# PRIVACY COMMISSIONER

annual report

1993 • 1994

# Annual Report
# Privacy Commissioner
# 1993-94

CANADA

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

(613) 995-2410, 1-800-267-0441
Fax (613) 995-1501
TDD (613) 992-9190


Cat. No. IP 30-1/1994
ISBN 0-662-61245-0

This publication is available on audio cassette.

Privacy Commissioner of Canada

Commissaire à la protection de la vie privée du Canada

The Honourable Roméo Leblanc
The Speaker
The Senate
Ottawa

July, 1994

Dear Mr. LeBlanc:

I have the honour to submit to Parliament my annual report.

This report covers the period from April 1, 1993 to March 31, 1994.

Yours sincerely,

Bruce Phillips
Privacy Commissioner

Privacy Commissioner of Canada

Commissaire à la protection de la vie privée du Canada

The Honourable Gilbert Parent
The Speaker
The House of Commons
Ottawa

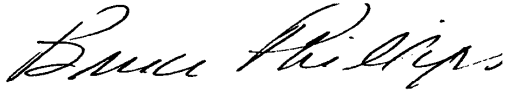
July, 1994

Dear Mr. Parent:

I have the honour to submit to Parliament my annual report.

This report covers the period from April 1, 1993 to March 31, 1994.

Yours sincerely,



Bruce Phillips
Privacy Commissioner

# Mandate

The Privacy Commissioner is a specialist ombudsman—appointed by and accountable to Parliament—who monitors the federal government's collection, use and disclosure of its clients' and employees' personal information, and its handling of individuals' requests to see their records.

The *Privacy Act* gives the Commissioner broad powers to investigate individuals' complaints, to launch his own complaint, and to audit 160-odd federal agencies' compliance with the *Act*. He also conducts research on his own behalf or at the request of the minister of justice.

# Mission

The Privacy Commissioner's mission is

- to be an effective ombudsman's office, providing thorough and timely complaint investigations to ensure Canadians enjoy the rights set out in the *Privacy Act*;
- to be an effective privacy guardian on Parliament's behalf, performing professional assessments of the quality of the government's adherence to the *Privacy Act*;
- to be Parliament's window on privacy issues, arming it with the facts needed to make informed judgements through research and communications;
- to be the primary national resource centre for research, education and information on privacy.

# Your Privacy at a Glance

## Is your personal information protected?

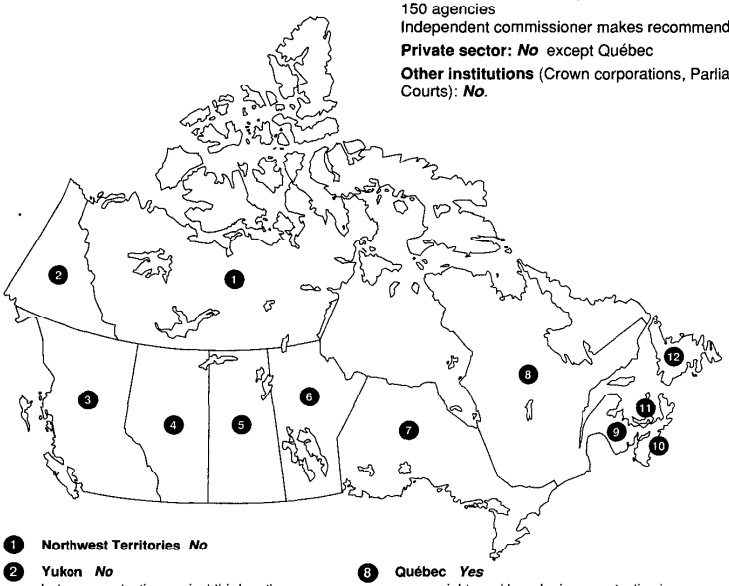
(July 1, 1994)

### Canada

**Federal government:** ***Yes***
Access rights and broad privacy protection in 150 agencies
Independent commissioner makes recommendations

**Private sector:** ***No*** except Québec

**Other institutions** (Crown corporations, Parliament, Courts): ***No***.




1. **Northwest Territories** ***No***

2. **Yukon** ***No***
   but some protection against third parties examining your personal information

3. **British Columbia** ***Yes***
   access rights and broad privacy protection in provincial and local governments. Independent commissioner makes orders.

4. **Alberta** ***No***
   Freedom of Information and Protection of Privacy Act passed but not yet in force.

5. **Saskatchewan** ***Yes***
   access rights and broad privacy protection in provincial and local governments. Independent commissioner makes recommendations.

6. **Manitoba** ***Yes***
   access rights, some privacy protection in provincial government. Provincial ombudsman makes recommendations.

7. **Ontario** ***Yes***
   access rights and broad privacy protection in provincial and local governments. Independent commissioner makes orders.

8. **Québec** ***Yes***
   access rights and broad privacy protection in provincial and local governments and the private sector. Civil Code and Québec Charter protection. Independent commissioner makes orders.

9. **New Brunswick** ***Yes***
   access rights, some privacy protection in provincial government. Provincial ombudsman makes recommendations.

10. **Nova Scotia** ***Yes***
    access rights and broad privacy protection in provincial government. Government-appointed "review officer" makes recommendations.

11. **Prince Edward Island** ***No***

12. **Newfoundland** ***Yes***
    access rights and some privacy protection in provincial government. Minister of Justice accepts complaints

*"**Access rights**" include right to examine one's own personal information and correct or annotate disputed information.*
*"**Privacy protection**" means legislated controls on an organization's collection, use and disclosure of individuals' personal information.*

# Table of Contents

# The Privacy Bottom Line

*For what shall it profit a man, if he shall gain the whole world, and lose his own soul?*

*Mark 8: 36*

Computers and fibre optics were still twenty centuries away when these words were first uttered by the shores of the Sea of Galilee. As it was two thousand years ago, so it is today. Humanity still struggles to reconcile its appetite for material advance with the preservation of spiritual and moral values which lie at the core of human existence. All that has changed is the technology.

Every important discovery since the dawn of history—from the discovery of fire to the automobile to nuclear fission—has posed the same problem of maximizing the good and minimizing the malign.

It is hard to imagine this problem being brought into sharper relief than by the issues covered in this report, because the year revealed more clearly than ever both the opportunities and the perils that progress by technology can present.

This has been the Year of the Information Highway. The phrase itself has joined the lexicon of contemporary buzzwords. Some skeptics doubtful of its claimed benefits have called it the information "hypeway". But even if oversold, the term undoubtedly implies linking up vast sources of information by computers and telecommunications, and making that information available to vastly increased numbers of people.

Doing so, we are told, will improve efficiency, competitiveness, knowledge sharing, create new jobs... the list is almost endless. Its proponents tell us that, once launched on this highway, we are headed toward a destination at once more prosperous and pleasurable.

These promises may well come to fruition. It's almost certain that some—perhaps many—will, and as a result constructing such highways has been embraced by all the important sectors of our commercial, academic and governmental life.

So much for the good news. The downside, which gets little attention from the advocates of pell-mell highway construction, is stark indeed. Unless some sensible rules of traffic management are a part of these systems, the first roadkill will be our personal privacy and dignity.

Not only have we yet to devise a privacy framework for any superhighway, we still have not come up with adequate rules governing most of the already enormous traffic in personal information. Thus, while we contemplate the multi-lane information expressways of tomorrow, we stumble about on the country lanes of today.

These are not alarmist observations. On the contrary, it is difficult to exaggerate the potential consequences of carelessness or indifference to privacy in this looming new environment. Just consider two examples:

Soon—very soon—Canadians will have available the wonders of interactive cable television. Using the television and telephone, they will be able to conduct much of their personal business from home, everything from shopping, banking, paying bills and selecting movies for home viewing. These are just a few of scores of potential uses. Most of this immense flood of information will be highly personal. Where is it going? How it will be stored? Who will have access, and who will not? What measures will ensure such information is used only for the purpose intended? All these questions await answers.

Second, consider the federal government's own Blueprint for its on-ramp to the information highway. It envisages, among others, partnerships with the private sector and with other levels of

government. What then becomes of the protections provided to Canadians by the *Privacy Act* for personal information held by the federal government?

**National privacy standards**

These two examples alone are enough to demonstrate the critical importance for placing privacy protection on the highest level of priority. Clearly, it is imperative to craft new, broadly-applicable national standards, and it must be a bedrock principle of such standards that any informational exchange involving the government of Canada carries with it the full protections of the existing federal privacy act.

Such is the main burden of this year's tour d'horizon of the privacy file—the urgent need to develop a proper regulatory framework not only for the new superhighways now a-building, but for the enormous traffic in personal information already going on in both private and public sectors.

Detailed discussion, observations and recommendations on these points are contained in following pages. They reflect the belief that enhancing privacy protection—threatened as never before by technological advance—must now be acknowledged as an urgent public necessity. The cautious, piecemeal approach of the past (and present) is already inadequate for the problems before us. How then can it possibly serve in the future?

Even now, almost all of us leave data trails in computer data bases where they can be (and are) sorted, analyzed, and compiled into extremely revealing personal profiles. Most of this information is protected by nothing more than the goodwill and conscience of the people into whose custody it falls.

The information society could just as well be characterized as the information jungle where the prevailing law is the survival of the fittest. The jungle is about to become much more lethal for our

privacy with the introduction of infinitely larger systems of collecting, manipulating and distributing our personal histories to countless others.

One recent study *Paradigm Shift: the New Promise of Information Technology*, describes the highway as an "electronic web". It's an apt description for a technology that not only builds pathways for our daily transactions—it also traps every detail. Author Don Tapscott says "computers will record whom we telephone, what movies we watch, what databases we access, what goods we buy—almost everything we do". Add governments and their enormous holdings to this mix—such things as medical, welfare, tax, immigration and police records—and it is evident how difficult it might be for any hapless individual to find a way unscathed though that jungle with his or her sense of self intact.

The past year has given us further forbidding examples of the future in the rush to more surveillance systems and multiplying proposals for personal identity cards. Doubtless such proposals have a public benefit as their primary aim, but how much farther can we travel down this road before we close altogether any right to consider ourselves as individuals, and not merely as data subjects. A decade ago, looking at our brave new computerized world, Professor David Flaherty opined that we had become a "surveillance society". Any who thought he might have overstated the case must now confess that his description unhappily has proved depressingly correct.

Others have argued that privacy must be re-defined to meet the demands of technology. This "new privacy" would focus on confidentiality, that is, ensuring the security of information from unauthorized access. Such a concept ignores altogether the most basic element of genuine privacy; the individual's ability to exercise some control over the disposition of his or her own personal information. Lost entirely is the concept of the right to be left alone, from being counted, surveyed, canvassed and monitored at will.

Such a notion argues that changing times demand changing principles. Of course humans must adapt to changing times, but not in ways that compel us to discard principles which have proved through history to be the indispensable foundations that define a civilized society. One such principle, beyond doubt, is the right of every person to be recognized as a unique individual, and that means a right to a private life.

Privacy is essential to maintaining a free society. It is fundamental to the democratic notion of self-determination or autonomy—of retaining control over our lives. It is at the heart of the concept that the individual is not the instrument of the state or—it needs underlining—the marketplace, but the reverse.

Trade away information about ourselves and we trade our freedom to conduct our lives without monitoring, supervision or outright interference from those with a particular political or social perspective, or a better product or service to sell. We cannot "make merchandise" of our principles.

