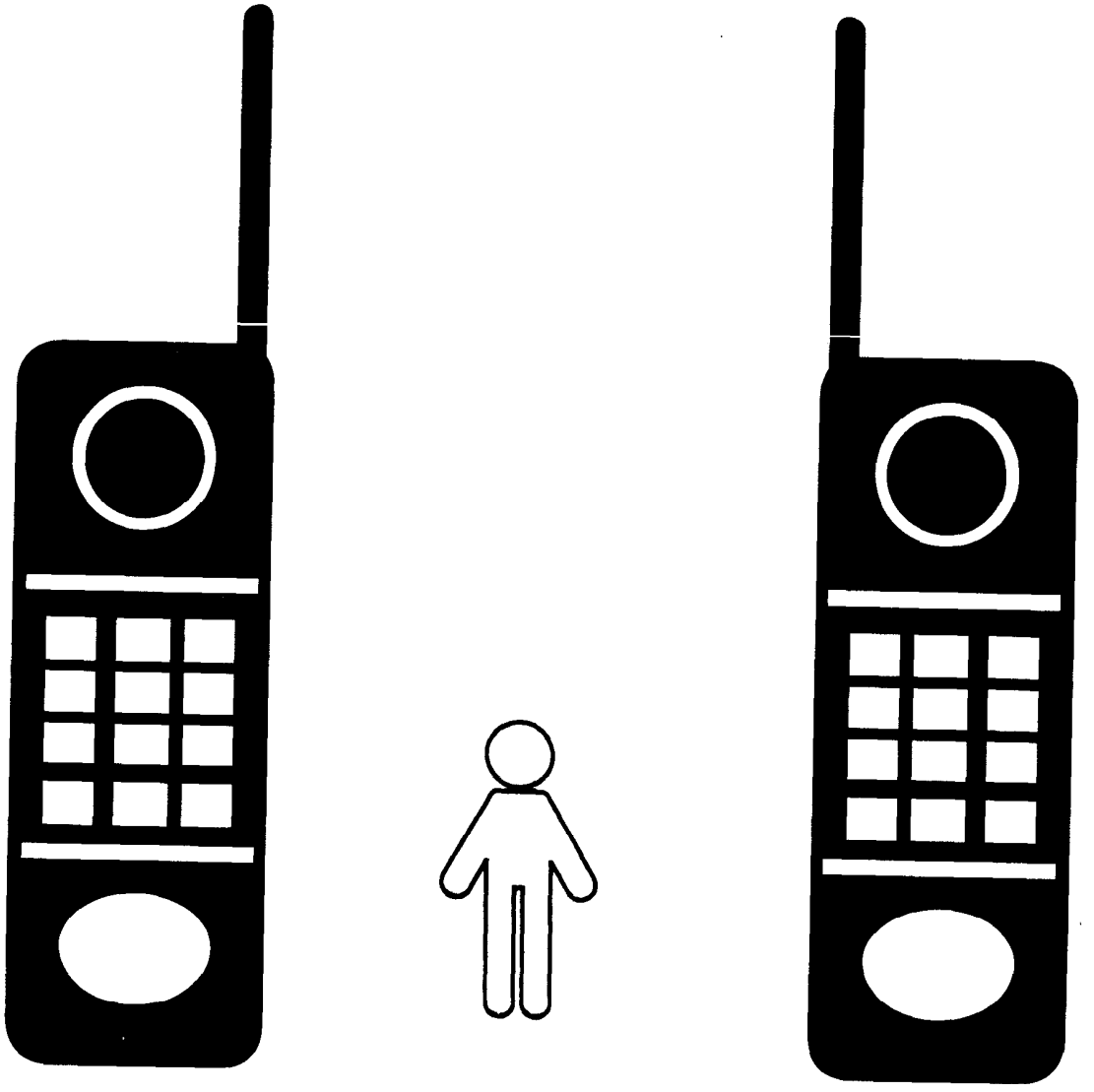
Privacy Commissioner

Annual Report 1992 - 1993



Annual Report
Privacy Commissioner
1992-93

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 30-1/1993
ISBN 0-662-59840-7

This publication is available on audio cassette.

The Honourable Guy Charbonneau
The Speaker
The Senate
Ottawa

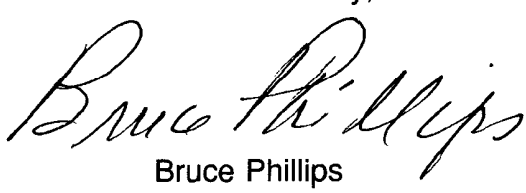
June 30, 1993

Dear Mr. Charbonneau:

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

This report covers the period from April 1, 1992 to March 31, 1993.

Yours sincerely,



Bruce Phillips
Privacy Commissioner

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

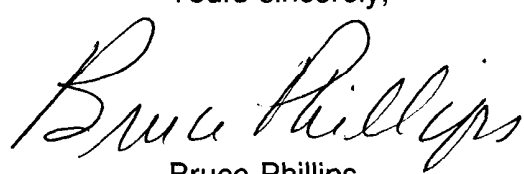
June 30, 1993

Dear Mr. Fraser:

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

This report covers the period from April 1, 1992 to March 31, 1993.

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.

Table of Contents

Ten Years After 1

Rising to the Technology Challenge
- Delivering service electronically 13
- A privacy checklist 14
- Other works in progress 16

Privacy on the Hill
- Protecting cellular calls 19
- Telecom privacy principles 20
- Amending the *Income Tax Act* 22
- Privacy in Banking 25

...On the Streets
- *Privacy Revealed: the Canadian privacy study* 27

...In the Courts
- Privacy Commissioner vs. Canada Post 29
- SINs for birth registration 30
- Patient access to medical records 31

...In the Labs
- Biotechnology update 32

...Here and There
- In the provinces 37
- Overseas 39

...In the Private Sector
- The CSA model Code 43
- CDMA privacy code 44

...In the Office
- Investigating Complaints 45
  - How institutions measured up 45
  - Notifying the Commissioner 48
  - Inquiries 54

Table of Contents

Some cases 57
Tables and charts 70

...In the Office
Assessing Compliance 75
Special investigations 75
Institution audits 77
Following up 81
It's 1993—Do you know where your information is? . . 85

Corporate Management 90

Organization Chart 92

Ten years after

Publication of this report falls on the tenth anniversary of the coming into force of the federal *Privacy Act* and with it the creation of the Office of the Privacy Commissioner. The question naturally posed by such an occasion, of course, is whether the birthday is a happy one.

