bases by making it far less cost effective.

The new SIN policy will:

- * freeze further collections and uses of the SIN by government, unless authorized by Parliament;
- * review all existing collection and uses of SIN to ensure compliance with the *Privacy Act*;
- * require that all not statutorily mandated existing collections and uses of SIN be discontinued unless the Treasury Board believes that the benefits of continued collection and use of SIN would outweigh privacy concerns;
- * permit no right, benefit or privilege to be withheld, nor any penalty imposed on an individual for refusing to provide a SIN, except where collection is required by statute;
- * inform individuals of the purposes for which a SIN is requested, whether disclosure is mandatory or voluntary, and whether there are any consequences resulting from failure to provide.

While these initiatives are welcome, Parliament could yet override the policies and the *Privacy Act* by authorizing new computer matching programs and new uses of the SIN. The U.S. Congress, for example, has authorized widespread computer matching, particularly to detect and prevent defrauding government programs.

It is difficult to argue persuasively against this purpose and in Canada, too, it may be an important force for the proliferation of data matching. However, there is growing U.S. evidence that computer matching produces less significant savings than previously claimed. Proper program design and alternative enforcement techniques are as cost effective as data matching, and eliminate the consequent invasion of the privacy of innocent individuals.

As has been stated, other social "goods" may outweigh privacy. But it is for Parliament to make these judgments on the most informed basis possible. One critical piece of information is a rigorous cost/benefit assessment of any proposed new data matching activity. However laudable the social purpose Parliament should not authorize matching activity without weighing the costs and benefits against the potential invasion of privacy.

"CONSISTENT USE"

Now that both the *Privacy Act* and the new policy restrict data matching, government departments may be tempted to interpret "consistent use" broadly enough to match unrelated files.

The *Privacy Act* has no mechanism for the Privacy Commissioner (or anyone else) to challenge misuse of information in the courts. Departments could use the "consistent use" provision to undermine effective control over data matching.

The Ontario *Freedom of Information and Protection of Individual Privacy Act* attempts to prevent too broad an interpretation by including a definition of "consistent purpose". Section 43 of that act provides:

"Where personal information has been collected directly from the individual to whom the information relates, the purpose of a use or disclosure of that information is a consistent purpose ... only if the individual might reasonably have expected such a use or disclosure."

Thus, the Privacy Commissioner recommends two amendments to the *Privacy Act*: a definition to clarify interpretation of "consistent use"; and authorization for the Privacy Commissioner or any aggrieved individual to seek judicial review of a government institution's decision to use or disclose personal information.

The difficulties which lie ahead in taming technology to the principles of privacy should not overshadow the importance of the controls which were referred to earlier.

PAROLEES, INMATES AND PRIVACY

As promised in last year's annual report, the Privacy Commissioner reviewed the use and disclosure policies of the National Parole Board (NPB) and Correctional Service Canada (CSC). NPB gave the Commissioner a revised draft use and disclosure code for review. CSC policies were examined during the privacy audit described elsewhere in this report.

From the review the Commissioner identified three matters which he considered infringements of the *Privacy Act*. They governed disclosures to the RCMP, to victims and to the media and public.

Disclosures to the RCMP

The NPB and CSC disclosure policies authorize the release of parolees' and inmates' personal information to the RCMP, considering all such disclosures a "consistent use" of the information (paragraph 8(2)(a) of the *Privacy Act*). This does not recognize that the RCMP may be seeking information concerning a crime unrelated to the one for which the individual was sentenced.

CSC and NPB do not follow the *Privacy Act's* direction that disclosures to the RCMP be made only on written request, specifying the purpose and describing the information sought. Copies of these requests and a record of the information disclosed must be given to the Privacy Commissioner at his request.

As the two agencies consider all disclosures to the RCMP “consistent use”, neither requires written requests nor does it keep records of disclosures for the Privacy Commissioner’s review.

Even if RCMP requests are “consistent”, the *Privacy Act* requires them to describe the uses in the Personal Information Index and, in the absence of a listing, to notify the Privacy Commissioner of the disclosure and its purpose.

Never has the Privacy Commissioner been notified of disclosures to the RCMP even though they occur routinely. Moreover, many of the relevant CSC and NPB Index descriptions do not advise that disclosures may be made to the RCMP.

This behavior clearly inhibits the Commissioner’s independent scrutiny of disclosures specifically required by the *Privacy Act*.

Disclosure to Victims

NPB and CSC have a policy of telling the crime victim the date of an inmate’s release, conditions of the release, and his or her destination, considering such disclosures as consistent uses by paragraph 8(2)(a).

The Privacy Commissioner disagreed. Only when there is reason to believe that the person would harass, harm or otherwise put the victim at risk would the release be a consistent use, or clearly in the public interest (subparagraph 8(2)(m)(i) of the *Privacy Act*). Both the NPB and the CSC were

encouraged to assess each case individually rather than give blanket approval for such releases.

The release of personal information to third-parties violate inmates’ privacy rights and could jeopardize their re-integration into the community and, even, put them at risk.

CSC and NPB have agreed to develop a new policy on disclosures to victims which provides a much greater degree of control over such releases.

Disclosures to the Media and Public

The NPB and CSC policies previously authorized the release of an offender’s criminal record to the media and the public. Both agencies considered an individual’s criminal record to be unprotected by the *Privacy Act* because the information is publicly available in court records.

The Privacy Commissioner disagreed with this interpretation since it would mean that the criminal records of anyone could be assembled and disclosed to the general public — an unacceptably broad interpretation of what is meant by “publicly available”.

An individual’s conviction may indeed be recorded in publicly available court records, scattered perhaps across the country (and out of the country). However, this should not mean that a cumulative listing of convictions, prepared by a law enforcement or correctional institution, is also public. The

impact of cumulative records is quite different and distinct from a record of an individual conviction, particularly because they differ both quantitatively and in the consequences of their release. This is all the more so since cumulative records are more susceptible to inaccuracy and incompleteness.

It should also be noted that the Solicitor General has a strict policy of confidentiality for the RCMP as the national custodian of criminal record information. That policy authorizes no disclosures to the public or media.

Subsequent revisions by CSC and NPB to the policy have removed the authorization for the public release of an offender's criminal record.

PRIVACY IN THE WORKPLACE

Workplace issues will increasingly consume the Privacy Commissioner's time and attention as Crown corporations and their subsidiaries come under the jurisdiction of the *Privacy Act*. The combined workforce of the 130 additional institutions is greater than the 147 institutions already covered by the Act. An added complication is that some of the major Crown corporations (such as Air Canada and Petro Canada) compete in the private sector where few privacy rules apply and employee screening and monitoring are more widespread.

During the year public servants became worried that too much information about them was accessible under the *Access to Information Act*. They were concerned, for example, that management was seeking too many details about their medical conditions; that long-time public servants were having to undergo new, rigorous reliability and security clearance checks; and that drug testing, AIDS testing and electronic surveillance could strip them of personal privacy and dignity in the workplace.

Accessibility to Employee Data

The Commissioner's 1986-87 annual report summarized an investigation into the compliance of the government's *Conflict-of-Interest Code* with the *Privacy Act*. The Commissioner found that the *Privacy Act* may not protect personal information about public servants from disclosure to third parties under the *Access to Information Act*.

There were several complaints launched this past year about disclosures of public servants' information under the *Access to Information Act*.

For example, both the Department of National Defence (DND) and the RCMP released lists of all members and civilian employees in the National Capital Region who were earning \$42,000 a year and above, their rank, classification and their area of service within the department. In these instances, described in detail in the report's complaint section, the Privacy Commissioner concluded that such

information is not "personal" according to section 3(j) of the *Privacy Act* and cannot be protected. In fact, the departments are required to disclose the information. However, individuals should not be sitting ducks for commercial solicitation because they happen to be public servants. As in the conflict-of-interest investigation, these disclosures simply emphasized the need for a greater protection of information that the government holds about its employees. This is particularly critical for public servants working in sensitive, high security jobs whose safety could be threatened by the mere fact of their public identification.

The government discussed these concerns in *The Steps Ahead*, promising amendments to the personal information definition ... "to ensure that sensitive employee information, such as employment equity or conflict-of-interest declarations and employment appraisals, is treated as personal information and subject to the protection of the *Privacy Act*."