**The privacy patchwork**

No longer is it sufficient to talk about protecting privacy with sectoral codes, self-regulation, patchwork legislation and industry watchdogs. Some brave attempts have and are being made. The results are uneven.

The Canadian Direct Marketing Association's code, introduced last year—and strengthened this past February—is a serious effort to deal with the public's flagging patience with unsolicited advertising. While it lacks an independent arbitrator to handle complaints, it restores considerable control to those who want to stop the mail and marketing calls.

The Telecommunications Privacy Protection Agency (TPPA), created for the telecommunications industry to regulate itself, and announced with great fanfare, appears to have been stillborn.

The Canadian Standards Association continues work on drafting a model private sector code—the most ambitious and earnest of all the work. However, it is in danger of being overtaken by the technology and the public's growing concern about the privacy implications of new interactive technology.

The Canadian Bankers Association code (and those of the individual banks) do not cover subjective information about individual clients nor do they protect bank employees. Broad disclosures are allowed to serve the banks' business interest (as anyone who has read the fine print at the bottom of a bank card application will attest). And the codes will do nothing to prevent banks exchanging clients' personal information with the insurance companies and stock brokerages they may now own following recent changes to financial legislation.

Each of these privacy solutions addresses only part of the problem. New communications networks will be shared by governments, most of which live by privacy codes, and a private sector, most of which is unregulated.

**Braking the "communications juggernaut"**

It is time to accept that nothing less than broad privacy legislation for everyone—governments and business—is the only way to hang on to our autonomy in the face of this communications juggernaut. What is desperately needed is national privacy legislation to establish the principles and framework for all the players.

Of course there are jurisdictional questions. But electronic communications leap political boundaries. If there is to be free trade in information, we must all sing from the same songbook. Personal data about Québeckers is now protected at home by the toughest privacy rules in North America. Private companies operating in Québec must live by Québec's new privacy law, and accept liability when sending clients' personal data out of the

province. Yet those same companies operating in the rest of the country have no obligations to other Canadians. This makes no sense.

This new technology makes national privacy protection both essential and inevitable. As Supreme Court Justice La Forest observed, "privacy in relation to information...is based on the notion of the dignity and integrity of the individual. It also has a profound significance for public order."

We must recognize in law the individual's right to control personal information, to understand and consent to its use and disclosure, to examine it and correct errors and, ultimately, to hold the users accountable.

It's our choice and we are fast running out of time.

# Some Early Traffic

Last year's report described the pressures on governments to rationalize programs, improve service and cut costs—and the privacy implications. One proposed solution, an interactive network of government kiosks (or InfoCentres) seems itself to have been overtaken by both budget cuts and advancing technology. However, two projects have crystallized the tensions which can arise between efficiency and privacy. They make concrete the possibilities and threats of these new systems.

First is the appointment of a national council to advise the federal government on speeding up development of the information highway. Second is the federal government's own *Blueprint for Renewing Government Services Using Information Technology.*

## The National Advisory Council on the Information Highway

In March the government appointed a 30-member advisory council to help the federal government develop and implement its strategy for the information highway. Members are drawn from industry, consumer and public interest groups, electronic network users and academia—but not from the privacy and information community. (However, Office staff are members of a government support group providing council members with expertise and services).

One of the council's first actions was to assign members to working groups to examine the issues in depth. One group will consider the access and social impacts of the highway—including the privacy issues. Although the group's objective is to ensure access at reasonable cost, two guiding principles are: protecting the privacy of personal information and ensuring security of service. The group plans to issue a working paper in August, then incorporate comments into a final report expected in December.

One hopeful sign is the council's acknowledgement of privacy as a discrete issue—not merely a subset of enhancing the security of

the electronic systems. The US National Information Infrastructure Initiative (a similar American project) has identified privacy—and the public's concern about it—as one of two potentially deal-breaking issues.

In Canada, the importance of dealing with the public's unease was confirmed by the recent Andersen Consulting survey on the information highway, conducted by Gallup. It's comforting to have an organization with solid business credentials confirm the message of privacy advocates. Andersen's survey found almost 84 per cent of respondents were worried about their privacy on the highway. The report observed that individual response will determine the success of most new information highway initiatives. "It is essential that their views be known before further substantial investment are made...." the report observed.

In follow-up interviews, Andersen staff acknowledged their surprise at the extent of the public's privacy concerns and the imperative of dealing with the privacy issues at the front end. If not, Canadians could stay away in droves.

**A hitchhiker's guide...**

Here then are the privacy considerations that need explicit recognition on the highway:

- Set out in law a fair information practices code to govern the highway;

- Give individuals control over the personal details that are transmitted on the highway;

- Assure individuals that the information will go when and where it is intended—the confidentiality of electronic communications must be protected;

- Limit the collection of personal information to the details essential to providing the service;

- Do not disclose personal information without the individual's explicit consent, and explain data collection practices to clients;

- Protect transactional data (the record of how and when individuals use the system). Do not gather and use transaction patterns for other purposes without the individual's consent;

- Develop cryptography and other technical and security measures to protect the privacy of electronic communications;

- Do not charge for privacy protection;

- Government must accept an oversight role to monitor privacy protection on the highway.

## The Federal *Blueprint*

In February the federal government unveiled its blueprint for an integrated electronic system to deliver its services. The *Blueprint*, essentially, is the government's plan to revamp the public service for the communications age by reducing duplication, cutting costs and improving service. It depends heavily on an electronic information network and envisages partnerships with other levels of government and the private sector.

The government intends to incorporate comments on this "discussion draft" into a series of pilot projects planned for next year.

Increasing government efficiency is a laudable objective which calls for innovative solutions. However, to achieve this new vision, the Blueprint appears to run counter to the protections set out in both the federal *Privacy Act* and its provincial counterparts.

It proposes standardizing, centralizing and sharing government information, and decentralizing service. Not only would federal agencies create and manage shared personal databases, the Blueprint also envisages sharing the information with provincial governments and the private sector (which, except in Québec, has no built-in privacy protections).

These features could dismantle the protective walls around personal data. They beg the question: How will governments reconcile sharing personal databases with that fundamental privacy tenet—collecting only the minimum personal details needed to administer a program? Shared systems must not mean sharing individuals' tax files, medical records or immigration dossiers.

The very reason for segregating personal information is to prevent governments from amassing detailed dossiers about individuals, with all the glittering and frightening possibilities that could hold for citizens.

Of course, the new delivery systems will rely on computer technology. But with the benefits of the technology come the legal questions. How will these integrated systems process requests for access to personal data? Which agency has "control" of the record under privacy laws and, therefore, the obligation to respond to the request. Who will ensure that information is accurate, up-to-date and complete? Will the system impose some contractual obligations on provincial and private sector users?

Privacy laws also prevent governments from making unrelated uses of the information and from disclosing it to others, except under limited and specific circumstances. Once information is downloaded from an electronic system into private databases, what recourse will individuals have against misuse or wrongful disclosures of their information? Will the subjects know who is using their information and how? And what becomes of the principle of an individual's "informed consent"?

Perhaps the more important worry is the social and ethical impact of our increasing reliance on computer technology to make decisions affecting Canadians. Those who rely on computers for their information often ascribe to it a relevance, importance—and accuracy—it does not deserve. The more users who can access and manipulate the data, the more dangerously unreliable it becomes.

The Blueprint acknowledges the need to ensure the "security, integrity and privacy" of the information. However, it seeks protection in various electronic and manual security measures (including better employee training). In truth, these measures treat privacy—the right to be let alone—merely as confidentiality; the promise that although we will not leave you alone, we will guard judiciously everything we know about you. Lost is that essential concept; the right not to be monitored or kept under data surveillance without our knowledge or consent.

Shared personal databases threaten becoming the single government computer file that privacy laws were enacted to prevent. They pose the threat of a national population database and with it the ominous possibility of a national identification card.

## ID Cards

The past year has seen a major assault by human ingenuity on the issue of how individuals prove to governments' satisfaction that they are who they say they are.

Three proposals caught public attention: a provincial cabinet minister's suggestion that the nation carry ID cards to catch welfare cheats; the federal government's plan to issue landed immigrants with a plastic identity card embedded with a photograph, and the US government's new INS PASS (a travel card containing the bearer's hand pattern) now available at the Toronto airport.

**A national ID card** The proposal that Canada consider a national ID card "like many European countries" to check abuse of the social security system sent shivers down many spines.

The arguments for this odious suggestion are the usual—efficiency, convenience and accuracy. They are seductive and hold considerable appeal for governments facing shrinking resources and taxpayers who believe they are being "ripped-off". The problems are real and solutions must be found. The question is whether this solution—treating every Canadian as a potential criminal—is worse than the problem.

A national identification card violates a fundamental notion of democracy—the liberty to live innocent lives free from surveillance by the state—or anyone else. Identification documents that must be carried at all times effectively become an internal passport without which we are nobody. They are undeniably efficient—and with biometric information imbedded, indisputably accurate. They are also the ultimate tool of state control.

Once in place, a national ID card could become the tool for governments to track individuals' family history, expenditures, whereabouts and medical treatments. Detailed profiles could be amassed. And the freedom to live our lives free from unwarranted surveillance would be lost—all in the name of efficiency. It may seem a small and useful administrative step from discrete identification cards to a single super card. But it's a giant leap in transferring power from the individual to the state.

The price is simply too high.

**The landed immigrant card** Not all ID cards pose privacy threats. The new landed immigrant ID card illustrates. Several media stories seemed to imply that the card was sinister and would stigmatize immigrants. The reality is a good deal less dramatic.

The immigration department is faced with a growing tide of forged landed immigrant documents, the forms which certify that a person has been accepted for permanent residence in Canada. As well, the paper document is large, contains substantial personal detail, and becomes worn and brittle with repeated use.

The replacement card carries the bearer's photo and is imbedded with security features that make it difficult to duplicate. The card face has a fraction of the personal data contained on the form it replaces—and there is no information hidden in the card. In effect, it appears more privacy sensitive than the documents it replaces.

Immigration anticipates that the cards will help speed border crossings, and do away with fraudulent documents which cast suspicion on legitimate immigrants.

**The "human hand passport"** A new US travel document known as the Passenger Accelerated Service System (PASS) also raised questions. The US Immigration and Naturalization Service introduced the card at Toronto's Pearson International Airport to speed passengers pre-clearing US Customs.

The card is imbedded with the pattern of the bearer's hand (apparently as unique as fingerprints). Electronic readers located in the airport can identify the person by matching the image on the card with the traveller's hand. Since the image is on the card, which the traveller controls, and is not stored in government records, there appear to be few privacy problems. As well, travellers are not obliged to use the system.

## A National Medical Record Collection

Shortly after publication of last year's annual report, the Office learned of plans to establish a national body to gather together

personalized medical records from provincial health institutions and transform it into aggregate statistical data for research.

In the past, provincial health centres provided information about individual hospital admissions, treatments and deaths directly to Statistics Canada and Health and Welfare (both covered by the *Privacy Act*) and to the Hospital Medical Records Institute.

In an effort to eliminate duplicated efforts and overlapping responsibilities, the National Health Information Council recommended integrating all the activities into a single not-for-profit institute. The new organization, the Canadian Institute for Health Information (CIHI), was incorporated in February 1994. It will operate as a national clearinghouse for aggregate medical data and research.

The change raised concerns that the records were being moved out from under the umbrella of the *Privacy Act* (and the even tougher provisions of the *Statistics Act*). In fact, CIHI will receive medical data from provincial databases and other health related bodies. Neither Statistics Canada or Health Canada will disclose their records to CIHI but will gather data from it for research and statistical purposes.