Let us acknowledge the truth that any anniversary which the subject is still around to observe has something going for it. And certainly the progeny shows signs of promise. All the same, we're disinclined to break out the cake and champagne.

Call the mood one of subdued satisfaction. The office is gratified at having given ten years of useful service helping Canadians exercise their privacy rights in their relations with the Government of Canada. That service includes more than 7,500 investigations completed and findings rendered, almost 25,000 inquiries received and answered, and major audits of about one-third of the government's information holdings conducted—no small achievement for an office which has never held as many as three dozen persons.

Despite the sceptics' direst predictions, law enforcement has not ground to a halt, there has been no sweeping abandonment of honest record-keeping and departments have not found themselves repeatedly before the courts. Nor have individuals' requests to examine their personal information yet brought any department to its knees (although until it changed its policy, privacy applications had National Defence reeling).

In fact, the *Act*, the complaints and audits have prompted many government institutions to better identify, organize and fine-tune their record-keeping—no small benefit in an era when virtually all government agencies have converted to electronic information systems.

And this Office can lay some claim to stimulating public debate about data matching, control of the Social Insurance Number, the

privacy implications of biotechnology, privacy principles in telecommunications services, controls on cellular telephone eavesdropping, privacy regulations in the financial sector and entrenching privacy rights in the *Charter*.

Many of these initiatives demonstrate graphically the changing role of this tiny office. Mandated (and funded) only to investigate complaints against 160-odd federal institutions, the Commissioner is under pressure from Parliamentarians, the public and media to answer their privacy questions, to comment on the privacy implications of new programs and legislation, to appear before committees, and to speak out on the issues beyond his narrow mandate. To refuse is to court irrelevancy. To accede is to risk insolvency. Parliament's privacy ombudsman strives to meet the demands but the budget is reaching crisis point.

However, the climate of fiscal restraint has far broader privacy implications. Pressured to rationalize programs, improve service and cut costs, the government is aggressively pursuing ways of conducting much of its business electronically. Direct deposit of benefit cheques is just the beginning. Already the federal government is using electronic data interchange (EDI) to collect GST and personal income tax, to document immigrants and refugees and collect customs duties at the borders.

One proposed new system is an interactive network of government information kiosks ("Infocentres") which will allow clients to get information about government services, check job openings, apply for various programs and send change-of-address notices to participating departments. Once in place, the network can be substantially expanded to become a one-stop shopping centre for federal government services.

These new electronic systems make a qualitative change to government information handling, including three ominous characteristics. The first is the need to have an identification card to receive the services, implying personal identification numbers,

probably photographs and, quite possibly, fingerprints or some other biometric identifier.

The second is the likely private sector involvement in any electronic interchanges of personal data–a sector without any legislated privacy controls.

Finally, the costs of developing and delivering these new services could demand government consolidate its programs across departments—and perhaps even across federal-provincial jurisdictions. The walls between databases may come tumbling down, raising once again the spectre of the single government file—or profile—and the spectre of Big Brother.

There is no shortage of work for a privacy commissioner.

In a "technological trance"

Any remaining temptation to celebrate is more than offset by an acutely painful awareness that increasingly we know only enough to realize how little we know. The office spends a good deal of time fighting fires. And in the wider world beyond the federal government and the limited reach of the *Privacy Act,* birthday celebrations may be premature.

Viewed in that wider context, several developments in the past decade have effectively laid siege to privacy:

- the explosion of computer technology, leaping from powerful mainframes, to personal computers, to electronic notebooks—each step bringing smaller, more mobile, more powerful and more accessible tools capable of being linked around the world, and the increasing sophistication of computer software;

- Western societies' uncritical acceptance of technology—including no systematic consideration of its impact

on individual rights. We are in what has been described as a "technological trance"—technology drives individuals' rights rather than the other way around and the response, both in the private and public sectors, has been sporadic, tentative, and only marginally effective;

- the rapid evolvement of biotechnology from a tool aimed at improving human health, to a powerful commercial and political weapon with an ominous potential for social surveillance and control;

- the "commodification" of information—the packaging of information as a commercial good which in an increasingly competitive business environment is seen as lighting the path to economic competitiveness.

And threats to informational privacy are only one part of the global privacy problem. Growing encroachments on physical privacy and increased physical surveillance round out the dilemma. Although perhaps beyond the general focus of this report on privacy of information, they form crucial elements of the chemistry of intrusion.

How long will it be before calls for better crime prevention put cameras at major street corners in our urban areas? In the name of suppressing crime, Canadians may see their own lawful movements monitored by the state. Perhaps Orwell was not wrong.

And the increasing use of technology to monitor workers is another omen. With each new form of surveillance we become less like individuals and more like automatons, monitored for defects and aberrant behaviour that will consign us to the reject pile or mark us for "corrective" measures.

Some experts feel that the game is already over, that technology has laid bare the life stories of us all, that Canadians should

consign the concept of individual control to history, stop worrying and learn to live with and love the free flow of information.

Privacy revealed

Thankfully, public awareness of the impact of technology on privacy has also grown during the past decade. One useful development was the release in the Spring of 1993 of the first major national study of public attitudes on privacy issues. The study provides the first hard statistical evidence that Canadians are alive to the privacy issue—incontrovertible proof if any were needed that privacy is not some elitist concern or fringe issue. The fact that 52 percent of the population voices "extreme concern" with the state of personal privacy ought to satisfy the most sceptical lawmaker or regulator. There is a strong public consensus on giving privacy a higher priority on the policy agenda.

This survey, sponsored and financed by a consortium of private and public sector organizations (including this Office) also revealed that Canadians know what they need to protect their privacy in an information society. An overwhelming majority said they want some control over the gathering of information about them; to be told in advance when it's being collected, by whom and for what purpose, and to have the right to consent to or refuse any transaction involving information about them. In short, they want those things that are the foundation of fair information practices, and which are absent from so much of today's traffic in personal data.