This amendment will not, however, resolve departments' dilemma when faced with request for lists of employees for commercial or soliciting purposes.

Disclosure of Medical Data

One public servant complained when he was denied sick leave benefits for refusing to give his superior the details of his illness or disability. The department argued that it needed the information because of the amount of

sick leave already taken, concern over the employee's physical well-being and its affect on the safety of the employee and others in the workplace, and the possible implications for long-term disability.

The Privacy Commissioner did not question the employer's need for evidence that the employee was unable to perform his duties due to illness or injury. However, collecting precise details of an illness, injury or other medical conditions is prohibited by section 4 of the *Privacy Act*. Employers questioning employees' sick leave claims can verify the medical status and fitness for work through a Department of Health and Welfare doctor.

The department agreed to this policy and the Privacy Commissioner recommended that all government institutions implement a similar approach.

Reliability and Security Screening

The Privacy Commissioner reported last year that while the government's new security policy did not contravene the *Privacy Act*, it left little to individual departments' discretion. This led to the spectacle of fingerprinting the staff shovelling snow from the skating rinks on Ottawa's Rideau Canal. After discussions with Treasury Board, the policy was amended to give departments the discretion to determine when credit and fingerprint checks would be a necessary part of an enhanced reliability check.

However, protection of the public servant's information collected under the policy should be addressed as part of the statutory amendment to the definition of personal information (see sample complaint on page 29). The Privacy Commissioner is also concerned that there may be too many public service positions requiring their incumbents to be security-cleared. Since security clearances to confidential, secret or top secret levels involve detailed background investigations, only those individuals whose duties truly require such clearance should be subjected to them. The Privacy Commissioner will be examining this matter to ensure that security clearances are not an arbitrary requirement.

AIDS testing

No one can ignore this as yet incurable and fatal disease, the acquired immune deficiency syndrome (AIDS). It is having an effect on all levels of our society and raises troubling, complex issues.

In responding to the AIDS epidemic, government policies and initiatives should balance two important and at times competing objectives: the protection of individual rights and the protection of the public health.

The government's collection, use and disclosure of AIDS-related information should, of course, comply with the *Privacy Act*. But should this category of medical information be treated

differently than personal information about other communicable diseases? *Does the Privacy Act prohibit or restrict mandatory AIDS testing? To what uses may AIDS-related information be put, to whom may it be disclosed and for what purposes.?*

Since the legal requirements are not clearly defined and a number of difficult questions need to be explored, the Privacy Commissioner has undertaken a study in close consultation with key government departments. A discussion paper is being prepared which should help the development of a policy on AIDS-related information which is both sensitive to privacy rights and the protection of public health.

Employee screening

The *Privacy Act* does not deal specifically with such screening and monitoring techniques as drug and polygraph testing and electronic surveillance. The Parliamentary Committee recommended that the Act be broadened from simply data protection, to include physical privacy and to give the Privacy Commissioner the authority to monitor developments in surveillance techniques. The government rejected this recommendation, believing that the *Privacy Act* should remain as a data protection statute and regulate only the collection, use and disclosure of the personal information produced by surveillance and tests.

The Act does deal adequately with the use and disclosure of results. However, compliance with the provision that government not collect personal

information unless it "relates directly to an operating program or activity" (section 4), continues to pose questions. Perhaps the most important one concerns the reliability of screening methods because the use of unreliable screening tests could itself contravene section 4. Similarly, intrusive screening, testing and monitoring techniques may represent prohibited forms of data collection if other, less intrusive, methods are available options.

The Privacy Commissioner will continue to watch closely the government's monitoring and testing of applicants and employees and will encourage the development of guidelines to protect individuals' privacy interests.

Exempt banks

Compliance audits on five remaining exempt banks found only one, National Defence bank DND/P-PU-040 (Security and Intelligence Information Files), properly constituted. (To be properly constituted, each file in the bank must be reviewed to ensure it consists "predominantly" of personal information whose release could injure Canada's international affairs, defence or law enforcement, or was obtained by an investigative body.)

The other banks listed as exempt in last year's report with the exception of RCMP bank CMP/P-PU-015 (Criminal Operational Intelligence Records), are now treated as open and their exempt status will be rescinded.

The Privacy Commissioner found the RCMP's remaining exempt bank too had not been properly constituted. He recommended the Solicitor General rescind the existing exempt bank order and seek a new, valid order if the Minister considers it necessary to maintain the bank's exempt status. The Solicitor General has disagreed, believing that all of the files which the Privacy Commissioner found not reviewed originally were not, in fact, part of the exempt bank.

Discussions toward resolving this factual dispute are in progress. In the meantime, the Solicitor General will maintain the exempt status of RCMP bank CMP/P-PU-015.

Complaints Branch

The office received 696 complaints during the year; 661 investigations were completed of which the Commissioner concluded that 155 (23 per cent) were well-founded and 492 (74 per cent) were not well-founded. The remaining 14 (3 per cent) were abandoned or withdrawn.

Compared with 1986-87 statistics, two changes are worthy of note. First, there has been a marked drop in delay complaints. Delay complaints account for 22 per cent of the caseload; the previous year they accounted for 56 per cent. This somewhat surprising change is responsible, in large measure, for this year's smaller proportion of well-founded decisions; delay complaints have usually been justified.

The second change is that 66 (8.6 per cent) fewer complaints were lodged than in the preceding year. For the first time in five years complaints have not risen by at least 10 per cent. While any reduction in complaints should be viewed positively — the ultimate goal, after all, is to have departments satisfy all users of the Act — the statistics do not necessarily reveal an entirely comforting story.

True, applications are now being handled by departments in a more timely fashion. There has been, however, a significant shift to more substantive complaints.

Almost 64 per cent of the year's completed complaints concerned denial of access to personal information. Compare this with only 36 per cent last year. The somewhat disturbing development is the sharp increase in

situations where departments have refused to provide requested information, not simply been tardy in processing a request. One year's figures do not make a trend but the rise in access denials will be carefully watched.

While the caseload for each of the seven investigators averaged a seemingly more manageable 99 for the year, down from 109 the previous year, the investigative effort required to complete the more complex caseload has in fact increased. In addition to the investigation of complaints, investigators also handled 1,248 inquiries, an increase of almost 10 per cent from the previous year (see page 46).

In total this represents an unsustainable work burden on investigators which would lead to an unacceptable backlog of cases. For this reason, as well as the anticipated new business from the Crown corporations being brought under the Act, it is encouraging to report that approval has been given for nine additional staff, including investigators.

The following cases illustrate the types of complaints the office dealt with during the year. Identifying details are removed because the Act requires that investigations be conducted in private.

COMPLAINTS

Commercial Use of Data

The vexed issue of releasing lists of departmental employees' names for commercial purposes commanded attention during the past year.

The concern can probably be best illustrated by the military officers who complained that releasing a list of National Defence personnel to an Ottawa man contravened the *Privacy Act*. The complainants concluded that the lists had been sold when they began receiving solicitations from a local real estate developer.

The man applied under the *Access to Information Act* for a list containing the "name, rank, job classification and level, office address and branch or unit" of all civilian employees and Armed Forces personnel in the National Capital Region "whose salary range equals or exceeds \$42,000 per annum."

Personal information may not normally be released under the *Access to Information Act*. The company's agent himself questioned whether obtaining this type of information violated the *Privacy Act*. However, the Act is clear; information about public servants' positions, functions and salary ranges, and their titles, business addresses and phone numbers is not "personal". This exception set forth in the *Privacy Act* establishes in law the public's right to know who is paid from the

public purse, and for what. The investigation, therefore, hinged on the interpretation of the definition of personal information about federal government employees.

The Commissioner concluded that DND was compelled to release the personal information and that he had little choice but to dismiss the complaints because the wording of the Act is clear. But the issue is troubling. Federal employees should not become targets for repeated canvassing for various goods and services. That possibility could not have been contemplated by those who drafted the *Privacy Act*.

There is even a potential security problem in releasing the names of staff and Armed Forces members. Many work in sensitive positions and they are not even listed in DND's own directories.

Following his investigation, the Commissioner wrote to the deputy minister of national defence to share his concern that "personnel working in particularly sensitive high security areas could be identified by hostile interests." It was pointed out that computer manipulation of particular lists could determine how DND "allocates its personnel by rank and location, thus inferring what military or intelligence priority it is giving to various activities and projects." The Commissioner asked DND to support an amendment to the *Privacy Act* closing this loophole. (See also next case).