Nevertheless, neither federal or provincial privacy laws will apply because CIHI is not a government agency. The Office has offered to provide any input CIHI might consider useful in developing principles to manage the information, including a code to ensure the privacy protection of the medical data.

## Following up

### —End "Investigative Body" Exemptions

An earlier report (1991-92) alerted readers to a Justice department proposal to add three organizations to the list of "investigative

bodies" allowed to apply blanket exemptions (under 22(1)(a)) to any information they gather during investigations. Two of these—Park Wardens of Canadian Parks Service and the Enforcement and Intelligence Divisions (GST)–Revenue Canada—remain under consideration.

Far from applauding the proposal, the Commissioner continues to question the very existence of this exemption which, unlike most others, need not meet a test of reasonable likelihood of harm. The exemption "merely provides a convenient shield for bureaucrats not wanting to be troubled by the tiresome need to justify their decision".

Several other exemptions give bodies like the RCMP, Revenue Canada and Correctional Services options for withholding information. For example, section 22(1)(b) allows any government institution to exempt information if disclosure would injure law enforcement, the conduct of a legal investigation—including revealing even the existence of an investigation, or the identity of an informant.

Other sections allow exemptions if disclosure would threaten the security of a penal institution or someone's safety.

Government institutions have now had considerable experience applying these types of injury tests. There is no evidence to support early concerns that assessing the harm of disclosures would impose a costly administrative burden or pose any risks to law enforcement. In fact, the exemption is relatively little used by few government institutions who have shown themselves increasingly willing and able to meet an injury test, even when not required.

In short, any future amendments to the *Privacy Act* should include abolishing this exemption.

**—Smart Cards**

Previous reports have discussed the development and introduction of smart cards (plastic cards with both memory and processing capabilities). The Office has received useful comments on its draft *Privacy and Smart Cards Framework* from the Advanced Card Technology Association and will issue a revised version in the fall of 1994.

The federal government's Smart Cards Working Group (of which the Office is a member) is preparing a technical standard for the physical characteristics of smart cards (based on international standards), and a guidebook on smart card applications and policies. No date has been set for completion.

**—CSA code**

Work continues to "continue apace" on the Canadian Standards Association draft privacy code for the private sector. In June, the full committee meets to consider a working draft of the code and expects to have a first draft ready for public comment in November.

The code is intended not only to establish principles for managing and protecting personal information, but also to set out standards by which the international community can measure the protection offered by Canadian organizations and to make the public aware of how personal information should be protected.

The CSA has also hired an outside expert, University of Victoria professor Colin Bennett to examine international experience with privacy protection codes and to recommend the best option for Canada.

# In the Courts

Two recent Federal Court decisions presented differing views on the definition of personal information and the relationship between the *Privacy Act* and the *Access to Information Act*.

The one case recognizes privacy as a fundamental human right worthy of and demanding government and court protection.

The other dilutes that right significantly.

## Balancing Privacy and Access

In *Robert Sutherland and the Minister of Indian and Northern Affairs*, a member of the Peguis Indian Band applied under the *Access to Information Act* for financial information—the names and job descriptions of individuals receiving or advancing band funds—under the control of DIAND.

In concluding that the information could not be disclosed, Justice Rothstein focused on the *Privacy Act* as a distinct legislative regime. Parliament has provided individuals with a right of privacy for their information which is held by government and a corresponding obligation on the government to assure that right. In this way, once section 19 of the *Access to Information Act* is invoked, it is the *Privacy Act* and its particular legislative scheme which regulates the matter:

> In my view, subsection 19(1) is a limited and specific exception to the right of access to information under the control of a government institution based, as it is, on the purpose of the *Privacy Act* which, as set out in section 2 of that Act, is to protect the privacy of individuals with respect to personal information about themselves held by a government institution.

Information which falls within the general definition of personal information in section 3 of the *Privacy Act* is entitled to protection.

Anyone else seeking access to the information must establish that Parliament intended that the information be stripped of that right:

> ...the general rule is that information about identifiable individuals is "personal information" and only if a specific exception applies, would such information not be "personal information". It follows that a party wishing to demonstrate that information about an identifiable individual is not "personal information" must show that an exception applies.

Justice Rothstein appears to accept the *Access to Information Act* and the *Privacy Act* as equal and parallel pieces of legislation. Government institutions must **disclose** government information; government institutions must **protect** individual information. The right of access under the *Access to Information Act* is subject to stated exemptions, one of which incorporates by reference the rules of the *Privacy Act*. The right of protection under the *Privacy Act* is limited by exceptions to the general definition in section 3 and by the rules of disclosure in section 8:

> As I comprehend the relationship between the *Privacy Act* and the *Access to Information Act* with respect to "personal information", it is first necessary to determine whether the "personal information" in issue falls under subsection 8(2) of the *Privacy Act*. If it does not, by virtue of subsection 8(1) of the *Privacy Act* and subsection 19(1) of the *Access to Information Act*, such information shall not be disclosed.

In *The Minister of Finance and Michael A. Dagg*, Mr. Dagg applied under the *Access to Information Act*, to see the names, identification numbers and signatures of all finance department employees on sign-in sheets for five weekends. He wanted to determine how many members of the Economists and Statisticians Group (ESSA) of the public service union were regularly working overtime. He proposed to determine the total number of hours they worked and market this information to ESSA for its next round of collective bargaining.

The department denied his request, considering it "personal information" which must be exempted from access under subsection 19(1).

Mr. Dagg argued that the information should be released because it concerned the employees' "position or function"—a specific exception to the definition in the *Privacy Act.* He also argued that a name without other accompanying personal details was not personal, and that there was a "public interest" in the disclosure. He complained to the Information Commissioner who upheld the department's decision.

Dagg then applied to the Federal Court for a review and the judge ordered the information released. In his judgement, Justice Cullen concluded that the information was not "personal" because:

> ...the names on the sign-in sheets would only be personal information if they 'appear' with other personal information, nor do the sign-in sheets disclose any other personal information as this is defined in subsection 3.

The judgement raises a "predominant characteristic" test, stating that only information which is predominantly personal and not professionally-related qualifies as personal information.

Finally, and most significantly, the decision unbalances privacy and access rights, shifting the onus in favour of access:

> ...it is important to recall the rule...that when there is any doubt as to whether information constitutes "personal information" which should or should not be released to members of the public, the benefit of the doubt is to be given to the interpretation which favours disclosure...

The Privacy Commissioner considers that the two acts have equal stature and that disclosures under the *Access to Information Act* must comply with the *Privacy Act.* The Commissioner would also

argue that the whereabouts of public servants on weekends is their personal information.

The Privacy Commissioner has formally intervened in the appeal which will be heard in the fall.

## On the courthouse steps: Canada Post identifies witness

Three days before a scheduled appearance in Federal Court, Canada Post Corporation agreed to the Privacy Commissioner's recommendation that it disclose a witness's identity to an applicant.

The case concerned a Canada Post employee who filed a grievance under his union's collective agreement. During its investigation, Canada Post obtained a handwritten witness statement from another union member which led it to dismiss the grievance. The employee requested the witness's name and statement under the *Privacy Act*.

Canada Post first refused to disclose both, arguing that they had been obtained "in the course of an investigation" (paragraph 22(1)(b)(iii)) of the Act. The employee complained to the Privacy Commissioner. During the privacy investigation, Canada Post released a typed version of the handwritten statement and removed the witness's name. The corporation argued that naming the witness would identify a confidential source of information (paragraph 22(1)(b)(ii)) and that the witness's identity was not the applicant's personal information (section 26).

The Privacy Commissioner asked the Court to review Canada Post's decision and order it to disclose the unedited statement. The Commissioner argued, first, that the grievance process is not an "investigation" for the purpose of subsection 22(1)(b), and, second, that there was no reasonable expectation of injury (as the Act requires), particularly when the investigation was complete.

## Investigating Complaints

The office received 1,290 new complaints during the year and completed 1,426 investigations, of which 561 (39 per cent) were well-founded, 798 (56 per cent) not well-founded, and the remaining 67 (5 per cent) abandoned or discontinued at the complainant's request.

### Rolling back extension notices

Approximately 30 per cent of this year's completed investigations concerned departments taking more than 30 days to respond to *Privacy Act* requests. This significant drop—down from 44.5 per cent last year—is a direct result of the Office's efforts to ensure departments do not abuse their right to extend the time limits.

The Act allows departments extra time to consult other organizations with an interest in the records, or if responding in 30 days would "unreasonably interfere" with the department's operations. Many complainants question departments' claims for extension notices.

Until the Office introduced complaints about these notices two years ago, there was no distinction between the validity of the notice and delay in obtaining the records. Segregating complaints about extension notices from time limits complaints led to a significant increase in 1992-93. More important, it identified the departments which were routinely claiming extensions but, in fact, neither consulting other agencies or demonstrating any interference with their day-to-day operations.

Correctional Service Canada and Revenue Canada Taxation, have stopped using extensions (which they often could not justify). This accounts, in part, for the 18 per cent drop in the number of new complaints received this year (1,290 compared with 1,579 last

year). However, the change begs the question: are departments no longer seeking extensions but delaying all the same?

Two issues prompt frequent complaints and need highlighting.

**"Shadow" files, personal notes and desk drawer files**

The office continues to receive complaints about records and notes not put on departmental files or destroyed prematurely. The Office first raised the issue in the 1989-90 annual report in the case of a supervisor who kept a diary on an employee's work behaviour and then refused to disclose it to respond to the employee's privacy request.

Managers routinely make notes about employees to help prepare performance assessments. Making notes is not wrong—treating them as one's personal property is. Privacy investigators often interview supervisors who maintain that the notes are for their own personal use. In fact, these notes are an integral part of the employee's departmental record and may be accessed and must be kept for the minimum retention period under the Act. In these cases, employees usually do not know that the supervisor has notes and if—or when—they find out, accuse the supervisor of keeping "secret" files.

It bears repeating. Supervisors' notes, taken to make decisions directly affecting employees, are part of the department's information holdings—even if kept in the manager's desk drawer. Managers must ensure that the information is protected by the *Privacy Act*. This means collecting only details directly related to the employee's work, keeping the records for at least two years, storing them securely, disclosing them to the individual when access is requested, and disposing of them once the period expires.

The same rules govern similar activities, such as

- staff relations officers keeping notes on discussions with employees coming to them with problems about their supervisors;

- board members taking notes of interviews with candidates when staffing a position;

- departmental officials conducting internal administrative investigations who make notes of witness statements and using them as aides-memoir to prepare a report.

**Investigating harassment complaints**

Several recent privacy complaints have revealed what are essentially inconsistent disclosures of personal information gathered during harassment investigations, though in each case the government institution may well have met the requirements of the *Privacy Act*.

At issue is how much information the parties to harassment complaints receive, and at what stage in the inquiry. The amount disclosed seems to depend on which organization deals with the complaint. Some departments disclose all the information the investigators gather, while others apply *Privacy Act* exemptions.

Yet others rely on a "disclosure process" which gives all parties the investigator's summary report, containing the preliminary findings, but not the identities and statements of witnesses. They then invite the parties to make representations.

Some individuals, dissatisfied with the amount of information disclosed, have used the *Privacy Act*, arguing that without the information, they cannot rebut the preliminary findings.