The Canadian public has thus grasped the essence of the privacy issue in the information age—personal control over the information which others know or can learn about them. The survey reveals a widespread sense of uneasiness; 61 per cent **strongly** agreed that "consumers have lost all control over how personal information about them is circulated and used by companies." And 60 per cent agreed that they have less privacy in their daily lives than they did ten years ago. Those whose business is studying

this matter know only too well how justified Canadians are in harbouring that belief.

Canadians are familiar with some highly-publicized privacy disasters including those resulting from monitoring and disclosure of cellular telephone conversations. But, in all probability, this is decidedly minor-league compared with the personal information about them that is routinely exchanged over computerized data bases and easily available to persons whose right to the information is, at best, debatable.

Thanks to numerous congressional investigations, and a fairly aggressive media community, a considerable body of knowledge has developed in the United States detailing the scope and nature of information trafficking through computerized data bases. Horror stories abound. For example, in one of the latest works, *Privacy For Sale*, author Jeffrey Rothfeder (himself not a computer expert) relates how, with little difficulty, he gained access to the credit reports of former U.S. Vice-President Dan Quayle and television anchorman Dan Rather.

He also recounts how every resident of a small New England town was listed as a tax evader by a credit reporting company, thanks to a computer input error. None of the 1,500 persons knew about this damning but inaccurate information until one of them, an affluent physician (presumably unused to being denied credit) looked into the matter.

Given the similarity in Canadian and U.S. business practices one must assume the very real possibility of similar events taking place in Canada. Just to cite a few recent examples culled from the media:

- a grocery chain began issuing "smart cards" to provide discounts to customers but neglected to tell them that their spending habits would be profiled and sold to direct marketing companies;

- a company given sensitive medical files to destroy, sold the documents to a television production company where they were used on camera as props;

- eight employees of a credit reporter misrepresented themselves as Revenue Canada employees to trace customers owing money to a provincial utility;

- a chartered bank released clients' card numbers, names, addresses and other personal data to a market research firm to test demand for new products;

- a man checking the accuracy of his credit file found several inquiries about him from a lawyer in a province where he has no business or personal contacts. He has no legal recourse because there is no national credit reporting legislation and no privacy protection in the private sector;

No-one reading any of these stories can rest easily.

Leaving a "datashadow"

Ten years ago, the first annual report of this office observed:

> ...it has become trite to say that personal privacy is threatened as never before in human history...The confluence of new technologies with ever-insistent claims of the state to know, to be efficient, or both, has changed the qualitative and quantitative nature of the problem.

If the threat was so well understood and clearly visualized 10 years ago, what does it say about the situation today? It says that, with limited exceptions, the situation is decidedly worse. Everybody is acquainted with the enormous increase in direct marketing, for instance—the floods of advertising mail, the nightly phone calls. While these are nuisances (and some would argue, easily dealt with) they depend on access to highly-detailed

personal profiles of customer prospects. Yet how many of us know what is in those profiles, or where the information came from, or who has them, or how accurate they are, or how secure they are, or, what is worse, to whom they might be sold? Not many.

The fact is, ten year's technology has transformed the inherent value of personal information. Every scrap of data about us, from such mundane "tombstone" information as name and age, to lifestyle data such as shopping habits or movie preferences, to such detailed medical information as our genetic makeup, is useful to somebody. Technology has furnished us with the tools to buy, manipulate, re-constitute and sell the details of others' lives for a profit. Under the harsh glare of all this electronic scrutiny Canadians leave a "datashadow"—a trail of personal details and transactions which they cannot control.

Consider the privacy implications of just two new technological developments: powerful new national information networks and the new personal communication devices. The first, the Canadian Network for the Advancement of Research Industry and Education (CANARIE) is a national initiative to stimulate creation of a high-speed digital network by the year 2000. The network will use optical fibres to connect the public and private sectors and citizens coast to coast. The federal government alone has earmarked millions of dollars over the next five years for the project. In five years, the amount of data being transmitted over electronic networks will grow 2000-fold. In effect, networks like these will transform information flow in the same way the transcontinental railroad did the flow of people and goods a century ago, and as modern highway networks did in this century.

The optical superhighway will revolutionize communication, carrying on its hair-thin glass fibres not just the words in electronic messages and computerized medical records but even such images as X-rays and Electrocardiograms.

The next five years will bring yet another new telecommunication tool; personal communications networks. These networks will redefine how Canadians use the telephone. Numbers will be assigned, not to locations, but to individuals. Calls will be routed through radio transmitters, satellites and computers, tracking down the recipient and feeding the communication. And the new devices will be capable of handling voice, audio, text and graphic display.

Useful as these devices may be, there are looming privacy problems. Not only is the content of the call at risk—this is wireless communication after all—but the more insidious invasion is the potential for surveillance. One has only to place a call and the telephone company will know (and the billing records will show) where both caller and recipient were, and when. Will these records be available to government? To police? Will they be sold for marketing purposes?

Facing the music

Must we continue to argue about the desperate need to get a better handle on the business of information? Trailing far behind in the information race is any effort to produce some reasonable respect for the rights of the individuals whose personal information is the raw material for this industry. The ten years since the first privacy commissioner drew attention to the "threat" have seen the gap between problem and solution yawn ever wider.

Frankly, it is becoming tiresome to hear people with a vested interest in unfettered information flow exclaim how "difficult" it is to protect privacy, when one suspects what they really mean is how "inconvenient."

One cannot fail to observe how readily solutions are found when specific cases force their way onto the public agenda. The recent example of intercepted cellular telephone calls leaps to mind. Once some sensitive political disclosures thrust the vulnerability of

these devices on politicians and the public, the legislative machinery was remarkably quick to propose a remedy.

So the evidence that solutions exist is recent and graphic. What is needed now is the will to deal with the issue in more than piecemeal fashion. One lesson the past ten years has taught: the pace of technological change makes unworkable proposing technical fixes for each new tool. We cannot envisage where technology will lead. What is needed is a privacy framework—a set of principles against which the new products and services can be measured.