Ditto RCMP

The security issue arose again in similar complaints from members of the RCMP. The police force had complied with an application almost identical to the request handled by DND. However, an RCMP staff relations representative expressed to the Commissioner "grave concerns" about the information "falling into the wrong hands".

The letter went on:

"The very nature of police work exposes members to possible reprisals by...terrorists, drug dealers and cop haters whose exploits fill our newspapers daily. Any member who is now working or has previously worked in the areas of drug enforcement or anti-terrorism will confirm that information such as work locations and business telephone numbers could, in criminal hands, jeopardize police operations and place both individual members and their families at risk."

The Commissioner reiterated his conviction that "a greater measure of protection should be given to information held by government about public servants." He recommended that Parliament amend the language of the section to make it clear which information about public servants should be considered public — and which should not. Until the definition has been tightened up, as promised in forthcoming amendments to the Act, departments should have a discretion to withhold certain job-related information about public servants when security is at issue.

Officer Gets Merit List Ranking

An Armed Forces officer complained to the Commissioner when DND would not tell him exactly where he stood on a promotion list. Such lists are prepared annually by merit boards which review all eligible members within each rank and occupational group.

National Defence did provide the officer with a computer-listing page containing column headings and his one-line entry. There was nothing to indicate his position on the otherwise blank page. He was told that DND had discontinued numbering positions in 1978 and, without numerical rankings beside each name, the department maintained it could not provide the information since it did "not exist on the record".

As a former career manager, the complainant said he knew managers often assigned numbers to promotion lists and, in fact, had been told his position every year from 1980 to 1985. As well, he believed the page number on the copy was wrong.

DND acknowledged that some members had been given their rankings in the past, but maintained that as word of the practice spread it became too time-consuming to respond to all the requests and the practice was stopped. The privacy investigator was told that although the department could determine an officer's position simply by counting down the list, it was not required to do so because the information "is not recorded or compiled in any form" and, therefore, does not qualify as personal information under the *Privacy Act*. (The staff also reiterated that the page number was correct.)

The investigator confirmed that the list was assembled "in order of merit" and that it was used to make administrative decisions about the individuals on such matters as promotion, attendance on courses and suitability for employment.

The investigator suggested that an officer's position on the list would come under the definition of personal information in the *Privacy Act* which covers "any identifying number, symbol or other particular assigned to the individual".

The discussion see-sawed back and forth over several months. The investigator examined the promotion list to confirm that there was no numerical ranking, and determined that the page number — as the complainant maintained — was wrong. The error was corrected.

The Commissioner alerted the deputy minister to a preliminary finding that the complaint was justified because the list contained two items of information about the individual: that he is on the list, and his standing relative to others on the list. The Commissioner wrote: "...to refuse to disclose X's exact position on the list, merely because no number corresponding to that position appears on the list, effectively deprives X of one piece of his personal information contained on the list."

In September 1987 the Chief of the Defence Staff advised the Commissioner that, upon review, DND changed its policy on releasing a merit list position.

"Commencing with the 1987 merit boards, a position number will be added to the merit lists..." the Chief wrote. Beginning January 1, 1988, applicants will be given both their merit list standing and the total number of members considered by the board.

The letter included where the complainant stood on the 1987 promotion list.

UI to Limit Pension Queries

An Ontario man complained about the pension coverage questions he was asked to answer when he applied for unemployment insurance.

The document, called a "fact-finding questionnaire", asked the unemployment insurance applicant to describe his pension coverage, including the source, the type of payments and the payment schedule, whether pension payments had been converted to RRSPs, annuities "or any other type of savings or investment plan, account or program".

During the investigation, Employment and Immigration Canada's (EIC) staff said that a 1986 amendment to the *Unemployment Insurance Act* provided that claimants receiving pension benefits could have their UI benefits reduced. The questionnaire, they said, was to determine whether applicants were receiving pension funds. Thus, the information related to administering the unemployment insurance plan and, as such, was permitted under the *Privacy Act*.

The Commissioner agreed that this rationale would be true if the questions concerned the period when the applicant was unemployed. However, the questions were completely open-ended, leaving applicants feeling obliged to reveal details about pension coverage that may be years away from producing benefits. He told EIC the collection of this information seemed premature.

EIC agreed to add a footnote to the questionnaire, limiting the pension queries to the period of unemployment and said that a new national questionnaire, without footnote, was to be introduced.

After three months of discussions, EIC agreed to add the limiting statement to the new form. Unfortunately, the man whose complaint changed the policy moved, left no forwarding address and never heard the good news.

Medical Information — Canada Post

A postal employee complained that Canada Post had improperly disclosed information to his physician, had obtained personal information from his physician without his permission, and had used a medical report filed during a compensation hearing to prevent his return to work.

Origin of Completed Complaints by Province and Territory

Newfoundland	3
Prince Edward Island	2
Nova Scotia	13
New Brunswick	8
Quebec	219
National Capital Region Quebec	4
National Capital Region Ontario	107
Ontario	131
Manitoba	30
Saskatchewan	25
Alberta	57
British Columbia	53
Northwest Territories	4
Yukon	1
Outside Canada	4
TOTAL	661

Investigation confirmed that Canada Post had referred to the medical report they had received at the hearing when they refused his attempt to return to work. The information bank containing the report ("Occupational Health and Safety"), is described as containing information used "to establish conditions under which employees...with identified illnesses or disabilities are able to continue to work...". The Commissioner concluded that Canada Post had not misused this information.

During the investigation, it was learned that Canada Post had obtained information from the employee's physician without his consent, but the request was made prior to the implementation of the *Privacy Act*, and therefore did not contravene the Act. It was also determined that a copy of correspondence containing personal information from Canada Post to the complainant had been sent improperly to the complainant's physician. Canada Post will ensure that this does not recur.

Leave and Medical Diagnosis

Two complaints were received about departments requiring detailed medical information from employees absent on sick leave.

In one case, cited earlier to illustrate the need for privacy in the workplace, a Department of Communications (DOC) supervisor had rejected both the standard sick leave declaration

and a medical certificate, insisting on knowing the medical details which kept an employee away from work. The employee had a history of lengthy absences for health reasons.

While refusing to supply the information, the employee agreed to be examined by a Department of Health and Welfare doctor. The government doctor found the employee in good health, but was unable to determine what condition had prevented the man working because he was refused permission to speak to the man's personal doctor.

When DOC refused to pay for sick leave, the individual complained that requiring him to provide the diagnosis violated the *Privacy Act*.

DOC argued that it had the right to the information because of the number of health-related absences, the concern for both the employee's own and other employees' health and safety, and the implications for long-term disability cases. DOC also cited the employee's collective agreement and a grievance adjudication decision to support this argument.

The Commissioner agreed that the employer legitimately required evidence that an employee was medically unable to work before being granted paid sick leave. He also agreed that employers could refer an employee to a doctor of their choice to confirm fitness for work but, he said, "in my view it is not necessary for the employer to know the nature of the illness".

As a result, the department changed its policy, saying that in future it would not request details of employees' medical conditions. Fitness for work would be verified, if necessary, through a Health and Welfare doctor. No details on an employee's condition would be passed back to the department. DOC subsequently paid the complainant's sick leave.

Diagnosis removed from file

A Quebec City woman complained that, without permission, her employer (Employment and Immigration Canada) asked her family doctor for medical details after she submitted a certificate of disability. The details then became part of her personnel file.

EIC explained that managers often reach employees' doctors in order to determine what work can be performed by an employee with health problems, but not to get details of their condition. This practice was said to be faster than waiting for employees to obtain the information themselves and, EIC said, the complainant knew they would call her doctor whether or not she agreed.

The Commissioner concluded that the onus is on the department to collect information directly from an employee or to get the employee's permission before reaching the personal physician. Even then, the only information an employer needs is the expected duration of the condition and any restrictions it could place on the employee when returning to work.

After months of negotiations, EIC agreed to remove the medical diagnosis from the file.

The Commissioner believes that the problem exists in other departments and urged Treasury Board to issue government-wide instructions consistent with the *Privacy Act*.