However, even citing the Act may not get complainants the information. Most departments claim that disclosure would injure "the conduct of a lawful investigation" (section 22(1)(b)), at least until the inquiry is closed. Departments with "investigative body" status have cast this cloak over even administrative inquiries—such as harassment investigations. They claim a blanket exemption which can last as long as 20 years (section 22(1)(a)).

Other departments have attempted to wash their hands of any responsibility by contracting out harassment investigations to private companies. When they receive access requests, they claim they do not have control of the information—it is the property of an outside contractor.

Two Federal Court cases illustrate the problems. In the first case a manager, accused of harassment by a subordinate, asked the Federal Court to order the department to disclose all the information it would use to decide the merits of the complaint. He argued that the Treasury Board policy did not allow him to adequately defend his own interests.

While the judge left it to the department to decide what specific details it should share with the parties, he suggested it would be consistent with resolving the complaint to disclose all information used to come to a decision.

In the second case, a man complained to the Commissioner that an "investigative body" had withheld the witnesses' identities and now intended to fire him. The Office could not persuade the department to release the information because, technically, the *Privacy Act* allowed the department to withhold it.

Fortunately the complainant had also filed an action in Federal Court. The court found that the department had denied the complainant his right to a fair hearing by withholding information

on the basis of which he was dismissed. Without it he could not properly defend himself.

These inconsistencies in applying the Treasury Board policy stem from departments misunderstanding their responsibilities under the *Privacy Act*. These are twofold: properly managing all their personal information holdings (sections 7 and 8), and providing individuals access to their personal information (section 12).

A government institution may disclose personal information to third-parties without the subject's consent if disclosure is consistent with the purpose for which it was collected (section 8). Gathering information and testimony during harassment investigations and then disclosing it to the parties is fundamental to any reasonable harassment policy. The process must be accountable and open. It must acknowledge both the complainant's right to know the disposition of the complaint and the accused's right to know and challenge the accusations. The *Privacy Act* already permits these disclosures to the parties to harassment complaints without resort to formal requests.

Some departments have difficulty reconciling these disclosures in the interests of "natural justice" with their obligations to give an applicant his or her **own** personal information and not that about others. If the institution decides to exercise its discretion to disclose information to the parties because it is consistent with ensuring that the process is open and fair, it is not required to exempt third-party information (as it would in all other cases under section 26).

During these investigations, the following should be kept in mind:

- departments must be able to demonstrate how the disclosures would injure the investigative process (22(1)(b));

- investigative bodies should not claim blanket exemptions for administrative investigations (22(1)(a));

- contracting out harassment investigations does not abrogate the department's *Privacy Act* responsibilities—the contractor is simply its agent, and

- disclosures to the parties of personal information collected to adjudicate harassment complaints are consistent with the process and permissible to meet the requirements of natural justice and due process.

**BC and Nova Scotia open access to RCMP files**

Residents of British Columbia and Nova Scotia will no longer be automatically refused access to provincial policing records gathered by the RCMP. The two provinces have rescinded agreements with the federal government which applied a blanket exemption to all RCMP records from provincial policing. The RCMP will process applications (and apply exemptions) under the federal *Privacy Act*.

(Of course, the change means more work for the RCMP—and possible delays for applicants. Without the blanket exemption, the RCMP will have to review all the records individually to determine what may be released.)

The change is good news for BC and Nova Scotia residents. However, it also highlights the unevenness of Canadian privacy rights. The RCMP has policing service contracts with all other provinces and territories (except Ontario and Québec). Canadians in the remaining provinces and territories will continue to be denied access until those governments follow BC's and Nova Scotia's lead.

# Who complains?

## The Public

### Postal employee reveals woman's whereabouts to estranged husband

An Alberta woman complained that Canada Post Corporation (CPC) improperly disclosed information about her which led to the discovery of her whereabouts by her estranged husband, whom she feared. The local postal station had given the husband the names of occupants and the street address of her postal box number, from which he found her telephone number (also listed under another name) and had contacted her.

She also alleged that her husband had used his authority as a Transport Canada employee to dupe the postal employee into giving him the information.

The husband admitted obtaining the information from an employee (whom he could not identify) at the local postal station. He gave the investigator a copy of his notes of the information he obtained from the postal station .

None of the postal station employees interviewed could recall disclosing the information. The investigator examined the Application Card for Lock Box and the details were exactly the same as those the ex-husband gave the investigator.

Since no employee could recall (or would admit to) disclosing the information, the investigator found no proof that the husband had misused his authority as a federal government employee. The Commissioner dismissed this complaint. However, he considered the improper disclosure complaint well-founded.

Canada Post has apologized to the complainant and reminded all CPC corporate and private postal outlets of their obligation to protect customers' confidentiality.

**Faxes—proof it's sent not proof it's received**

A complaint against CSIS illustrates how the law struggles—and often fails—to keep up with technology (and not very high technology at that).

The complainant alleged that the Canadian Security Intelligence Service (CSIS) had not responded to his access request within 30 days. The complainant had his fax machine's activity report to prove that he had faxed a single page to CSIS's privacy office on that date. However, CSIS had no record of its receipt. CSIS's fax machine was not on the same floor as the privacy section and was used by other staff, so the document could have been misdirected. However, the complainant had faxed earlier requests to CSIS without incident.

The investigator did not dispute the complainant's evidence or CSIS's statement that it had not received the document. At issue was whether faxing a request form was a *prima facie* case that a department had received it. The investigator could find no jurisprudence on the status of faxed documents.

Ultimately, the Commissioner had to rely on commonly accepted practices in both the private and public sector. These virtually all recommend that the sender call ahead of the transmission to alert the receiver, or afterwards to confirm that the message was received. The complainant had done neither. The Commissioner concluded that the onus is on the sender to confirm receipt and dismissed the complaint.

**Update agreements to share bank account numbers**

Canadians consider their financial information particularly sensitive. A senior citizen from British Columbia was more than a little concerned to find that Health and Welfare Canada had given her bank account number to the B.C. Ministry of Social Services. She discovered the disclosure when she noticed that her B.C.

Social Service income supplement had been deposited directly in her account. The bank told her that the information had been provided by Health and Welfare.

The B.C. Income Supplement is calculated on an amount provided by the federal government. When the complainant opted to have her federal government benefits deposited directly to her account, Health and Welfare passed the bank account numbers to B.C. on computer tapes.

The department relied on old federal-provincial sharing agreements dating back to the 1970s—well before the *Privacy Act* came into force—and long before the direct deposit option. The agreement was obsolete and did not authorize disclosing to other governments the information Canadians provided to take advantage of the direct deposit program.

The problem posed a dilemma for Health and Welfare. On the one hand, they were disclosing personal information without proper authority. On the other hand, not providing the information could severely disrupt the program and lives of many people who depend on it. The deputy minister of Health and Welfare undertook to make a priority of renegotiating the information sharing agreements with the provinces.

**No letters on public files without consent**

A man complained to the Privacy Commissioner that his letter to the Canadian Radio-Television and Telecommunications Commission (CRTC) about obscene language in a television program had been sent to the broadcaster without his knowledge or consent. He also objected strongly to having his letters placed on the CRTC's public file.

The investigation confirmed that the CRTC gave the broadcaster a copy of the complainant's letters for a reply and placed both the letters and replies on its examination files. These files (and the correspondence on them) are public because the complaints process is "open". CRTC also argued that broadcasters have a right to know the nature of the allegation, the identity of the complainant and have the right to reply to the actual complaint as made.

The Privacy Commissioner agreed that providing the broadcaster with copies of the complainant's letters was entirely consistent with the complainant's reason for writing to the CRTC—to have the complaint investigated and resolved. (However, personal details in some of the letters on file were entirely superfluous and could be withheld without damaging the investigation.)

However, the Commissioner could not accept the CRTC's argument that all correspondence should be put in its public files. Given the nature and amount of personal detail found in those letters, it was evident that the writers expected confidentiality. Making them available to the public was an undeniable loss of the individual's privacy and could not be justified without the person's consent.

After lengthy debate, CRTC officials agreed to change their complaints procedures and allow individuals to decide whether to have their complaint letters and associated material placed on public files. The CRTC will explain the procedure when it updates its publications.

The Commissioner concluded that the complaint, while well-founded, was resolved because the CRTC has removed the letter from the public file.

## Taxpayers

### Taxation reveals second income to justify high garnishee

Another taxpayer, who owed money to Revenue Canada-Taxation, complained that Taxation had disclosed his Canada Pension income to the Saskatchewan Workers' Compensation Board.

Taxation revealed his other income source when the Board asked it to justify what it considered might be an excessive garnishee (50 per cent) of his compensation benefits. The news that the complainant had other income prompted the Board to begin its own action to recover compensation overpayments. (Worker compensation benefits must be reduced by any Canada Pension income.)

The *Income Tax Act* allows Taxation to make disclosures to ensure it can enforce the act; the *Privacy Act* allows disclosures to comply with another act of Parliament. Since Taxation released the information to justify the rate at which it recovered taxes owing, the Commissioner concluded there was nothing improper in the disclosure.

### Health & Welfare replaces "intrusive" questionnaire

A questionnaire used by Health and Welfare Canada to determine which parent is eligible for the child tax benefit prompted a Winnipeg woman to complain to the Commissioner. She found the questions excessively intrusive.

The questionnaire asked the parent to explain the details of the child's daily care, and how they supervised each activity, "from the time they awaken in the morning to the time they go to bed at night". This included bathing, selecting clothing and after-school and evening routines. The parent was also asked to list all the child's recreational activities and medical and dental appointments,

including the dates of last and next visit, who made the arrangements, how the child was transported and with whom.

Health and Welfare's Manitoba region sent the woman the questionnaire because she and the father shared custody and both had applied for the benefit. In trying to determine which parent was primarily responsible for the child's care, the department assessed the woman's application against eight factors set out in the Income Tax Regulations. These factors include where the child lives, which parent provides meals, clothing, and attends to the child's daily needs.

The investigator determined that only five out of the 18 questions were directly related to the factors. The remainder asked either for more detail than needed or for information not required at all. The Commissioner concluded that some of the questions were indeed intrusive and well outside what the program required. The complaint was well-founded.

The department agreed and issued a new national questionnaire which reflects faithfully the factors in the regulations. The Office has reviewed the questionnaire and the Commissioner concluded that it resolves the complaint.

**Spousal agreements more detail than taxman needs**

A Saskatchewan resident complained that Revenue Canada Taxation was improperly collecting personal information when it asked him for a copy of his spousal agreement. Taxation wanted the information to establish the amount he could claim as a tax deduction for maintenance paid to his ex-spouse. The amounts he deducted and she declared did not match. The complainant felt that Taxation should only be interested in the portions of the document relating to child maintenance, alimony and Canada Pension Plan obligations.

RCT Taxation Operations Manual required that assessors copy the Interspousal Agreement and retain the copy on file.

Taxation officials explained that information from interspousal, separation and divorce agreements was required to determine the tax implications of support payments and division of assets and pension benefits. The privacy investigator explained the Commissioner's concern that Taxation was collecting more personal information than needed to determine individuals' tax obligations.

Taxation agreed that it did not need all the details and has amended its procedure and its policy manual concerning verifying a client's claim. Taxation assessors will now copy the original document and, in the client's presence, delete the personal details not pertinent for taxation purposes. The Commissioner considered the complaint well-founded but resolved.

## Immigrants

### Psychiatric assessment not needed for complaint to Bar

Several 1992 Federal Court decisions opened up immigration hearings, with the potential to make "public" any documents used in the hearing—including sensitive medical records.