These observations in no way denigrate or diminish the value of much useful work now being done. On the contrary, the last annual report and this one draw attention to encouraging developments. Indeed there has been commendable action on several fronts which we report later. But the time has come for a more aggressive and co-ordinated approach to the problem of reconciling privacy protection with the informatics revolution.

Canadians are entitled to respect for their privacy no matter what government jurisdiction, no matter what industry sector, and no matter what technology. The Commissioner pressed strongly during the recent constitutional debate for entrenching in the *Charter* an explicit right to privacy. But there were other priorities. Nevertheless, it is imperative to develop a set of principles to secure those rights. These principles should include:

All governments should recognize that every Canadian is entitled to the data protection rights expressed in such documents as the OECD privacy protection guidelines and the federal *Privacy Act*.

Broadly speaking, this means that personal information should be collected only when truly warranted, used only for the purposes set out beforehand, disclosed only in narrowly defined circumstances and accessible to the individual it concerns,

including the right to ask for correction. And the mere words in codes or statutes are not enough. Governments must be willing to establish a means of ensuring compliance with these tenets.

All governments should recognize that such privacy rights should apply to public and private sector alike. Where such rights do not exist, the obligation rests with government to secure them.

All Canadians are entitled to be fully informed about the potential impact of technology on their lives—what information is involved, what will be done with it—and how to regulate the use of technology.

A commitment of this kind necessarily implies greatly improved public education. It also requires coordinated federal and provincial efforts to marshall the expertise capable of understanding and explaining the implications of technology on personal privacy. An equivalent to the U.S. Office of Technology Assessment might be a good starting point. The OTA helps legislative policymakers anticipate and plan for the consequences of technological change, and examine how technology affects people's lives.

The objective now should be to strengthen and extend the protection. Obviously, where more than one jurisdiction is involved, there must be leadership. It seems equally obvious that the government of Canada is best positioned to provide it. The Commissioner recommends that Parliament take steps to develop a national action plan aimed at achieving the objectives set forth in the proposed principles.

The issue, remember, is not whether technology will continue to change our lives. It will. The issue is whether the changes will be governed solely by what the technology itself makes possible, without regard to the consequences for timeless and deeply-held values such as respect for individual autonomy and privacy.

All technology, from the invention of gunpowder to nuclear fission, has had the capacity to serve ends both ill and benevolent. The computer is no different. The decision, as always, is ours to make. But we no longer have the luxury of time—the next ten years could tell the tale.

Rising to the technology challenge

Delivering services electronically

The next decade will challenge all governments to be more accessible to their taxpayers; to provide information, services and benefits directly to the individual—all at a time of eroding resources. The federal government's strategy to meet this challenge is to enhance its services by innovative use of interactive technologies.

Given the range of programs and services the government delivers, the issues are complex and the investment costs enormous. And new technological advances often threaten to undermine individual control of personal information and to erode the protection offered by privacy laws.

The federal government has recognized that, until now, technology and the technologists have operated in isolation to drive personal information management. But that is about to change. Government now acknowledges that technology simply offers us choices and that human values—including privacy—must be a part of developing and applying new information systems.

To begin with, the government has created an electronic services initiative secretariat within Treasury Board to develop a coordinated vision and framework for introducing new electronic services. The secretariat will help departments use technology as their primary means of renewing services, determine what services can be delivered electronically and provide guidance on how best to implement that technology.

Recognizing this Office's ongoing concern and interest in the issue, Treasury Board has invited the Commissioner to work in partnership, providing advice on protecting personal information in the development of new electronic services and communication systems.

The invitation (gratefully accepted) recognizes the legitimate place for privacy in the debate. Reasonable privacy protection is not incompatible with technological change; there simply must be a convergence of disciplines that will build human values into the design and application of new systems.

The Office also hopes to work with government officials to establish an interdepartmental working group on privacy and technology.

As a first step, the Commissioner has proposed a "privacy checklist" to guide senior government officials during the design stage. While the search for a "framework" goes on, the proposal would at least ensure respect for clients' and employees' privacy. What follows is an informal sketch of some of the issues that need to be considered.

A Privacy Checklist

Openness/Transparency: Individuals must be thoroughly informed of their rights under the new technologies. Before introducing new systems, government must notify the public about the development, its objectives and extent, the type of data to be collected and used and the individuals who will be affected. Those individuals should also be given specific notice of their right to refuse to participate; to know what information is involved in the technological process; and to be made aware of the situations likely to develop around the use of the technology.

Informed Consent: Individuals must be informed clearly and their consent obtained for all uses and disclosures of the information being processed. Individuals should also have the right to withdraw consent for uses or disclosures without penalty.

Gate Keeping: Security measures must prevent misuse or inadvertent access to individuals' data. This means incorporating

a combination of personal identification numbers (PINs) with internal security mechanisms for individual transactions.

Matching: Systems shared by several users should be segregated internally to prevent possible merging or cross-over of personal information during any transaction. All transactions must be secure to and from the host computer.

Access: Individuals must have the right of access to and correction of the information held about them as a result of any transaction.

Non-Discrimination: New technologies must not limit the government services offered to a client and services offered electronically must respect the universality of government programs. (However, it is evident that even when participation is voluntary, participants may enjoy such advantages as faster service or service after normal business hours.)

Beneficence: Government must acknowledge and affirm that new technologies are tools to help deliver service to individuals—**not** instruments to enable it to exert control over individuals' information. (Of course, there are exceptions for the legally-mandated authority of government to properly control and administer its programs.) Government must resist the temptation to use any technology to conduct overt and covert surveillance on its citizens.

Respect: All intermediaries must respect the principles of privacy ethics or laws—all participants in the process must be made aware of and adhere to those principles.

Responsibility: Those entering information into systems must exercise the highest standard of responsibility to ensure the reliability of the system.

The checklist may strike some as a tall order—it may mean additional steps. But the privacy agenda can be incorporated into the technological arena in a way that will ensure taxpayers both improved government service and enhanced privacy protection.