No Information to Police

An inmate complained that Correctional Service Canada had misused his personal information by giving his "penitentiary file" to a city police force. He alleged that the police then passed it to a Crown Attorney and a Crown psychiatrist before giving it to his lawyer.

The Privacy Commissioner's investigator could find no evidence that personal files had been passed around. The complainant produced a page copied from a court transcript in which the Crown psychiatrist cited tests and files on which he based his assessment of the inmate. One of the items was described as "police reports and penitentiary service files".

While the Crown psychiatrist had seen files, this appeared to be a consistent use of the information since the hearing was to determine whether the inmate was a dangerous offender. There was nothing to prove that the information had been passed to the police.

The Commissioner found no evidence that personal information had been misused or improperly disclosed and dismissed the complaint.

Union and Security Checks

Three public service unions complained about Revenue Canada's implementation of the government's security and reliability checks. The unions said their memberships considered the collection of criminal records, financial transactions and fingerprints "illegal". They asked the Commissioner to investigate, in particular, Revenue Canada, Taxation's personnel screening policy.

Following the theft of tax microfiche (see page 10 — 1986-87 Annual Report), the minister of national revenue ordered immediate implementation in the tax department of the new government-wide security policy. The policy's basic reliability checks include verifying education and professional qualifications, employment data, performance and character assessments and a name check of the criminal records bank. The more rigorous "enhanced" security check also requires fingerprinting and a credit check.

The Commissioner found that Treasury Board had the right (indeed, the duty) to assess its employees' trustworthiness and loyalty to prevent the abuse or disclosure of taxpayers' personal information.

However, he continues to be concerned that third parties may apply to see individual security files under the *Access to Information Act*, given the limited protection for public servants' personal information. Following discussions, prompted by a similar complaint about the government's conflict-of-interest code, Treasury Board promised to ask Parliament to amend the *Privacy Act* to limit availability of public servants' personal information to name, salary-range, title, position duties and business address.

Treasury Board accepted the Commissioner's recommendation that deputy ministers be given discretion to decide whether fingerprinting and credit checks are reasonable and for which employees. The policy has been changed.

Tax Auditor Obtains Meeting Notes

A Revenue Canada tax auditor complained to the Commissioner when the department withheld material from a letter which accused him of a conflict-of-interest. He considered the edited pages to be "meaningless".

In a letter to the revenue minister, a man alleged that the tax auditor (his wife's first husband) was using his position to advantage in a legal dispute with the wife. The letter also mentioned that the auditor had recently caught one of the writer's fellow employees for unreported earnings, implying that the incidents were connected. The department's internal inquiries revealed no wrongdoing on the auditor's part.

An investigator persuaded the department to release more of the original letter. However, much of the exempted material was personal information about someone else. The exemptions were valid.

In the meantime, the complainant again wrote to the minister concerned that an internal inquiry would produce more documents than he had received. In a meeting with the departmental privacy coordinator, the complainant asked for any personal notes taken by managers during interviews for the internal conflict investigation as well as the investigation file. He also asked to review the tax file of the employee caught not reporting earnings.

The investigator negotiated the release of some meeting notes and a record of a phone conversation with the person who alleged the conflict-of-interest. However, the investigator confirmed that there were no other personal notes, no investigation file, and no references to the complainant in either the minister's letter responding to the original complaint, or in the fellow employee's tax file.

The Commissioner upheld the complaint because the department had not provided all the material in response to the first request. The applicant now has the material to which he was entitled

Accepts Correction, Refuses Another

A Manitoba man complained that the RCMP had denied his request to correct factual information in a file obtained as a result of a *Privacy Act* request.

The investigator found that the RCMP had accepted one correction but denied the second because an RCMP officer had reported a different version of the incident. The complainant's comments were noted on the file.

In his letter to the complainant, the Commissioner explained that there is no clear method of resolving disputes in which there are different perceptions of an incident. Since the complainant's version is now on the file, the Commissioner considered the RCMP's response was reasonable.

Permission Prompts File Release

An Employment and Immigration Canada (EIC) employee, accused of conflict-of-interest in hiring, alleged that EIC had not provided all the material he had requested, had improperly collected information during the inquiry, and had delayed responding to his request.

EIC had not responded to the complainant's memo asking for copies of documents from the inquiry. However, he had not used the proper form, had not cited the *Privacy Act* and had not sent the request to the privacy office. Thus, it was not technically a formal privacy request and the department was not obliged to respond.

Once EIC received a formal request, it extended the deadline to the full 60 days so as not to "unreasonably interfere with the operations of the government institution". Since staff had to process a large volume of material, the extension was reasonable.

When he received the material, the applicant found information had been withheld because it concerned another individual (much of it about the person hired). He had also expected to receive his supervisor's notes from their meeting, material from the labour relations unit, interviews with staff members about hiring and relevant correspondence with the minister. When he found none of this material he complained to the Commissioner.

The investigator found the supervisor's handwritten notes were destroyed once his report was written. There was no material in the labour

relations unit and notes from interviews with others had been properly exempted. The minister's correspondence, originally overlooked, was released. After the complainant obtained the third party's permission, EIC also released that information.

The Commissioner dismissed the complaint that EIC had collected the information improperly. Although EIC had made inquiries outside the department, including interviews with neighbours, existing case law gives employers considerable scope in ensuring employees are not involved in misconduct.

Completed Complaints by Department, Type, and Result

Department	Complaint Type	Number (Total)	Justified (Total)	Dismissed (Total)	Abandoned (Total)
Agriculture Canada	Access	6	—	6	—
Bank of Canada	Access	1	—	1	—
Canadian Commercial Corp.	Access	1	1	—	—
Canadian Human Rights Com.	Access	4	1	3	—
	Misuse	1 (5)	— (1)	1 (4)	—
Canadian Labour Rel. Board	Access	6	—	6	—
Canada Post	Access	23	4	19	—
	Misuse	2	1	1	—
	Correction	1	—	1	—
	Delay	1	—	1	—
	Col/Ret/Di	3 (30)	— (5)	3 (25)	—
Canada Ports Corporation	Delay	4	4	—	—
Correctional Service Cda.	Access	104	12	88	4
	Misuse	7	—	7	—
	Correction	6	1	5	—
	Delay	39	33	5	1
	Language	9	1	8	—
	Col/Ret/Di	5 (170)	— (47)	5 (118)	— (5)

Completed Complaints by Department, Type, and Result

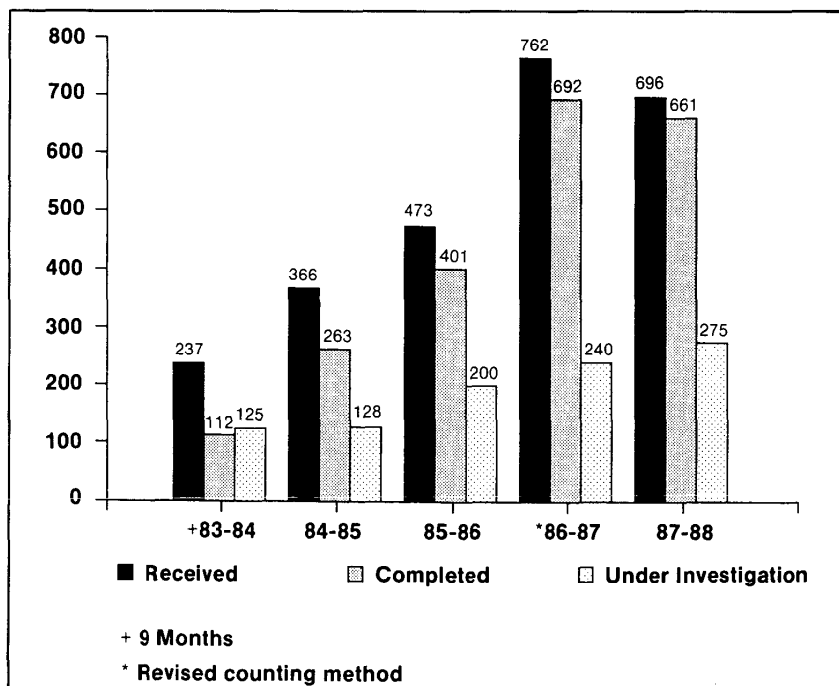
Department	Complaint Type	Number (Total)	Justified (Total)	Dismissed (Total)	Abandoned (Total)
Canadian Security Intelligence Service	Access Delay	20 3 (23)	1 — (1)	19 3 (22)	— —
Canadian Transport Com.	Access	3	—	3	—
Communications	Access	1	1	—	—
External Affairs	Access Misuse	4 1 (5)	— 1	3 —	1 —
Environment Canada	Access	2	—	2	—
Export Development Corp.	Access	1	—	1	—
Employment and Immigration Canada	Access Misuse Delay Col/Ret/Di	62 4 25 5 (96)	11 — 20 1 (32)	49 4 5 3 (61)	2 — — 1 (3)
Health & Welfare Canada	Access Misuse Delay	9 3 9 (21)	3 1 4 (8)	6 1 5 (12)	— 1 — (1)
Immigration Appeal Board	Access Misuse	1 1 (2)	1 —	— 1	— —
Indian & Northern Affairs	Access Misuse	1 1 (2)	— 1	1 —	— —
Justice	Access Delay	9 2 (11)	1 — (1)	8 2 (10)	— —
Labour Canada	Access	8	1	7	—
National Defence	Access Misuse Delay Col/Ret/Di	6 4 32 1 (43)	2 — 22 — (24)	4 4 10 1 (19)	— — — —
National Archives Canada	Access Correction	11 2 (13)	4 — (4)	7 2 (9)	— —
National Energy Board	Access	1	—	1	—
National Parole Board	Access Correction Delay	11 1 3 (15)	— — —	9 1 3 (13)	2 — — (2)