A lawyer alleged that Employment and Immigration's Adjudication Branch had improperly collected a psychiatric assessment of a woman during an immigration hearing and then disclosed it to the Québec Bar in a complaint about his behaviour during the hearing. (The branch is now part of the Immigration Refugee Board.)

The lawyer was at the hearing in case the adjudicator needed legal services. However, it was not clear that the lawyer was acting for the woman. In fact, the investigator was not sure the woman even knew about the complaint. Several weeks elapsed

before the investigator received the woman's authorization to proceed. The subsequent investigation called into question whether the woman fully understood the authorization. However, the allegations would have been serious enough for the Commissioner to proceed on his own authority.

The woman was a permanent resident but had left Canada for more than the permitted two-year absence. During the hearing to determine whether she could return, the adjudicator questioned whether she had the mental capacity to understand the proceedings or to formulate an intent to leave the country. When he appointed a representative, a dispute erupted with the lawyer who was asked to leave.

It was evident from the transcripts that the representative, a provincial social worker, had asked for the psychiatric assessment to determine whether the woman understood what was happening, and whether she needed a lawyer. The collection complaint was not well-founded.

Once the psychiatric assessment was complete, it was tabled before the hearing and EIC was given a copy. There was no doubt that the report had been attached to the complaint to the Québec bar but EIC argued that complaints require substantive supporting evidence and that documents presented at the now-public hearings are "public".

The Commissioner did not agree that so sensitive a document was intended to be publicly available. He could find nothing in the *Privacy Act* which would allow the disclosure and considered the complaint well-founded.

## Inmates (and parolees)

### Privacy request turns up documents for appeal

A complaint that Justice Canada had improperly denied an applicant information—although not well-founded—brought to light a case in which the *Privacy Act* was instrumental in providing information vital to the man's court appeal.

The case illustrates how the Act can be an effective tool to hold governments accountable.

The complainant told the investigator he had been convicted of a 1961 armed robbery and was imprisoned for seven years. Protesting his innocence, he had written to any government official or department he thought might help, and began searching for any documents that might support his case.

Finally, in 1990, he wrote to the Justice Minister requesting a pardon. After reviewing his case, the Minister told him he might have grounds for an appeal and suggested he pursue this avenue before applying for a pardon.

The Québec Court of Appeal agreed to hear his case in the summer of 1994. In preparation for the hearings he applied to Justice under the *Privacy Act* for all information it held about him. Among the documents Justice found were Québec provincial police reports on the robbery and the subsequent investigation. He considered these essential for his appeal, believing they corroborated his innocence.

Years of fruitless searching for the documents ended with his *Privacy Act* application. His complaint to the Commissioner was simply to confirm that he now had all the material to which he was entitled.

The investigation revealed that although Justice had withheld some information about another individual, it supplied the complainant not only with all his personal information but also any information about others if it had previously been disclosed in open court.

**No charge to examine medical records**

A former inmate objected to Correctional Service Canada's (CSC) method of providing him access to his information in its Psychiatric Treatment Centre and Psychology personal information banks. CSC released some documents informing him that:

> ...you may receive an explanation of the content of portion/pages ___ by a psychologist of your choice; however, you cannot be given a copy of these portion/pages. Therefore, if you provide us with the name and address of a psychologist, we will send him the relevant documents. Please be advised that CSC will not pay the fees if you choose to consult a psychologist who would charge a fee for services.

The Privacy Regulations permit CSC to provide individuals access to their medical information in the presence of a qualified medical practitioner or psychologist. The intent is to ensure that the applicant understands sometimes technical information and can have questions answered. CSC's method does not violate any access right under the *Privacy Act.*

However, the Commissioner was concerned that some applicants (specifically ex-inmates) were effectively paying for access to personal records—a fee to a doctor or psychologist to interpret the information. (There is no charge to examine personal records under the *Privacy Act.*) Both the *Act* and *Regulations* put the responsibility on federal government departments to arrange convenient and reasonable means for examining personal information. The Commissioner did not consider this method either convenient or reasonable for the applicant.

After some discussion, CSC agreed to change its process and give applicants the option of meeting a CSC doctor or psychologist in their area (at no charge) or consulting their own medical practitioner (for which they would pay a fee). Although the Commissioner found CSC's procedure wanting, technically the complainant was not denied his right of access so his complaint was not well-founded. The Commissioner appreciates CSC's sensitivity to the issue and decision to change its process.

## Employees

### Mint monitors employee phone calls

One complaint revealed a practice that the Act does not forbid but about which the Commissioner has profound reservations—monitoring employees' telephone calls.

An employee complained that the Royal Canadian Mint's monitoring of its employees' telephone calls was an improper collection and use of their personal information.

The investigator found that employees of the Direct Marketing Service (which promotes and distributes collector coins) were told of the monitoring three days before it began. Several days later they received a note which explained that the system was "solely for training and performance evaluation purposes". The supervisor monitors—but does not record—the calls and may take handwritten notes.

The Commissioner had to concede that the Mint's collection of this personal information for employee assessment did not contravene the *Privacy Act* and, therefore, the complaint was not well-founded. However, he reminded the Mint that employees have a right to examine any notes made about them.

The complaint raised several other privacy questions. Has the Mint established any procedures to ensure that notes will not be

used or disclosed for other purposes? What happens to notes once they are no longer needed for performance appraisals? Are customers told that their conversations with Mint staff might be monitored? Do supervisors' notes include customers' personal information?

The Mint undertook to answer the Commissioner's questions and is drawing up internal guidelines which the Office will review. In a follow-up about three months later, the investigator found telephone conversations had been monitored but no notes taken.

**Customs employees' names not personal information**

A Revenue Canada–Customs employee complained on behalf of her co-workers that Customs intended disclosing the names of employees in the Prohibited Importations Directorate in response to an Access to Information request. The employees considered this an improper disclosure of their personal information and worried for their safety.

Customs had been asked for both the names and qualifications of the directorate's employees. The employees told Customs' officials that the requester was suspected of being a high-ranking member of a white supremacy group which had been denied importation of "hate material" into Canada. They feared repercussions if he obtained their names.

Reluctantly, Customs complied with the request because the *Privacy Act* states that names of government employees, their duties and responsibilities, are not "personal information". (The definition is intended to ensure the openness and accountability of the public service.)

The investigator found that Customs had disclosed only the surnames, an initial and the statement of qualifications for each position—not the individuals' resumés. The Commissioner agreed with Customs' handling of the response and considered the complaint not well-founded.

**SINs, home addresses not for unions**

Union actions against members who worked during the last public service strike led to three complaints against National Defence and Revenue Canada, and a fourth initiated by the Commissioner against Treasury Board.

The employees complained that departments had given their social insurance number (SIN) and home addresses to the Public Service Alliance of Canada (PSAC), the public service union which called the strike.

During a tense period following the strike, some union locals voted to suspend members who continued to work. The National Defence local posted the minutes of its meeting and a list of names and SINs on a DND bulletin board.

PSAC is not covered by the *Privacy Act* or any other privacy legislation, so the employees had no way to proceed against the union.

The departments were following Treasury Board policy which required them to give PSAC employees' names and SINs in order to remit dues it collects on the union's behalf. The policy also obliged departments to complete PSAC forms for each new employee, including the home address.

Since it was obvious that the departments were simply following government policy, the Commissioner opened a complaint against Treasury Board.

The government may only disclose personal information if the individual consents, or if there is specific authority set out in the *Privacy Act*. Treasury Board argued that its authority came from collective agreements under the *Public Service Staff Relations Act*. The Commissioner did not agree. Collective agreements do not have the force of law. If an agreement conflicts with a law, the law—in this case, the *Privacy Act*—takes precedence.

The Board resolved the complaint about disclosing home addresses by giving each new employee the PSAC enrolment form. Those who opt to become union members provide their home addresses, those who do not simply pay dues from their work location.

The complaints about improper disclosure of the SIN was soon to be resolved by Treasury Board's conversion to new internal employee numbers and a second record number for outside agencies, such as unions. The change came as a result of the federal government's restrictions on use of SIN to social benefit programs and income tax reporting.

The Commissioner concluded that all four complaints were well-founded and resolved.

**Stenographer's notes transcribed**

A National Defence (DND) employee complained that he was denied access to the stenographic notes (and transcriptions) taken during two meetings to discuss his conduct.

DND personnel claimed that the stenographer's notes were not available and the reports the complainant had already received adequately reflected the minutes of the meetings. The complainant disagreed. At the investigator's insistence, DND searched elsewhere and uncovered the notes. The investigator then compared them with the reports and found many omissions and discrepancies.

Stenographic notes about an individual are personal information and, since most people do not read shorthand, should be transcribed for the applicant. DND refused to prepare a word-for-word transcription, maintaining that the reports were accurate (with the exception of one paragraph inadvertently omitted from the original).

The investigator was not satisfied and the base commander ordered the notes transcribed. The results were disappointing—the transcription was still not accurate. All attempts over several months failed to produce a true transcription. In frustration, the investigator went to the base and, working with the secretary who had taken the notes originally, produced a more accurate transcription.

Since DND had refused to provide the complainant with the stenographic notes and then withheld a complete and accurate transcription, the Commissioner considered the complaint well-founded and ultimately resolved—but not without considerable time and effort.

**Disciplined for refusing to consent to disclosure**

An employee complained that Canada Post had suspended him without pay because he had refused to sign a "Consent for Release of Medical Information" form authorizing his doctor to disclose medical details about an injury at work.

An examination at a hospital emergency room found the employee too disabled even for "modified duties". At Canada Post's request, he saw a second doctor who confirmed the emergency doctor's diagnosis. The second doctor described the employee's physical limitations and estimated the dates on which he could return, first to modified, and then to full duties.

However, when the employee applied for Workers' Compensation, Canada Post challenged the claim, saying it had modified his duties to accommodate his injury. Then it asked him to complete the consent form and provide more medical details. He refused, but offered to have his doctor respond to specific questions. Arguing that it did not have enough information to process the claim, Canada Post put him on "off-duty status" without pay until he consented to the disclosure.

Faced with an employee who will not sign the consent form, Canada Post's policy is to have the employee examined by a physician of its choice. In this case, Canada Post seemed able to modify the employee's duties based on information supplied by the second doctor but then attempted to collect more medical details, after the fact. It did not follow its own policy and the Commissioner concluded that the attempted collection was unreasonable. The complaint was well-founded.

Canada Post is changing its procedure for collecting additional medical details. This should help prevent a recurrence and will resolve the complaint.

## Notifying the Commissioner

One vital feature of the *Privacy Act* is its prohibition against government disclosing clients' and employees' personal information without their consent. However, there are some specific exceptions, two of which require the government agency to notify the Privacy Commissioner—disclosures in which the "public interest" outweighs any invasion of privacy, and those that benefit the person concerned.

Determining whether there is an overriding "public interest" is the responsibility of the head of the government body—usually a deputy head. The Commissioner cannot prevent the release. However, the notification gives him an opportunity to alert the person if he thinks it necessary. It also allows government managers and privacy staff to discuss proposed releases and sometimes to focus the disclosure on the essential information and not gratuitous personal details.

The Commissioner may initiate his own complaint and, of course, the individual may complain—albeit after the fact.

Staff examined 3986 release notifications, 3938 of which were disclosures to MPs. Once Parliament is dissolved for an election, MPs lose their status. This means they no longer benefit from a provision in the *Privacy Act* allowing government agencies to give MPs personal information about constituents who have turned to them for help (for example, to track down a visa application).