Other works in progress—smart cards

This privacy checklist is drawn largely from *A Privacy and Smart Card Framework*, prepared by this Office as part of a users guide for the federal working group on implementing smart card technology. The paper sets out both an ethical framework for using smart cards as well as standards and guidelines that will take privacy protection into account in the applications design of smart card systems.

The working group is attempting to identify the possible government applications for smart card technology and to suggest an operational framework in which the cards would function.

The Department of Communications (after an earlier and unsatisfactory brush with the technology in its infancy in 1988) has begun several pilot projects. These include using the cards to control inventory of expensive high tech equipment at its Communications Research Centre and to replace the in/out employee board at the Canadian Conservation Institute. DOC also plans to use smart cards as electronic "money" in its stockrooms. The card will be loaded with an amount and each purchase will be deducted from the balance and the transactions recorded electronically.

DOC is also considering using smart cards to store employees' passwords for access to various computer systems. Employees will have to remember only their personal identification number which will give them access to their various system passwords. The passwords will be protected by the card's encryption capabilities.

Given the cards' ability to validate identity, employment status and security clearance, the most likely government-wide application of the technology is an employee card. The challenge will be to ensure it does not become a tracking device. However, the Office is convinced that government can devise standards and guidelines that will harness the technology, improve program delivery and still respect individual privacy.

Telework

The smart card group is just one of a number of committees on which privacy staff are working. Another is the Telework project committee. This committee will assess the results of a three-year pilot project to allow some employees to work at home and send the product to the employer electronically.

The government has recognized that information technology can help us deal with wider social issues such as allowing employees to achieve a better balance between their work and personal lives, as well as reducing energy consumption and pollution and easing traffic congestion.

The government has also acknowledged that while working at home can be beneficial, it also has some privacy implications. How will government protect clients' (and other employees') personal information while it is off the premises or in transit? And how will it ensure that working at home does not compromise employees' private home life?

Security safeguards for personal data must equal those provided at the work site. How much security will depend on the sensitivity of the personal information and the protection provided by each government agency. Clearly some agencies will allow teleworking with personal data; others will not.

The committee will examine the results of the project and its implications (not just for privacy). Its report is expected in late 1995.

Public Service Compensation System

The Office will also review the new public service compensation project, a huge single database to store the pay and benefit information of all federal employees and pensioners. The implications of a single database are substantial; linking and merging of data, movement of data between departments, need for security safeguards and restricting access to those who need to know. The challenge will be to ensure that this system does not become the single, all-inclusive government profile.

Privacy on the Hill

Telecommunications and privacy has been a recurring theme in these pages for several years. Again this year there are important developments to report—new legislative provisions to enhance the confidentiality of cellular communications and the Department of Communications' publication of a set of telecommunications privacy principles. Two other legislative initiatives get mixed reviews: the struggle for privacy regulations in the financial sector and amendments to the *Income Tax Act*.

Protecting cellular calls

In his 1990-91 annual report, the Commissioner alerted Canadians to the growing threat to privacy posed by interception of cellular telephone calls. Two highly publicized cases—one concerning a British Columbia cabinet minister who resigned after a newspaper printed extracts from calls he made on his car phone and suspicion that cellular communications were intercepted during the Meech Lake Conference—served to illustrate the point.

The Commissioner urged Parliament to act quickly to protect the privacy of cellular phone users.

There is good news to report. Last December the government introduced Bill C-109, amending the *Criminal Code* and the *Radiocommunications Act* to make it illegal to intercept private cellular phone conversations maliciously or for gain, and to provide for both civil damages and criminal penalties. The *Criminal Code* amendments also expand the definition of a private communication to include encrypted radio based communications.

Although the amendments do not ban cellular scanners, nor do they make it illegal to eavesdrop on cellular calls, they do give cellular telephones some of the protection of conventional "line-based" telephones.

Much as the Privacy Commissioner would like to take some credit for catalysing the legislative process, he suspects the intercepted

Wilhelmy-Tremblay call during the constitutional negotiations (and the ensuing media attention) did more to concentrate legislators' minds.

Some will argue that these measures do not go far enough because they do not ban scanning devices, an approach taken in the United States. While the Privacy Commissioner might prefer the American approach—and its clear statement that the interception itself is wrong—he is nonetheless gratified with any legislative measures to enhance the privacy of Canadians.

Telecom Privacy Principles

The second significant development in telecommunications this year results, in part, from an item in last year's report which discussed the privacy impact of new technological advances and the seeming futility of trying to devise technical solutions for each new technical marvel. The Office had begun work on broad privacy principles and commended this approach—borrowed from New York state—to the Department of Communications in December 1991, and to the Senate Transportation and Communications Committee in June 1992.

The combination of the Communications minister's commitment and his department's resources and expertise have produced a framework of privacy principles to guide the telecommunications industry. These principles emerged for the most part out of two significant events.

First, Bill C-62, the proposed new *Telecommunications Act* was introduced in February 1992. It sets out as one of eight policy objectives for the government:

> "... to respond to the economic and social requirements of users of telecommunication services, including the protection of the privacy of individuals."

Second was the caller I.D. decision by the CRTC. This decision, a reversal of an earlier verdict, put to rest perhaps the most controversial issue arising from the introduction of Call Management Services by the telephone companies. In the end, the CRTC required all companies in its jurisdiction to provide free per-call blocking for callers who did not want their numbers displayed.

Caller ID and cellular telephones are two good examples of the double-edged nature of technological advancement. In each case, important benefits and conveniences were made possible by new technology but, without some special arrangements, both carried with them significant potential loss of personal privacy. With privacy principles to guide it, the CRTC might have foreseen the problems with Call Management Services and dealt with them during the first review. This would have avoided the fuss and the need to review and overturn its earlier decision.

To implement the principles the minister has chosen a voluntary approach. There are obvious benefits. One; it allows industry to tailor a privacy protection framework that will suit its specific needs. Two; it provides a solution that transcends jurisdictional boundaries—all players whether private, public, provincially regulated, or federally regulated can participate. Three; it will be jointly funded by public and private concerns.

Key to the department's partnership approach is two bodies: a telecommunication privacy foundation and a telecommunications privacy council. The foundation will bring all the players together; the council (representing industry and consumers) will receive and adjudicate complaints.