Department	Complaint Type	Number (Total)	Justified (Total)	Dismissed (Total)	Abandoned (Total)
Privy Council Office	Access	10	—	10	—
	Misuse	1 (11)	—	1 (11)	—
Public Service Commission	Access	20	—	20	—
	Correction	1 (21)	—	1 (21)	—
Public Works	Access	2	1	1	—
	Misuse	2 (4)	1 (2)	1 (2)	—
Revenue Canada Customs and Excise	Access	5	2	3	—
	Misuse	2	—	1	1
	Correction	1	—	1	—
	Delay	2 (10)	1 (3)	1 (6)	— (1)
Revenue Canada Taxation	Access	12	2	10	—
	Misuse	1	1	—	—
	Delay	3	—	3	—
	Col/Ret/Di	2 (18)	— (3)	2 (15)	—
RCMP	Access	71	6	64	1
	Misuse	7	—	7	—
	Correction	7	1	6	—
	Delay	13	5	8	—
	Language	1	—	1	—
	Col/Ret/Di	1 (100)	— (12)	1 (87)	— (1)
Statistics Canada	Delay	1	—	1	—
	Language	1 (2)	—	1 (2)	—
Solicitor General Canada	Access	4	—	4	—
	Correction	1 (5)	—	1 (5)	—
Supply and Services Canada	Access	1	—	1	—
Treasury Board	Access	1	—	1	—
	Misuse	2 (3)	—	2 (3)	—
Transport Canada	Access	3	—	3	—
	Correction	2	—	2	—
	Delay	3 (8)	2 (2)	1 (5)	—
Veterans Affairs Canada	Delay	8	—	8	—
TOTALS		661	155	492	14

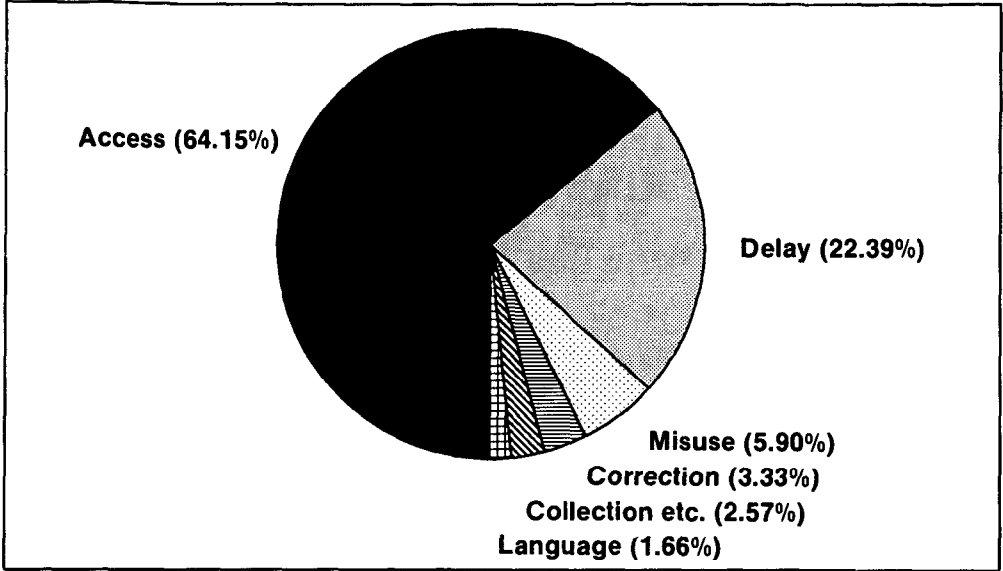
Grounds of Complaints and Investigation Results

Grounds	Abandoned	Justified	Dismissed	Total
Misuse	2	6	31	39
Access	10	54	360	424
Correction	—	2	20	22
Language	—	1	10	11
Index	—	—	—	—
Collection/ retention/disposal	1	1	15	17
Delay	1	91	56	148
TOTALS	14	155	492	661

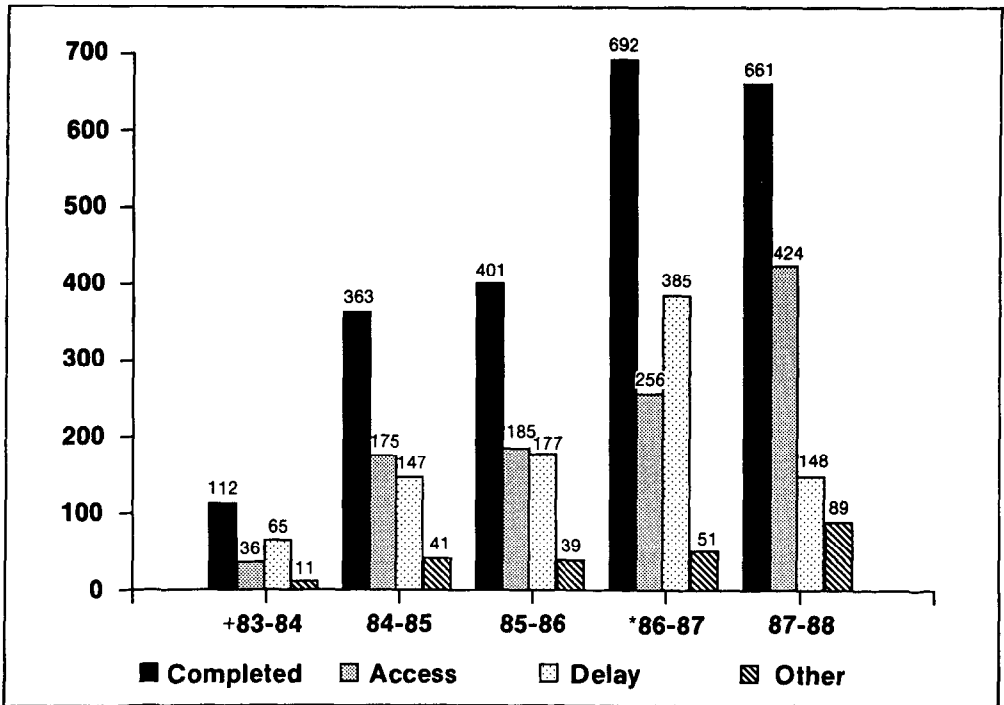
Completed complaints 1983-88



Caseload by grounds 1987-88



Completed complaints and grounds 1983-88



Disputed Status Hinders Access

A husband and wife complained that an immigration consultant hired to represent them had been refused access to their immigration files. EIC maintained that the couple did not meet the *Privacy Act* requirement that applicants be Canadian citizens or permanent residents.

Both had obtained landed immigrant status early in 1985. However, when they returned from a 1986 vacation abroad, immigration officers believed the couple had abandoned their status in Canada and so told them. The couple argued that neither had been outside the country longer than the maximum 183 days allowed and no immigration adjudicator had rescinded their status.