In order to allow MPs to continue providing this "benefit" to constituents, the Office arranged with Immigration and Citizenship Canada to submit periodic reports to the Commissioner's office for monitoring during election campaigns.

Following are other examples of disclosure notices.

**Parks Canada confirms address from voters' list**

The Commissioner was less comfortable with Parks Canada checking addresses with Elections Canada's voters' lists. Parks had asked Elections Canada to verify a couple's address on its Calgary lists from 1980 onwards. The check was to determine the couple's eligibility to live in the town of Banff which is inside the National Park.

There were several obvious questions surrounding the disclosure. Did Parks Canada notify the individuals? Did it try to get their consent? Did it try examining Calgary municipal lists first? Unfortunately it was too late; the disclosure had already been made. The Commissioner notified the couple.

**Possible abuse cases released to police**

During the past two years, Indian and Northern Affairs (INA) notified the Commissioner of several disclosures from departmental files concerning allegations of abuse of native children in church-run residential schools. The allegations had surfaced during the hearings of the Royal Commission on Aboriginal Peoples. INA gave the information to Health and

Welfare, the RCMP, the Ontario Provincial Police and the Sûreté du Québec.

The INA disclosures follow its review of more than 2,200 files stretching back to the 1940s. INA discovered at least 33 cases in which there may be criminal prosecution.

A privacy investigator examined the material prior to release and the Commissioner did not notify the individuals.

**Immigration Board alerts law societies of "ethical" breaches**

The Immigration and Refugee Board notified the Commissioner about several disclosures of information from refugee claimants' files to provincial law societies. The Board was concerned about the behaviour of several lawyers representing claimants at its hearings, suspecting some had breached rules of professional conduct. (For example, one lawyer withdrew from a case the day before the hearing.)

The Board submitted that there is a public interest in ensuring lawyers abide by the ethical standards of their profession. The Commissioner did not notify the clients. However, IRB has agreed to give privacy staff an opportunity to examine the material before detailed files are given to law society investigators.

**Family Allowance database identifies young voters**

During last year's federal election, Employment and Immigration (EIC) advised the Commissioner that it would disclose information from its Family Allowance database to Elections Canada to help update voters' lists.

Elections Canada did not conduct the usual door-to-door enumeration for the 1993 election (except in Québec), relying instead on its lists from the October 1992 Constitutional referendum. However, to identify Canadians who had turned 18

since the referendum (and were now eligible to vote) it turned to EIC. EIC searched its Family Allowance database, identified the new voters and Elections Canada mailed them information about getting on the voters' list.

Although clearly not a "consistent" use of the information, EIC argued that its disclosure was in the "public interest" of encouraging both broad and individual exercise of the democratic right to vote. The Commissioner did not object.

## Inquiries

The Office's inquiries set another record—8,688 compared to 5,184 last year, a 68 per cent increase. The majority of these are answered by two officers who act as a privacy clearinghouse, providing details about the federal *Privacy Act* or background and contacts at other government agencies and in private industry.

Most callers asked how to use or interpret the Act (41 per cent), 26 per cent wanted Office publications, 17 per cent complained about organizations not covered by the *Privacy Act* and seven per cent concerned use and abuse of the Social Insurance Number.

Callers are often puzzled to find that some federal Crown corporations are not covered by the Act. Staff answered several calls from employees of Atomic Energy of Canada Ltd. (AECL) who were denied access to their personal files. AECL management also called to ask whether they could simply follow the rules in the *Privacy Act* even though AECL is not covered.

Obviously the Commissioner encourages any organization to live by the privacy code. Nevertheless, it is disappointing that seven years after Parliament reviewed the Act (and recommended covering the Crown corporations), a good deal of the federal government remains outside the Act.

One of those federal institutions not covered is Parliament itself. Many callers were frustrated at getting no response to requests for access to correspondence in the offices of the Prime Minister or Cabinet members.

The new Québec law (which took effect on January 1, 1994) had an immediate impact on the unit's work. Québeckers now have privacy rights in the Québec private sector and are happy to discover that the Québec Information and Privacy Commissioner may be able to help them.

Two segments of the private sector prompt recurring complaints—credit bureaus and financial institutions. With the individuals' consent, the Commissioner referred several complaints to Equifax for follow-up. (Credit bureaus are now covered in Québec.) Elsewhere in Canada, inquiries about financial institutions' collection and disclosure of personal information must be referred back to the banks.

**Big Brother on Highway 401**

Several callers complained that they had been monitored while travelling on Highway 401 (Southern Ontario's main East-West route). Apparently the Ontario Ministry of Transportation had set up video cameras to monitor traffic flows, recorded licence plates and sent the questionnaires to the registered vehicle owners. One caller generated two questionnaires—once driving his own car and a second driving his girlfriend's.

Staff referred the calls to the Ontario Privacy Commissioner who opened his own complaint.

**No Fingerprint Fees for Privacy Requests**

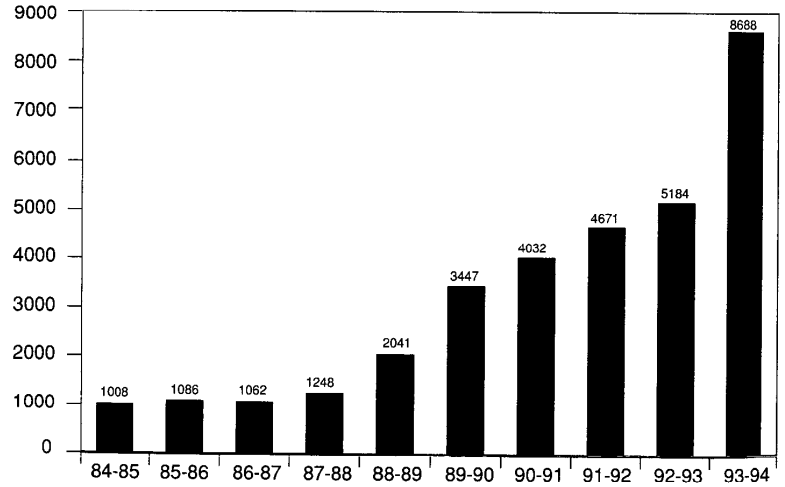
Other callers wanted to know why the local RCMP detachment charged $26.75 to take their fingerprints to prove their identity

when making a privacy request. There are no fees for personal records under the *Privacy Act*.

Inquiries staff established that the Force now recovers costs to fingerprint for "employment" purposes. There should be no charge for fingerprinting to confirm a privacy applicant's identity. RCMP headquarters has explained the procedure to detachments and privacy staff will refer future calls to headquarters to arrange a fee waiver.

(The RCMP returns the fingerprints with the records.)

## Inquiries 1984-94



## Top Ten Departments by Complaints Received

| Institution | TOTAL | Grounds | | |
|---|---|---|---|---|
| | | Access | Time Limits | Privacy |
| Correctional Service Canada | 202 | 80 | 91 | 31 |
| Employment and Immigration Canada | 184 | 64 | 51 | 69 |
| Revenue Canada - Taxation | 135 | 52 | 67 | 16 |
| National Defence | 103 | 48 | 36 | 19 |
| Royal Canadian Mounted Police | 94 | 56 | 26 | 12 |
| Canada Post Corporation | 68 | 40 | 2 | 26 |
| Canadian Security Intelligence Service | 59 | 39 | 19 | 1 |
| Agriculture Canada | 57 | 34 | 6 | 17 |
| Indian and Northern Affairs Canada | 48 | 4 | 44 | 0 |
| Revenue Canada - Customs and Excise | 44 | 21 | 11 | 12 |
| OTHER | 296 | 166 | 48 | 82 |
| TOTAL | 1,290 | 604 | 401 | 285 |

## Completed Complaints by Grounds and Results

| Grounds | | Disposition | | | | |
|---|---|---|---|---|---|---|
| | | Well-founded | Well-founded; Resolved | Not Well-founded | Discontinued | TOTAL |
| Access | | 13 | 216 | 524 | 31 | 784 |
| | Access | 11 | 212 | 481 | 29 | 733 |
| | Correction/Notation | 2 | 4 | 41 | 1 | 48 |
| | Index | 0 | 0 | 0 | 0 | 0 |
| | Language | 0 | 0 | 2 | 1 | 3 |
| Privacy | | 23 | 84 | 110 | 15 | 232 |
| | Collection | 8 | 6 | 26 | 6 | 46 |
| | Retention & Disposal | 5 | 6 | 9 | 0 | 20 |
| | Use & Disclosure | 10 | 72 | 75 | 9 | 166 |
| Time Limits | | 223 | 2 | 164 | 21 | 410 |
| | Time Limits | 192 | 1 | 127 | 21 | 341 |
| | Extension Notice | 31 | 1 | 37 | 0 | 69 |
| TOTAL | | 259 | 302 | 798 | 67 | 1,426 |
| | | 561 | | | | |

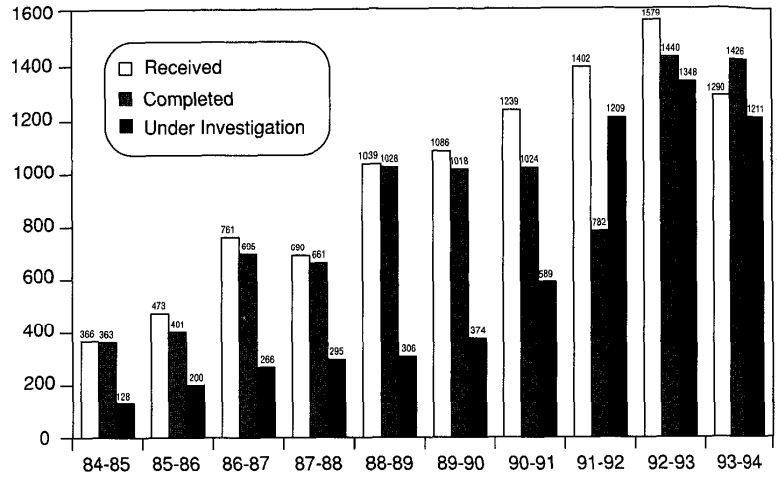
## Completed Complaints by Department and Result

| Department | TOTAL | Well-founded | Well-founded; Resolved | Not Well-founded | Discon-tinued |
|---|---|---|---|---|---|
| Agriculture Canada | 4 | | | 3 | 1 |
| Canada Mortgage and Housing Corporation | 1 | | | | 1 |
| Canada Post Corporation | 150 | 13 | 45 | 90 | 2 |
| Canadian Commercial Corporation | 1 | 1 | | | |
| Canadian Human Rights Commission | 2 | | | 2 | |
| Canadian International Development Agency | 1 | | | 1 | |
| Canadian Radio-television and Telecommunications Commission | 6 | | 1 | 4 | 1 |
| Canadian Security Intelligence Service | 97 | 1 | | 96 | |
| Commissioner of Official Languages | 4 | 2 | 1 | 1 | |
| Communications, Department of | 3 | | 2 | 1 | |
| Consumer and Corporate Affairs Canada | 4 | | | 4 | |
| Correctional Investigator Canada | 1 | 1 | | | |
| Correctional Service Canada | 267 | 61 | 59 | 144 | 3 |
| Elections Canada | 1 | | | 1 | |
| Employment and Immigration Canada | 149 | 43 | 29 | 55 | 22 |
| Energy, Mines and Resources Canada | 3 | | 1 | 2 | |
| Environment Canada | 4 | | 1 | 3 | |
| External Affairs Canada | 17 | 5 | 3 | 8 | 1 |
| Health and Welfare Canada | 131 | 14 | 13 | 104 | |
| Immigration and Refugee Board | 10 | 10 | | | |
| Indian and Northern Affairs Canada | 5 | | | 5 | |
| Industry, Science and Technology | 5 | | 2 | 3 | |