However, this approach lacks specific statutory underpinnings and does not establish an independent dispute resolution mechanism—two elements necessary for an unconditional endorsement by the Privacy Commissioner.

Nevertheless, if industry commits to this approach, it may provide an adequate privacy protection framework. The Communications minister announced his willingness to consider a legislated solution if there is no support for this concept. With that added caveat, the Privacy Commissioner supports the initiative.

Amending the *Income Tax Act*

The Privacy Commissioner was also interested in amendments to the *Income Tax Act* and *Excise Tax Act* (bills C-92 and C-112). If enacted, these amendments would allow any Revenue Canada, Taxation official to use taxpayer information to supervise, evaluate or discipline a departmental employee.

The Commissioner raised two important concerns about these proposals. First; they designate Taxation employees as a new class of federal employee, subject to government monitoring and controls that differ from those of other employees. And second, they diminish existing confidentiality rights of all taxpayers because their files could be used in proceedings unrelated to the income tax process.

However, safeguards were included in the latter case to protect the confidentiality of taxpayer information in legal proceedings. The safeguards provide for in camera hearings, banning the publication of the information, concealing the identity of the taxpayer, and sealing the record of proceedings. Such a use of their files may, nonetheless, come as a surprise and source of concern among many taxpayers. The Commissioner recommended that prior to implementing such a system, Revenue Canada should consider acquainting taxpayers with the change.

Of greater concern was the first proposal designating Revenue Canada employees as a special class. Although the Commissioner recognizes the need to ensure the integrity of the tax system, he considered the proposals, as drafted, apply too broadly and open up the potential for abuse of employees' privacy. They could be

interpreted as allowing a supervisor the arbitrary power to retrieve and examine an employee's tax return at will. Thus, for example, should a Taxation employee be involved in a grievance proceeding against a supervisor (on matters unrelated to income tax collection), the supervisor could examine the employee's tax return and use it to threaten or intimidate.

Some occupations and professions often demand different or enhanced standards of behaviour of their members. However, the Commissioner thought that Taxation could achieve the desired level of integrity without resorting to such broad measures.

For example, the department could establish stringent criteria under which the management could examine employee tax files. It could define conditions of reasonable cause to avoid the potential for fishing expeditions in employees' personal and sensitive files.

As well, the department could devise a protocol allowing only senior program officials (not supervisors or personnel staff) to review employee files and determine whether to release information for the personnel uses envisaged. Revenue Canada should not contemplate such examination and disclosure for routine supervision and evaluation but only "for cause" to be defined in law.

At best, the present proposals represent a derogation from existing privacy rights without a corresponding protection of the employees' interests. Such measures should not be taken lightly and certainly not without a full and open public debate. They create the potential of a privacy underclass of citizens whose legitimate concerns are equally as important as the integrity of the taxation program. The privacy of their files is a priority consideration for Taxation employees. Any system that envisages diminishing that privacy demands stringent safeguards. A balance is necessary.

This apparent lack of balance between competing interests was not lost on members of the Commons Finance Committee. The amendments were initially voted down by the committee, but reinstated at the report stage by the government.

In letters to the Privacy Commissioner and the Committee, the department acknowledged that the proposals fundamentally alter existing confidentiality provisions, but insisted that

> It is our duty to ensure that Revenue employees conduct themselves in a manner appropriate for persons who have privileged access to the tax system. While the vast majority do, it would be unfair to other taxpayers if a Revenue employee who had abused the system or who was demonstrably incompetent was shielded from normal disciplinary action simply because the relevant tax-related evidence could not be used or provided.

The department argued that the amendments provide additional privacy protection since taxpayer information could only be used if it is **relevant to**, and **solely for** a purpose related to supervision, evaluation and discipline. As well, the department proposed to issue guidelines to deal with the Privacy Commissioner's objections. Officials assured the Commissioner that both he and union officials would be consulted on the guidelines before they are finalized and implemented.

The Commissioner accepted the department's offer to work on a set of mutually-agreed safeguards, in cooperation with the public service unions concerned. This will mark the first time this Office has worked directly with a department to improve the privacy aspects of its employee administration process. The results seem certain to be of interest both to the bureaucracy and to Parliament. Pending the outcome, the Commissioner acknowledges Revenue Canada's ready response to his concerns.

Two further amendments also caused the Commissioner some concern; those to section 241 of the *Income Tax Act* proposing that an official "may" provide access to taxpayer information for the purposes of section 45 of the *Privacy Act* (and similar wording for section 295 of the *Excise Tax Act*). These provisions could have been interpreted to mean departmental officials had the discretion to refuse to disclose taxpayers' information to the Commissioner's staff during a complaint investigation.

Revenue Canada agreed that these sections should be interpreted simply as enabling department officials to allow the Privacy Commissioner to carry out his duties without Revenue Canada being in breach of those sections of the *Income Tax Act* or the *Excise Tax Act*.

Privacy in Banking

The Commissioner reported last year that a great divide may have been traversed with the introduction of two pieces of legislations—a bill dealing with banks and financial institutions, and a new Telecommunications law. As reported earlier, recent initiatives now offer more than a mere glimmer of hope that privacy will be adequately protected in telecommunications. The news is not as encouraging for the banking provisions. They seem to be snagged somewhere along the divide.

In April 1992, the Commissioner appeared before the Senate Banking Committee to urge Parliament to seize the opportunity to draft regulations that would protect privacy in the banking world. The Committee was quick to pursue this suggestion and with the help of Professor David Flaherty of the University of Western Ontario drafted a set of regulations. These regulations are based on existing *Privacy Act* provisions but adapted for the banking industry.

As promised, the Commissioner was invited to reappear before the Committee last December. He reiterated his strong support for

embodying basic privacy protection standards in the legislation. As well, he contended that no privacy protection scheme could command public confidence without an independent dispute resolution mechanism—one with the power to investigate complaints and to review both the information holdings and information management practices of the financial institutions. As of this date, the Senate Committee has not issued its final report.