The privacy investigator discussed their application with EIC staff who offered to process the request under the *Access to Information Act* because the immigration consultant could apply for their information with their consent.

The consultant refused, believing that would constitute an admission that his clients were not permanent residents. While discussions continued with EIC, the immigration problem was resolved and the couple withdrew their complaint.

Contractor's Employees Protected

An Ottawa man told the Commissioner that External Affairs gave him not only the name of an agency providing the department with temporary help, but also the names of the individuals performing services.

He complained that this breached the *Privacy Act* because only the names of those signing service contracts with the government may be released because they are not "personal information". In this case the contract was with the agency and the complainant believed the individual names should be protected.

The complainant told the Commissioner that departments were not treating these applications consistently, citing several that give out only the company's name and withhold the individual employees' names. He said that the conflicting practices needed to be resolved and that the Information and Privacy Commissioners ought to provide guidance.

From his investigation the Privacy Commissioner concluded that the complaint was justified. Employees of any company providing services to the federal government on contract are not themselves government employees and, therefore, have a right to protection of their personal information.

The same applicant then asked External Affairs what security clearance was required for those individuals' jobs. The department refused to respond because the individuals had already been identified. The applicant complained to the Information Commissioner that access was denied and this case is now before the Federal Court.

USING THE PRIVACY ACT

According to the latest Treasury Board statistics (December 31, 1987), the number of applications under the *Privacy Act* to all departments continues to climb. There were 12,013 applications during the October 1 to December 31, 1987, quarter alone — an all-time high. The total applications since July 1, 1983, when the *Privacy Act* took effect, has reached 159,835.

Processing Time

Despite the mounting number of applications, government departments appear to be more than keeping pace.

Between 1983 and 1986, only 53 per cent of the applications were processed within the 30 days allowed by the Act, 16 per cent were completed from 31 to 60 days, and 31 per cent took longer — technically a denial of access. In this fiscal year by comparison 65 per cent of the applications were handled in 30 days; 22 per cent in 60 days, and 13 per cent in more than 60 days. This steady improvement (the result of departments' increased experience, more resources and plain hard work), is another reason delay complaints are dropping.

Getting It All

Just over 64 per cent of applicants receive everything they asked for (and occasionally more). Almost 22 per cent of applicants are denied some of the information primarily because it concerns another person (47 per cent), it was supplied by a province

which considers it confidential (21 per cent) or it concerns law enforcement and investigations — including RCMP information when acting as provincial police (17 per cent).

Six per cent of applicants receive nothing: one per cent either because the information is already publicly available or it is confidential Cabinet material; for the remaining five per cent information simply does not exist. For eight per cent of applicants, there is insufficient information provided to process the request, processing has proved impossible, the request has to be transferred or the request is abandoned.

These breakdowns have not changed significantly since the *Privacy Act* took effect.

Who Gets Asked

National Defence remains far ahead of all other departments in the number of applications received — it had a somewhat remarkable total of almost 73,000 by the end of 1987 — to maintain the stranglehold it has had on first place since the program began. This results largely from DND requiring its own employees to make formal applications to see their personnel files.

The next four departments in order of applications are Correctional Service Canada, 27,899; National Archives, 25,964; RCMP, 11,111; and Employment and Immigration Canada, 9,719.

Compliance Branch

"The Privacy Commissioner may, from time to time at the discretion of the Commissioner, carry out investigations...of personal information under the control of government institutions to ensure compliance..."

Section 37, Privacy Act

This year marked the first time the auditors of the compliance branch planned and completed a series of audits using the audit risk model developed last year. As the series of lost document incidents described in the 1986-87 report abated, staff was able to concentrate on auditing the compliance of four departments which management selected from those identified as "high risk".

The four, Transport Canada (TC), Correctional Service of Canada (CSC), Environment Canada (EC) and Agriculture Canada (AC), were the office's first exposure to large departments with many regional offices and full ranges of personal information banks. Previously, experience was confined to a test audit of Fisheries and Oceans and to the exempt banks of eight institutions.

The exempt bank audits proved a too-optimistic indicator of resources needed for thorough investigations. By their nature, files in exempt banks are particularly sensitive and are more uniform or homogeneous than those in other banks. They are collected according to exact parameters and are controlled centrally (though not necessarily held in a central location). There are few surprises.

This is not true of other personal information holdings. The result was a revised estimate of the depth and time required for investigations, and the development of new methodologies to handle what originally appeared to be routine audits.

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

The auditors examine:

- * the department's collection, use, disclosure, retention, disposal and security of personal information;
- * the adequacy of internal policies and the department's compliance with central agency policy and guidelines on personal information;
- * the accuracy and completeness of the department's listing 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 debrief the managers and discuss any areas of non-compliance. The department receives a draft report for discussion, then a final edition. In line with accepted audit practice, the reports address only those areas requiring correction.

The findings

Considering the differences in the four audited departments, the findings were surprisingly similar.

For example:

- * apart from those in the privacy sections, few employees were aware of the impact of the *Privacy Act* on their day-to-day handling of employee or client personal information;
- * with the exception of CSC, the physical security of personal information was often inadequate;
- * some personal information holdings had not been identified and described in the Index;
- * some information bank listings did not describe the "consistent uses" which the department routinely made of the information.

Some departments' personal information policies were found in conflict with the *Privacy Act*. Most are being remedied.

The proliferation of working copies of personnel files was another frequent observation. Although the existence of multiple copies is not addressed specifically in the *Privacy Act*, departments are required to review all

copies when responding to an access request and to insure that each copy complies with the Act. The growing use of personal computers offers a new challenge in meeting this responsibility.

One final observation: each department gave auditors their complete cooperation. Most staff found the investigations interesting and treated them as an opportunity to learn more about the *Privacy Act*.

Summaries of the individual departments' reports follow.

THE AUDITS

Environment Canada

Environment Canada's three principal components, Atmospheric Environment Services (the weather office), Conservation and Protection Service and the Parks program, are spread across the country. The department collects a limited amount of personal information about the general public and what it does hold tends not to be sensitive. For example, the department has information banks containing permits issued under the *Migratory Birds Convention Act* and the *Ocean Dumping Control Act*, duck hunting and fishing licenses issued and surveys of national park visitors. The greatest part of Environment Canada's personal information holdings is that of its own employees.

The audit team visited EC offices in Sackville, New Brunswick, Dartmouth, Nova Scotia, Toronto, Ontario, Calgary, Alberta and national headquarters in Hull, Quebec.

Investigators found that:

- * most Environment Canada employees knew little about the *Privacy Act*, its application and implications for their work. Internal directives were often inadequate, inaccurate and unknown;
- * disposal schedules were not being applied, leading to information either being kept longer than necessary or less than the two years required by the Act;
- * some personnel files were stored in insecure locations;
- * personnel files about individuals on personal service contracts, volunteers, and unsolicited job applications were not described in the Personal Information Index;
- * individual managers throughout the department maintain duplicate or private file systems containing personal information derived largely from personnel records, increasing the risk of unauthorized disclosure, alteration of information and denial of access;
- * the *Ocean Dumping Control Act* bank contains no personal information—the files concern companies, corporations, and other federal government departments. (This bank can be removed from the Personal Information Index.)

Transport Canada

Transport Canada is one of the largest federal government departments, employing almost 22,000 persons to develop and operate a safe and efficient national transportation system. The department comprises five groups; Airports Authority, Aviation, Marine, Surface, and Policy and Coordination. The audit examined Airports Authority and Aviation and Marine groups at national headquarters and in selected regional offices.

The investigation found personal information generally well protected at Transport Canada. Employees are vigilant in preventing improper disclosure; a records management information system identified and recorded most personal information. The weaknesses found are grouped here into descriptions of personal information banks in the Personal Information Index, protection of personal information, retention and disposal, security, collection and informed use, and access.

Employee Assistance Files: One group of high risk files was identified during preparation for the investigation. These are Employee Assistance Program (EAP) files containing highly sensitive personal details. (The EAP program provides counselling and support for federal employees coping with health or behavioural problems such as alcohol abuse.) Access to these files is limited to counselling staff.