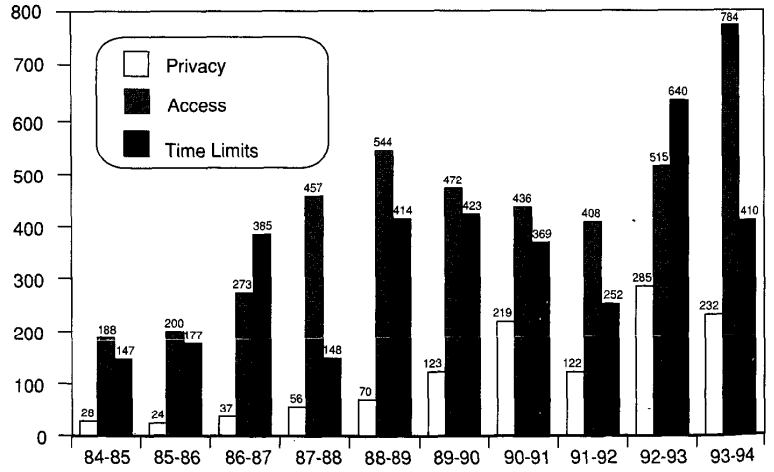
## Completed Complaints by Department and Result

| Department | TOTAL | Well-founded | Well-founded; Resolved | Not Well-founded | Discontinued |
|---|---|---|---|---|---|
| Justice Canada, Department of | 13 | 1 | 1 | 9 | 2 |
| Labour Canada | 4 | 1 | 1 | 2 | |
| National Archives of Canada | 72 | | 50 | 22 | |
| National Defence | 76 | 30 | 11 | 35 | |
| National Parole Board | 29 | 3 | 7 | 19 | |
| Privy Council Office | 6 | 3 | | 3 | |
| Public Service Commission of Canada | 10 | 2 | 2 | 4 | 2 |
| Public Works Canada | 4 | | | 4 | |
| RCMP Public Complaints Commission | 4 | 2 | | 2 | |
| Revenue Canada - Customs and Excise | 99 | 35 | 20 | 43 | 1 |
| Revenue Canada - Taxation | 80 | 16 | 11 | 29 | 24 |
| Royal Canadian Mint | 3 | 1 | 1 | 1 | |
| Royal Canadian Mounted Police | 94 | 11 | 6 | 74 | 3 |
| Secretary of State | 4 | | 1 | 3 | |
| Solicitor General Canada | 7 | | | 7 | |
| St. Lawrence Seaway, The | 1 | | | 1 | |
| Statistics Canada | 1 | | | 1 | |
| Supply and Services Canada | 10 | 1 | 3 | 5 | 1 |
| Transport Canada | 40 | 1 | 30 | 6 | 3 |
| Treasury Board of Canada Secretariat | 1 | | 1 | | |
| Veterans Affairs Canada | 2 | 1 | | 1 | |
| TOTAL | 1,426 | 259 | 302 | 798 | 67 |

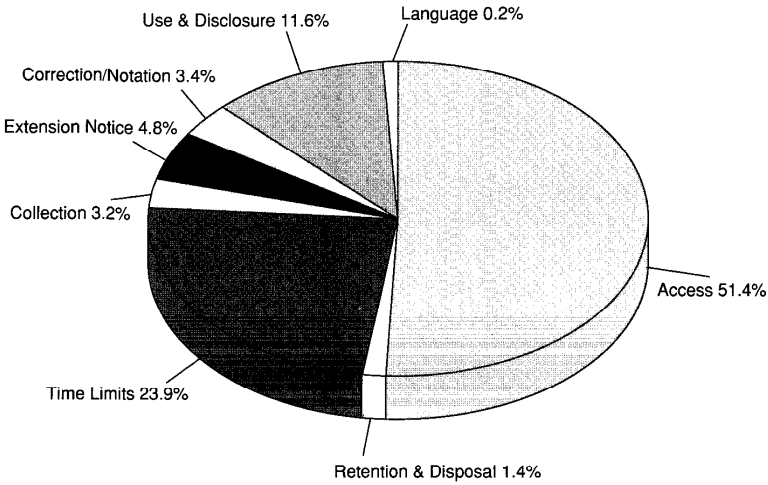
## Completed Complaints 1984-94




## Completed Complaints and Grounds 1984-94



## Complaints Completed by Grounds 1993-94




## Origin of Completed Complaints

| | |
|---|---|
| Newfoundland | 19 |
| Prince Edward Island | 3 |
| Nova Scotia | 63 |
| New Brunswick | 96 |
| Quebec | 191 |
| National Capital Region Quebec | 30 |
| National Capital Region Ontario | 156 |
| Ontario | 448 |
| Manitoba | 43 |
| Saskatchewan | 70 |
| Alberta | 106 |
| British Columbia | 196 |
| Northwest Territories | 0 |
| Yukon | 0 |
| Outside Canada | 5 |
| TOTAL | 1,426 |

## Assessing compliance

This was a year of constantly shifting ground: the federal government underwent a massive re-organization, new technological issues continued to emerge, and the Office completed its re-structuring to better respond to new priorities and increased workload.

In June the government announced it would eliminate or consolidate 15 departments and central agencies in order to streamline operations and improve efficiency. Since the Office's mandate includes auditing compliance of all federal institutions subject to the *Privacy Act*, the directorate created broad program envelopes to reflect the changes. The portfolios are Social and Cultural, Legal and Security, Economy and Environment, Government Services and Central Agencies, and one containing Transport, Canada Post and 12 other agencies.

New portfolio leaders will ensure that the Commissioner has resident experts able to conduct audits and special investigations, monitor new legislation and provide advice and training to departments. These officers will pinpoint privacy hot spots and concentrate their efforts and resources where they will have the maximum impact. Audits now concentrate more on issues than on departmental functions.

The Office has also combined policy planning with compliance auditing. This allows staff to diagnose trouble spots during audits and deal with them both in that agency and across government. Staff can also identify issues that require special research.

While adjusting internally, the directorate carried out seven departmental audits, 13 follow-up reviews of previous audits, nine incident investigations, two special studies and reviewed one audit completed by internal auditors of a Crown corporation—a full load.

Following are summaries of the common issues and trends found in audits and follow-ups, a brief summary of audit findings and recommendations, and several special incident investigations.

## Incident Reports

The number of incidents of lost, stolen or improperly disclosed personal information reported to the Privacy Commissioner is rising. Whether due to heightened sensitivity or more carelessness is unclear. Departments reported 12 incidents during 1993-94, compared to three the previous year. Of the 12, seven required the Commissioner to make recommendations to the departments, two did not violate the *Privacy Act* and three are under investigation. Following are some examples.

### Inmates receive others' files

Correctional Service Canada (CSC) notified the Commissioner twice that it had accidentally disclosed one inmate's personal information to another. In both cases staff made clerical errors while processing inmates' requests to examine their personal files. The error was compounded when no one noticed the discrepancies between the names on the request forms and the files. Considering the number of requests CSC processes, this does not happen often. However, it is a serious mistake which could jeopardize an inmate's safety.

Although existing procedures should have prevented the disclosure, the Privacy Commissioner recommended that CSC issue directives to all staff involved in processing inmates' personal information requests. Clerks who select the files will be required to check both the inmate's name and the Federal Penitentiary Service Number against the request form to ensure that they have the correct individual's file.

### RCMP investigates Immigration "brown envelope"

The Commissioner initiated an investigation of an improper disclosure following an April 29, 1993 article in the *Globe and Mail*. The article concerned a municipal politician's disclosure of personal information about illegal immigrants and refugee claimants to the journalist at a forum on crime. The politician apparently received a "brown envelope" of documents from an Employment and Immigration (EIC) employee. The documents included personal information from the Canadian Police Information Centre and listed foreigners who have been charged with various criminal offenses and who may have violated the *Immigration Act*.

Privacy staff confirmed that the documents contained personal information, had been under EIC's control, and the politician was not authorized to have them. However, EIC has asked the RCMP to conduct a criminal investigation so the Commissioner has closed his inquiry. EIC has also introduced measures to prevent similar incidents.

### Those tempting laptops

These small computers have become a tempting target for thieves because they are valuable, easy to carry and in high demand. Quite apart from their considerable worth, their memories are often packed with personal data, witness one machine stolen from a Veterans' Affairs employee's car. The computer contained the names, addresses, dates of birth, monthly income and the cheque amounts for 1100 beneficiaries of veterans' programs and the personal details of surviving relatives eligible for the benefits.

Later Veterans' Affairs reported a second theft—this time of two laptops during a break-in at one of their district offices. None of the computers was protected by the "Watchdog" security computer program because the department was waiting for a bulk

order of the software. Consequently, the information in all three computers could be accessed.

Of course, Veterans' Affairs is not alone. Several other departments have reported similar thefts. For example, Consumer and Corporate Affairs (now part of Industry Canada) has had 15 portable computers stolen since February 1992. According to security staff, several were new and contained no data, others were used primarily by Consumer Bureau inspectors and the data was not personal. CCA staff did not know whether the laptops were protected by security software.

It is unlikely laptops are stolen for their information. Nevertheless, departments would not think of allowing employees to store sensitive departmental records in unlocked cabinets. Yet employees may travel with the same data transferred to laptop computers without security software. Knowing their vulnerability to theft, this borders on negligence.

In the Veterans' Affairs case, the Commissioner concluded that it was impractical to notify so many clients (some of them deceased) of the possible disclosure. But he recommended that the department stop issuing laptop computers to personnel until the machines are secure. And it should be mandatory to activate the security measures while the machines are unattended.

**Pension Advocate files lost in move**

Last June, the Chief Pensions Advocate notified the Commissioner that the Ottawa District Office had lost three client files, probably during its move between floors of the building. The Bureau notified the individual subjects of the files. The loss appeared to be an isolated incident and not caused by an employee failing to follow established procedures. Nevertheless, privacy staff recommended additional measures to ensure the security of client files in any future moves.

### Farm Credit document found on street

Farm Credit Corporation (FCC) notified the Privacy Commissioner in February 1994 that a four-page document containing personal information (including the client's credit history) was found on a Regina street. The finder returned the document to the client, who was understandably upset. When FCC's internal investigation was unable to determine how the document came to be on the street, it asked the Commissioner to investigate.

Privacy investigators were no more successful. FCC had already apologized formally to the client and taken steps to reduce the chances of a recurrence. However, the Commissioner made several recommendations concerning fax transmission and physical security.

## Auditing institutions

### Canada Labour Relations Board

The Board is a quasi-judicial body which can grant, modify or terminate bargaining rights and resolve complaints of unfair labour practices under the Canada Labour Code. The audit was conducted at the Board's head office in Ottawa and at the Toronto regional office.

The audit found CLRB's personal information handling generally complies with the *Privacy Act* and its fair information principles. However, auditors identified several privacy concerns:

- Training is needed to fill a substantial information gap about the *Privacy Act* and what constitutes personal information.

- Personal information bank descriptions are incomplete. They refer only to information about employees and not Board members. In one case an entire EDP system containing case

management information is not described in *Info Source*. The entry should be amended.