A strong private sector lobby led by the Canadian Bankers' Association advocates a completely self-regulatory approach. The Commissioner while no great fan of government intervention for its own sake, continues to believe that basic common standards and independent oversight are necessary to guarantee fairness and transparency in this field.

Privacy revealed: the Canadian privacy survey

For the first time in its ten-year history, the Commissioner's office has reliable analysis of Canadians' expectations, knowledge and fears about their privacy—and they feel "under siege."

The results of the first broad spectrum study of Canadians' views about privacy are long overdue. They are dramatic confirmation of people's awareness and concern about the threats from technological, commercial and social changes.

Ninety-two per cent of Canadians expressed some concern about their privacy—52 per cent were "extremely concerned"—comparable to extreme concern about the environment (52 per cent) and unemployment (56 per cent) and well ahead of worries about national unity (31 per cent).

The majority of Canadians (60 per cent) feel they have less privacy than they did a decade ago—40 per cent feel "strongly" that their privacy has eroded. Four out of five respondents said that computers are reducing our privacy and 54 per cent are extremely concerned about the linking of personal information from one electronic data base to another.

Perhaps the most startling finding for the Commissioner's Office is that, whether or not they have ever read a privacy act or heard of a privacy commissioner (and as the survey says, few have) Canadians have put their fingers on the fundamentals of privacy protection. And the watchwords are knowledge, control and consent.

One of the key patterns evident in the findings is the greater the respondents' sense of control and knowledge of the process, the greater their level of comfort. This need to participate and control is evident in the following findings:

- 81 per cent feel strongly that they should be notified in advance when information about them is being collected;

- 83 per cent strongly believe that they should be asked for permission before information about them is passed from one organization to another;

- 87 per cent strongly agree that when information about them is collected they should be told what it will be used for;

- 72 per cent said that being in control of who can get information about them is extremely important, and

- 67 per cent feel controlling what information is collected about them is extremely important.

The survey (entitled *Privacy Revealed*) also revealed a very strong desire for action. Although respondents were prepared to consider some creative approaches such as partnerships between government and business—and also to take responsibility themselves—it was clear that pure self-regulation by business (the status quo) was the least acceptable at 26 per cent. The strongest support was for the active involvement of government.

The survey was conducted by Ekos Research Associates Inc. of Ottawa on behalf of the Privacy Commissioner, AMEX Bank of Canada, Canadian Bankers' Association, Consumer and Corporate Affairs Canada, Communications Canada, Equifax Canada, Statistics Canada and Stentor Telecom Policy Inc.. Ekos surveyed 3000 Canadian households;—the results are valid within a range of +/- 1.8 points, 19 times out of 20. The study will establish a base line against which future studies can be measured.

A survey of this size and rigour would have been impossible for the Commissioner's Office alone and likely for the other federal partners. The Commissioner is grateful to Ekos Research for the quality of its analysis and the many extra hours spent; to Stentor Telecom Policy for the initiative, financial commitment and staff work, and to Communications Canada for the contributions of its policy staff. It would not have been possible without them.

Privacy Commissioner v. Canada Post Corporation

For the first time in the *Act*'s ten-year history, the Privacy Commissioner has asked the federal court to review an institution's denial of access to personal information.

The Commissioner asked the court to determine whether the complainant has the right to know the identity of a witness who provided testimony against him during a grievance hearing, and on the basis of which the grievance was denied.

Canada Post initially denied the man both the name and the substance of the witness's testimony because it had been "prepared or compiled in the course of an investigation" and its release would injure the conduct of a lawful investigation (paragraph 22(1)(b)). He complained to the Commissioner. During investigation, Canada Post relented and provided the testimony but removed any identifying details and refused to name the witness.

The corporation argued that revealing the name would be "injurious to enforcement of any law" since the information was prepared during an investigation and it would identify a confidential source of information. It also maintained that revealing the witness's identity would offend the Act's provision against disclosing personal information about someone other than the complainant (section 26).

The *Privacy Act* defines personal information as including "the views or opinions of another individual about the individual." In other words, if Mary makes a comment about John, that is John's personal information. The Commissioner has asked the court to consider the distinction between a confidential source who provides information during law enforcement and a witness whose testimony is heard as part of an administrative process. The court will also be asked to assess what harm disclosure could cause once this type of administrative investigation is completed.

No date has been set for the hearing.

During the year courts issued decisions in two cases dealing with privacy matters.

SINs for birth registration

The first concerned Prince Edward Island's requirement that newborn babies be issued a Social Insurance Number, reported in the Commissioner's 1991-92 annual report.

Briefly, a couple refused to apply for a SIN for their newborn baby and were subsequently denied all claims for the baby's medical care because she did not have a SIN (the province's health care number). The parents argued that requiring someone to have a SIN to be eligible for medical benefits violated the *Charter*, denied equal treatment under the law and breached a person's reasonable expectation of privacy.

The court ruled against the parents on each ground. However, of particular interest to this Office was the court's comment on the *Privacy Act* and its application to a 1970 federal-provincial agreement under which Employment and Immigration Canada issues SINs for births registered in PEI.

In the court's words, "...the province does not have the right to receive information on individuals' Social Insurance Numbers from the Government of Canada without the consent of the individual, as it has not met the provisions of subsection 8(2) of the *Privacy Act*."

The Commissioner reviewed the decision which buttressed his own suspicion about the validity of the 1970 agreement (made well before the *Privacy Act* came into force). He wrote again to EIC, this time asking it to stop issuing SINs on the basis of the old agreement. EIC and Health and Welfare Canada have both committed to recommending PEI stop using SINs as health numbers and have undertaken to help the province adopt its own

personal identifier for health care. However, EIC will await the outcome of the parent's appeal of the decision.

Patient access to medical records

In another case, the Supreme Court of Canada ruled that a New Brunswick patient had the right to see all the documents in her medical file, not just those created by her current doctor.

The doctor had provided copies of all the documents she had prepared, but refused to allow the patient to examine any created by other medical practitioners. The doctor considered that would have been unethical since the records were someone else's property.

The court concluded that the physical records were indeed owned by the doctor. It also affirmed the physician's duty to protect the confidentiality of a patient's medical file unless the patient or the law authorized otherwise. But the court made it clear that the doctor-patient relationship "is fiduciary in nature" and information a patient reveals to a doctor "remains, in a fundamental sense, one's own."