The department was understandably concerned about files being seen by outsiders — even a privacy investigator. Any unauthorized release of the information could cause irreparable harm to the individual. The office arranged with Transport Canada to have a senior privacy staff member examine a random selection of files to ensure they were properly maintained and protected. The personal identifiers were hidden.

The investigator found the files were already depersonalized, and locked in a cabinet in a locked office in a building that is inaccessible after work hours. He found no evidence of inappropriate release but made several suggestions to improve the physical security of the files.

Problems with other Transport Canada files follow.

Personal Information Index descriptions: Investigation revealed a number of defective listings including:

- * the Enforcement bank (P-PU-015) contains files on enforcement activities against those holding a valid aviation document, rather than only those “not in possession” of the document;
- * the Aviation Licensing Database (P-PU-005) does not indicate that its contents may be shared with the Canadian Aviation Safety Board, nor that the Medical “C” file is part of the database;

- * the Vehicle Accident bank (P-SE-908), described as an employee bank, contains significant amounts of information on members of the public who have filed claims about accidents while using Transport facilities.

Protection of personal information:

The investigators found that some personal information is not adequately protected from disclosure to unauthorized individuals. For example, information about aviation licence holders is available over the telephone. Lists of several employees' payroll deductions were found on individual personnel files and sensitive employee information (which belongs on a “history” file) was found on rating files.

In one regional office privacy staff found an unofficial 26-volume file containing often sensitive information on all employees, arranged in alphabetical order by name. Managers could examine the information of any employee, not just those he or she supervised.

Security was lax at some locations. Investigators found: computer disks available at night; an open concept record room with files stored on open shelves directly in front of the elevator; cleaning staff with access to licensing files, and sensitive waste thrown in regular garbage.

Retention and disposal of files: The audit team found that one information bank had no disposal schedule; two others needed review in order to send old files to National Archives for destruction or historical storage. Temporary regional files in a bank containing

accident reports are destroyed before the minimum two-year period. Although some of the material duplicates reports sent to headquarters, the files include the accident investigators' notes which should be kept.

Collection of personal information and informed use: The *Privacy Act* requires government institutions to tell individuals why they collect personal information. Such an explanation should be provided on application forms. However, forms used to issue various civil aviation licences and permits do not contain any statement of purpose. There is no indication that applicants are ever told.

Investigators found collection of what appeared to be excessive information. For example, pilots' medical examination reports ask for education data and several others require the applicants' place of birth.

Access to personal information: In one region applicants to the Aviation Licensing Database were not being given access to their medical file held in the bank unless they so specified.

Agriculture Canada

Agriculture Canada has 13,000 employees in 11 branches administering 40 different acts. Programs range from maintaining the productivity of Canada's agri-food sector to the protection of livestock and plant-life, including Canada's forests.

The audit took place in Moncton, New Brunswick, Calgary, Alberta, and Ottawa-Hull headquarters.

Protection of personal information: Investigators found a number of working personnel files in regional offices containing sensitive personal details. Other files contained unnecessary information about third parties. In several locations, personal information was unlocked in open offices. In one case, the open files concerned investigations of alleged wrongdoings.

Working personnel files are common in regional offices where they are kept for routine management purposes. Working files do not necessarily contravene the *Privacy Act* providing that they are exact duplicates of official files; their use is restricted to those with a need to know, and they are reviewed when an employee submits a privacy request.

Improper disclosure: Agriculture Canada signed a 1985 Memorandum of Agreement with Canada Customs and the RCMP to provide investigation reports to an automated RCMP database. These three agencies, police forces and the United States Customs Service share the information.

Investigators considered that, with few exceptions, the disclosures were unrelated to the original collection purpose and suggested the department stop releasing information unless it conforms to the *Privacy Act*. The department should respond only to written requests from investigative bodies such as the RCMP, keeping records of all disclosures for the Privacy Commissioner's examination.

Awareness of the Privacy Act: Few employees were familiar with the Act. The result can be improper handling

of personal information, for example, keeping indefinitely conflict-of-interest reports about former employees. The department agreed to delete old information on one system and to modify its new system to include file destruction dates. The difficulty with the agreement with Customs and the RCMP, described above, stemmed from lack of knowledge of the Act.

Correctional Service Canada

Correctional Service Canada consists of the Penitentiary Service, responsible for inmate custody and care, and National Parole Service which supervises those freed on parole or mandatory supervision.

Given the demands of their jobs, employees consider security, confidentiality, and protection of personal information a routine part of their work.

However, there were areas where improvements could be made.

Personal Information Index descriptions: Investigators found inaccurate or incomplete bank descriptions in the Index or, in some cases, the purpose for the collection was unclear. There were files containing information services inquiries, ministerial inquiries, administrative inquiries, inmate transfer files and offender administrative case files — all of which are collections of personal information but not described in the Index.

In addition, there were 12 series of files containing personal information not listed in the Index, thus effectively removing the information from access and leaving the public unaware of the extent of the collection or its purpose. It can also mean these files are not held for the minimum two years nor reviewed for regular destruction.

Protection of personal information:

The investigators found that employees in the Ontario and Quebec regions can only review their personnel file through a request to their supervisor and in the supervisor's presence. Some Ontario and Quebec offices lack policies for secure disposal of legible computer and typewriter ribbons.

At national headquarters, sensitive pardon records were found on open shelving in a basement storage area. They were available to anyone with access to the room.

Access rights: Inmates requesting access to the Psychology bank (CPS/P-PU-070) in the Ontario Region are not receiving their raw test data. Psychology staff at the Ontario Regional Psychiatry Centre and Joyceville Institution routinely withhold the scores before sending the files to headquarters, without the knowledge of the department's privacy coordinator. Applicants are not told of the omission, nor of their right to complain to the Privacy Commissioner.

Use and Disclosure Code: The problems the Commissioner's office has encountered with CSC's use and disclosure code are discussed in detail on page 16.

Notifying the Commissioner

One of the tenets of the *Privacy Act* is its protection against release of individuals' personal information. But as with most rules, there are exceptions. For example, personal data may be released "in the public interest", to comply with another act of Parliament or a warrant or subpoena, to specified investigative agencies, and to the National Archives for storage.

But government departments must notify the Privacy Commissioner when they decide to so release personal information or for any new use "consistent" with the purpose for which it was originally collected. This notice gives the Commissioner an opportunity to object to those releases he considers improper and to advise the individuals if he considers it necessary.

The Commissioner received the following such notifications this year:

Statistics Canada: confirmation of several persons' birthplaces or ages to relatives to apply for pension benefits or to confirm citizenship for Canadian or U.S. passports.

— refused release of information about individuals, born in East bloc countries, who died in Canada intestate.

Indian Affairs and Northern Development: confirmation of deceased man's Indian status to help daughter obtain Indian status.

Justice: release of lawyer's opinion concerning Canadian government funding of the Allan Memorial Institute. The department released the opinion (which contained personal information about three men), after obtaining the subjects' consent;

— release of two letters to a law society for background in a complaint of misconduct against a departmental lawyer.

National Defence: release of treating physician's affidavit to wife of man in coma, to permit her to manage family's financial affairs.

Royal Canadian Mounted Police: release of RCMP report on death of serving member to his widow to pursue pension claim.

Veterans' Affairs: release of deceased veteran's medical records to his daughter's doctor to investigate possibility of inherited disease.

— release of deceased's medical records to son to help treatment of suspected hereditary conditions.

National Parole Board: release of parole board decision and reasons for decision to an MP querying allegations of political interference in the decision.

Solicitor General: release to House of Commons of report, prompted by McDonald Commission findings, recommending how Canada should fulfil outstanding obligations to Warren Hart.

Secretary of State: release of woman's Canadian citizenship data so Japanese authorities could enforce a Canadian child custody order.

— confirmation of dates on which 13 individuals granted Canadian citizenship to determine eligibility for Order of Canada. Three nominees' information could not be found.

Spreading the Word

The Privacy Commissioner and his staff continued to stump the country for privacy. The Commissioner spoke to, among others, Canadian Club audiences in Moose Jaw, Saskatchewan, and London, Ontario. He discussed privacy auditing with the Institute of Internal Auditors; privacy codes with the Canadian Direct Marketing Association; privacy and human rights with the Canadian Law and Society Conference; monitoring and surveillance at the annual conference of international data protectors in Quebec City and the implications of privacy legislation on information management at the national records management conference in Melbourne, Australia.