- The central registry (where operational files are stored) should be locked when the office is closed to ensure that employees who work outside normal hours do not have unrestricted access to more personal information than they need.

- The Board should buy shredders for regional offices which now have no facilities to dispose of sensitive waste.

- The Board should develop procedures to verify transmission and receipt of its considerable traffic in faxed personal information between headquarters and regional offices.

- The Board does not accept that notes taken by members during hearings are personal information under the control of CLRB. This issue is the subject of an unresolved complaint investigation.

Another matter which remains unresolved is CLRB's authority to publish its decisions, which frequently contain personal information about the parties and witnesses. The Office has asked CLRB to demonstrate its statutory authority to disclose this information or show how the disclosure complies with the *Privacy Act*.

**Farm Credit Corporation**

The audit was conducted at the FCC head office in Regina and at the regional district offices in Moncton.

Audit personnel identified several privacy concerns, among them that FCC:

- make clear in its *Info Source* bank descriptions that FCC also uses personal information from farmers' loan applications in

hearings before the Loan Appeal Board and Farm Debt Review Board;

- improve its internal security. Privacy investigators found record room doors open, individual offices open, unoccupied and with computers on and personal documents left on desks;

- restrict supervisors' access to such sensitive employee personal records as medical information, financial records and payroll deductions unless there is a demonstrated "need to know";

- ensure that such records as rejected and cancelled loan applications and employee appraisal files are not retained beyond the National Archives-approved disposal schedule;

- ensure that all service contracts involving access to personal information (such as payroll, EDP software services and off-site storage) include provisions to protect the personal data;

- improve overall staff awareness of the *Privacy Act.*

FCC responded quickly to the Commissioner's recommendations and suggestions and has dealt with the concerns.

**Federal Business Development Bank**

The Federal Business Development Bank is a Crown corporation established to promote and develop the small business sector in Canada. The Bank is not subject to all Treasury Board rules and policies, giving it greater administrative freedom. In view of this, the Office modified its normal audit approach.

The Bank received high marks for protecting personal information from disclosure. Auditors also confirmed that the Bank collects only the information it needs to grant and administer small business loans. It gathers the information directly from the client and when it needs more information from other sources, it obtains

the client's written consent. The Bank also requires clients' written authorization before disclosing information unless to comply with a Court order or to collect an outstanding loan.

The audit did note some weaknesses. The Bank has not identified in *Info Source* all the information it collects about clients and employees, it has not described all its uses of the information, nor has it told them that they have the right to examine the information under the *Privacy Act*.

Auditors soon noticed several problems common to many federal institutions:

- managers have unlimited access to employees' files which may contain medical and financial information;
- staff know little about the *Privacy Act* even though they deal constantly with personal information;
- staff faxed large amounts of personal information between offices over open lines;
- there were no policies or directives on the privacy considerations of travelling with client files or laptop computers, and
- the Bank does not include privacy clauses in personal service contracts to bind contractors to the same terms and conditions as Bank employees.

**Labour Canada**

This audit investigated Labour Canada prior to its becoming a component of Human Resources Development Canada. The audit found Labour Canada's personal information practices generally comply with the *Privacy Act* and the fair information practices.

However, investigators raised three privacy matters during the audit.

The first concerns releasing decisions of unjust dismissal cases adjudicated under the Canada Labour Code. Labour Canada publicizes the detailed decisions in a monthly newsletter and on a computer disk. Cases are also printed in a privately produced manual.

Although the Privacy Commissioner recognizes the importance of a body of jurisprudence on unjust dismissal (and other labour matters), he does not consider it necessary to publicize the individuals' names and other personal identifiers. Removing the identification would not negate the usefulness of these cases as precedents yet would protect the privacy of the individuals involved.

The department has agreed to consider the Commissioner's comment.

The second matter is a recurring privacy issue—contracting-out to private companies work which requires access to personal information. Investigators found not all Labour Canada contracts contained adequate privacy provisions. The faulty ones were usually for less than $5,000 and had been initiated by local managers. They included contracts for temporary help or appointing arbitrators to handle various labour disputes. Contracts for larger amounts are routinely reviewed by ATIP staff and contained the proper clauses.

Labour Canada officials have agreed to include proper privacy provisions in all future contracts involving access to personal information.

Lastly, the investigation revealed very limited knowledge of the *Privacy Act* in regional offices. Although National Capital Region staff were more aware, this seems more the result of proximity to

the department's ATIP office rather than active promotion. After receiving the preliminary audit results, Labour Canada's ATIP staff has expanded distribution of its ATIP newsletter to include management team members. The unit will also sponsor additional courses on administering the Privacy and Access Acts to sensitize staff to their responsibilities.

**Internal audits—the Bank of Canada**

The Commissioner encourages departments to conduct their own internal privacy audits although few have done so. Most organizations have some internal audit capacity and adding personal record handling to the audit scope should not be onerous. Privacy staff provide guidance and review the results.

The Bank of Canada conducted the only internal privacy audit this year. Bank auditors' findings virtually mirrored what privacy staff have found elsewhere. Some personal information is kept longer than required and other information is not properly protected from access by staff with no operational need. The audit also revealed a need for the Bank to review its *Info Source* listings and to develop guidelines on using fax machines to transmit personal information. The Bank is correcting the shortcomings.

The Office's new portfolio leader will continue following the Bank's review.

## Following up

This year staff continued following up earlier audits to determine whether the organizations had implemented the Commissioner's recommendations. Investigators reviewed audits of 13 institutions and found that 41 of 53 recommendations (77 per cent) had been completely implemented, a slightly higher proportion than last year. Eight had been partially implemented and only four recommendations had seen no action at all.

The institutions reviewed were the Canadian Advisory Council on the Status of Women, the Canadian Cultural Property Export Review Board, the Great Lakes Pilotage Authority, the Export Development Corporation, Investment Canada, the Laurentian Pilotage Authority, the Office of the Commissioner of Official Languages, the National Capital Commission, the Security Intelligence Review Committee, the Social Sciences and Humanities Research Council, the Standards Council and the Status of Women Canada.

The organizations had responded to all recommendations about increasing staff awareness of the *Privacy Act*, primarily with training programs and, in one case, an in-house newsletter. They had also established formal contracts with third parties to protect the personal information entrusted to them, tightened procedures when transmitting information to regional offices, upgraded physical security measures, and paid closer attention to hiring cleaning staff.

Recommendations about the length of time some personal records were kept led three organizations to review disposal schedules with National Archives. Others added the necessary details to *Info Source*. Some institutions were in the process of reviewing old records and disposing of outdated material, including employee appraisals kept for more than five years.

In many instances, auditors had found the information bank listings in *Info Source* were inadequate or non-existent. In six cases the organizations had not made the changes. Keeping *Info Source* up-to-date is more than a paper exercise. The directory is individuals' key to exercising their right to access their personal information and correct errors. Incomplete or inaccurate listings mean the organization is also not meeting its other obligation under the *Privacy Act*—to spell out what information it collects and how the data is used and disclosed.

## Disposing of Computers

Information technology continues its frenetic pace, rendering computers obsolete long before they are worn out. When the old ones are carted off, their hard disks (where most data is stored) go along for the ride, often with massive amounts of data. Sometimes the data includes sensitive personal information—as a provincial government found recently.

An Alberta government agency sent a computer for service. The faulty hard disk was removed, repaired and subsequently sold in a local computer store. No-one thought to make sure the disk had been purged of data. It had not; the buyer found employees' personal information on his new disk and the story found its way to the media.

This could happen to anyone. Wiping the hard disk memory clean requires special software, a simple "erase" or "format" command is ineffectual. With the Alberta experience fresh in their minds, Office's auditors have checked the federal government's practice .

It is impossible to tell whether surplus federal computers have been sold with loaded hard disks because the process was changed recently. However, the Office's experience with surplus file cabinets (see 1992-93 annual report) makes one wonder. Obsolete computers—like other items—were once sold by the government's Crown Assets Disposal Corporation (CADC). However, CADC apparently did not check that hard disks were erased, that being the departments' responsibility.

In Summer 1993, the departments of Industry and Government Services set up the Computers For Schools (CFS) program with help from the Telephone Pioneers of America (Canada). The program collects obsolete computers at sites across the country, tests and repairs them, then donates them to schools. This process includes checking every hard disk and wiping it clean

using an RCMP-approved program. No computer is released with any data remaining.

It is fortunate that the CFS program does such a thorough job; service technicians report that about 95 per cent of all donated computers contain either data, old programs, or both. This despite government directives to departments to ensure the computer disks are clean. Given the poor job departments are doing now, only luck may have prevented embarrassing disclosures.

Aside from the obvious benefits of providing working computers to Canada's schools, the CFS program ensures that surplus computers memories are blank before leaving government hands. Nevertheless, government departments must accept the responsibility before this equipment is donated or sold.

# Corporate Management

Corporate Management provides administrative support services to both the Information and Privacy Commissioners. The services (finance, personnel, information technology, library and general administration) are centralized to avoid duplication of effort and to reduce costs.

The Offices' combined budget for the 1993-94 fiscal year was $6,819,000, an increase of $58,000 over 1992-93. Actual expenditures for the same period were $6,582,000 of which personnel costs of $5,230,000 and professional and special services expenditures of $565,000 accounted for more than 88 per cent of all expenditures. The remaining $787,000 covered all other expenditures including postage, telephone, office equipment and supplies.

Following are the Offices' expenditures for fiscal year 1993-94.

| | Information | Privacy | Corporate Management | Total |
|---|---|---|---|---|
| Salaries | 1,809,422 | 2,172,003 | 653,121 | 4,634,516 |
| Employee Benefit Plan Contributions | 243,950 | 267,750 | 83,300 | 595,000 |
| Transportation and Communication | 50,267 | 78,214 | 156,280 | 284,761 |
| Information | 24,100 | 47,775 | 1,383 | 73,258 |
| Professional and Special Services | 317,490 | 62,998 | 184,885 | 565,373 |
| Rentals | 10,854 | 294 | 12,797 | 23,945 |
| Purchased Repair and Maintenance | 8,300 | 1,533 | 2,620 | 12,453 |
| Utilities, Materials and Supplies | 23,634 | 15,491 | 36,602 | 75,727 |
| Acquisition of Machinery and Equipment | 84,185 | 80,955 | 140,833 | 305,973 |
| Other Payments | 9,587 | 1,182 | 75 | 10,844 |
| **TOTAL** | **2,581,789** | **2,728,195** | **1,271,896** | **6,581,880** |

* Expenditure figures do not incorporate final year-end adjustments reflected in the Offices' 1993-94 Public Accounts.

The Offices approved new policies on Official Languages and Deployment. The personnel unit continued its support of the Commissioners' plans to implement government-wide measures to simplify employment classifications and legislative reforms under the *Public Service Reform Act* (Bill C-26).

A number of security-related renovations were completed during the year. A new, secure reception area and a specially-designed computer room for the local area network file servers were constructed. In addition, a more effective assets control system was developed and implemented.

The Offices are using a recently-introduced computer network of Microsoft Windows-based tools and case management systems to support access to information and privacy investigations.

During the year, the library acquired 547 new publications and answered 1,246 reference questions. In addition to information on freedom of information, the right to privacy, data protection and the ombudsman function, the library has a special collection of Canadian and international ombudsman's reports and departmental annual reports on the administration of the two Acts. The library is open to the public.

# Organization Chart