Since privacy is particularly relevant to statistical collection (statisticians rely heavily on manipulation of administrative records), the Commissioner addressed Statistics Canada's management conference as well as international statisticians in both Ottawa and Stockholm. In addition, the Commissioner was interviewed by the media and he participated in meetings with newspaper editorial boards.

His staff briefed candidates on the senior management courses at the federal government's executive training centre, and spoke to post secondary classes, federal employee seminars, and the annual meetings of the Canadian Information Processing Society and the Canadian Society for Information Science.

Inquiries

The year's 1,248 inquiries ranged from whether a jewellery store owner could require employees to inspect one another's handbags and parcels before leaving work, to a call from a utility company wondering whether it could use Social Insurance Numbers to locate customers who moved, leaving unpaid accounts. The jewellery store is not under the jurisdiction of the *Privacy Act* and the utility company can use SINS, but having clients' numbers won't give it access to the federal government's data banks to find their new addresses.

Just over 14 per cent of the inquiries were applications for personal files which were redirected to the departments holding the information. These particular inquiries are reminders that many individuals continue to believe that Ottawa has one large file about them — a perception the Commissioner is happy to dispel.

Almost 50 per cent of callers ask what the Act is, how they can see their personal information, or want some clarification about the law.

Nearly six per cent called about the potential invasion of privacy from such federal programs as Statistics Canada surveys and the government's new conflict of interest and security clearance policies for its employees.

About ten per cent of the calls, while related to privacy, were not in the federal jurisdiction. The Commissioner's office is now able to refer such Ontario callers to their new

Information and Privacy Commissioner, although he too is unable to deal with complaints involving private businesses.

Just over seven per cent of the calls were unrelated, including requests for leads to track down natural parents and a call wondering why a local housing authority wanted an applicant's tax return.

Queries and complaints about Social Insurance Number incidents increased to more than 15 per cent of the total inquiries, partly reflecting the Commissioner's comments in his last annual report, and partly because of the federal government's promise to tighten its own collection and use of the numbers. Callers objected to such things as having to produce the number to vote in a municipal election, join a seniors' travel club and, in one novel instance, to having it programmed into their employer's photocopier to restrict their access to the machine as well as to monitor use and cost.

The office receptionist referred an astonishing 5,756 calls to either the federal government's central switchboard or, more recently, Reference Canada. The majority of these completely unrelated calls are prompted by the national toll-free number listed under "Information Commissioner" (with whom the Privacy Commissioner shares offices) in the blue pages of municipal telephone directories. Callers believe the office is the new Information Canada.

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 approved by Parliament for the 1987-88 fiscal year were \$3,922,000 and 58 person years, an increase of approximately \$3,000 over the 1986-87 expenditures. Personnel costs of \$2,970,000 and professional and special services expenditures of \$512,000 accounted for more than 89 per cent of expenditures. The remaining \$440,000 covered all other expenses.

Personnel

Staff increased by five during the fiscal year, to a total of 58 on March 31, 1988. There were 21 staffing actions during the year, including one appointment to a senior management position: Executive Director, Office of the Privacy Commissioner.

Administration

During this past year, space was acquired on the third and fourth floors, Tower B, Place de Ville. This space is presently being fitted-up and will be ready for occupancy by the summer.

The following are the Offices' expenditures for the period April 1, 1987 to March 31, 1988

	Information	Privacy	Administration	Total
Salaries	\$ 968,062	\$1,121,001	\$ 483,768	\$2,572,831
Employee Benefit plan contributions	159,200	149,640	88,160	397,000
Transportation and Communications	25,028	59,518	98,698	183,244
Information	47,258	50,028	558	97,844
Professional and special services	412,534	72,754	26,411	511,699
Rentals	76	727	11,172	11,975
Purchases repair and maintenance	222	1,163	1,225	2,610
Utilities, material and supplies	4,191	11,171	27,778	43,140
Construction and equipment acquisition	32,494	33,141	16,344	81,979
All other	79	1,245	177	1,501
TOTAL	\$1,649,144	\$1,500,388	\$ 754,291	\$3,903,823

Data Processing

Computerization of the Offices has increased in most areas and as a result, staff has become more adept at using data processing equipment in their daily tasks. A larger volume of information has been processed and computer stored.

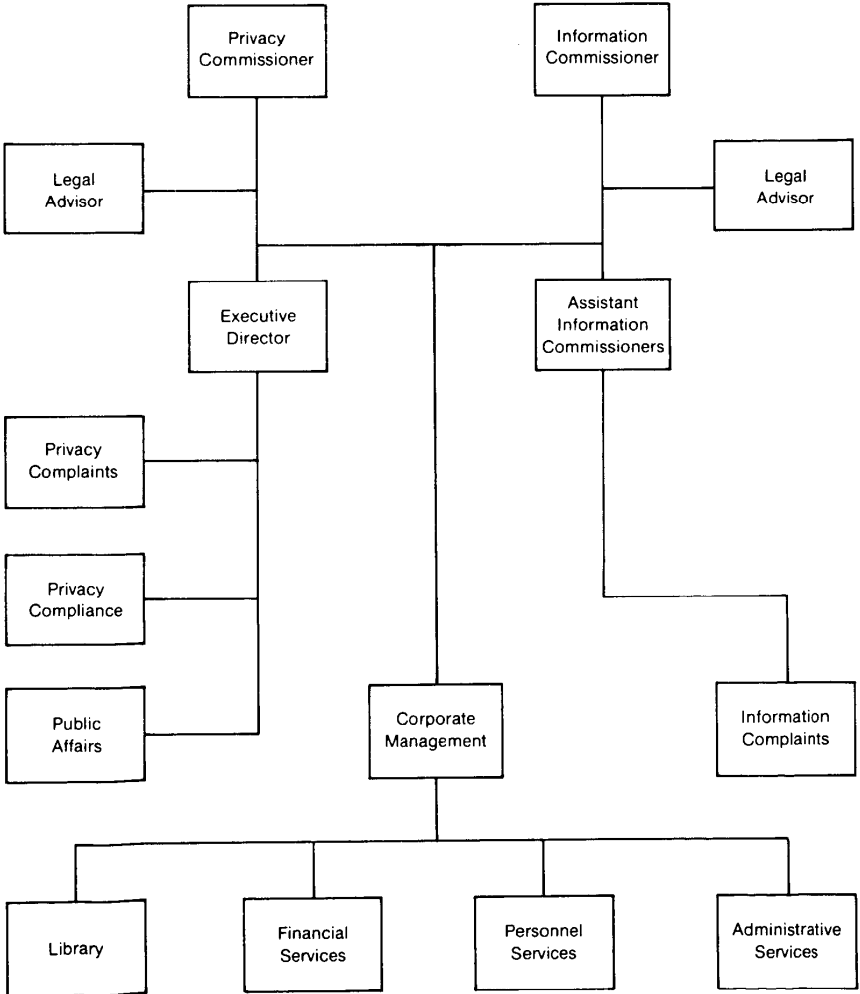
Library

The library obtains and disseminates information for both Commissioners' offices. To assist in this function, subscriptions to several automated bibliographic and full text data bases are maintained. An interlibrary loan service is also available to the users. Freedom of information, protection of privacy and the Ombudsman function are the main subject areas of the library's collection of approximately 3000 items. The public is invited to consult the library for reference and research. Last year 25 visitors were welcomed, 630 reference questions were answered and 450 items were added to our collection.

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

Canadian Unity Information Office	Freshwater Fish Marketing Corporation
The Canadian Wheat Board	Grain Transportation Agency Administrator
Communications, Department of	Great Lakes Pilotage Authority, Ltd.
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 Appeal 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 (formerly Foreign Investment Review Agency)
Energy, Mines and Resources Canada	Jacques Cartier and Champlain Bridges Incorporated
Energy Supplies Allocation Board	Justice Canada
Environment Canada	Labour Canada
Export Development Corporation	Laurentian Pilotage Authority
External Affairs Canada	Law Reform Commission of Canada
Farm Credit Corporation	Medical Research Council
Federal Business Development Bank	Merchant Seamen Compensation Board
Federal Mortgage Exchange Corporation	Metric Commission
Federal-Provincial Relations Office	National Archives 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 of Canada	

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

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