The court observed that this "trust-like beneficial interest of the patient in the information indicates that, as a general rule, she should have a right of access to the information and the physician should have a corresponding obligation to provide it."

The right is not absolute. The court acknowledged that a doctor might have reason to believe it would not be in the patient's best interest to see some material. However, the decision puts the onus on the physician to justify denying a patient access.

While the case has limited immediate impact—applying only to those jurisdictions without specific legislation on patient access—it is important re-enforcement by the nation's highest court of individuals' proprietary interest in their personal information.

Biotechnology update

Two major developments occurred in drug testing at the federal level this year. In May 1992, regulations authorizing a wide range of drug testing programs in the Canadian Forces came into effect. In November, the *Corrections and Conditional Release Act* came into force, also authorizing a wide range of testing programs for inmates and offenders released into the community.

Drug testing remains a concern of this Office. Alcohol, not drugs, poses the greatest threat to workplace and public safety. Yet, the government continues its march towards drug testing.

Unlike alcohol testing, drug testing (urinalysis) cannot measure impairment. Even alcohol testing is an imprecise measure and the legal limit is arbitrarily set. Drug testing can measure only past drug use. It cannot tell how much was used, exactly when (only within days at best, and weeks at worst), or whether the drug impaired the user at the time. Most important, it cannot tell whether the user is **now** impaired. Thus, drug testing cannot reveal the only information that has any relevance—present impairment.

Simply put, drug testing will not tell air travellers whether their pilot is impaired. It will tell them only that the pilot has used a drug sometime in the past—information no more useful than knowing that their pilot may have had something to drink or been impaired by the flu or jet lag within the last month or week. Drug tests give no indication of the pilot's present ability to fly safely.

This Office is not insensitive to concerns for public safety. It accepts that some circumstances justify privacy intrusions. The legislation allowing the taking of breathalyser tests for alcohol impairment is a good example. But drug testing has no such justification. Instead, it represents a major new type of state-sponsored intrusion into the human body. Even persons charged with murder cannot be forced to surrender bodily

substances for forensic purposes, so great has been the law's protection of the integrity of the human body.

In short, drug testing is a major intrusion that is not offset by any significant benefits.

Canadian Forces' testing programs

Of particular concern is the drug testing program now underway in the Canadian Forces. This Office's 1991 report, *Drug Testing and Privacy*, questioned the need for testing within the Canadian Forces. If anything, our conviction that testing is not justified has strengthened. The results of a 1989 survey of Forces' members demonstrated clearly that use of alcohol, not illegal drugs, poses the greatest potential drug-related safety problem in the CF. The simplest way to explain the 1989 survey results is as follows: for every 1000 members of the Canadian Forces asked which drugs they had used in the past month

three would say they had used LSD;
five would say they had used cocaine;
25 would say they had used marijuana, and
780 would say they had used alcohol.

If there are drug-related safety problems in the CF, they stem to a far greater extent from alcohol, not illegal drugs. Yet the drug testing program almost exclusively targets the illegal drugs. The 1989 survey showed clearly that illegal drug use in the Canadian Forces is not of such magnitude that it justifies a massive intrusion into the bodies of its members through drug testing. The Commissioner has expressed his reservations to National Defence officials and written to the Chief of Defence Staff, all to no apparent avail. The Commissioner does not intend letting this issue drop.

A subsequent "blind" test (on December 8, 1992) collected more than 5,500 urine specimens at 15 locations in Canada and in

Germany. These samples were then analyzed for cannabinoids (e.g., marijuana), cocaine, opiates, amphetamines and phencycladine (PCP).

The results of the blind testing (although not strictly comparable with the results of the earlier survey), support the Office's position that members' rates of drug use are very low, and that the massive testing program introduced to detect those drugs is an unwarranted intrusion.

Testing inmates and parolees

The *Corrections and Conditional Release Act*, which came into force in November 1992, introduces a broad range of drug testing programs for inmates and those who have been released into the community. The justifications advanced for testing inmates and parolees differ from those for testing others. The drug trade in prisons is said to lead to increased violence and coercion within prisons. Reducing the demand for drugs through drug testing, it is argued, may help reduce these problems.

This Office certainly does not oppose reasonable measures to reduce violence within prisons. However, it remains to be demonstrated that drug testing will accomplish this. If it does, the violation of privacy may be warranted. If it does not, we hope that the Solicitor General of Canada will be sufficiently open-minded to reconsider the program.

Drug testing in prisons could pose one particularly grave danger. Drug users worried about being caught may switch from drugs that can be detected long after use (like marijuana) to those detectable for only a short period (like heroin and cocaine). This means switching from a smokable drug to one usually administered by injection. Given the scarcity of syringes (and syringe cleaning materials) in prisons, this could greatly increase the risk of HIV infection. While not strictly a privacy matter,

anything that increases the risk of HIV infection is yet one more argument against violating individual privacy through drug testing.

Transportation industry employees

A third major testing issue concerns the transportation industry. As this report goes to press, drug testing legislation aimed at safety-sensitive transportation positions appears unlikely to even be introduced before Parliament's summer recess.

Nevertheless, the Commissioner's concern bears repeating—the proposed transportation testing program constitutes overkill. It also unnecessarily sacrifices hard-won privacy rights. There is good news: the minister of transport has decided not to proceed with the department's planned random testing. Still, several other aspects of the testing program remain objectionable.

Testing athletes

The Office continues watching developments in drug testing in sport. Athletes too have basic human rights, including the right to privacy. Drug testing programs may help to make sport somewhat more fair, but at what cost? Particularly worrying is the response of a few to a recent Canadian Centre for Drug-free Sport questionnaire—they identified blood testing for drugs as an appropriate activity for the Centre. Urinalysis is intrusive, but at least it does not involve entering a person's body to remove body fluids, as blood testing would. It is frightening to think that some people will contemplate violating the very physical integrity of human beings, an integrity protected for centuries by law, in the name of men and women playing games.

Genetic Testing

The Office continues to follow rapidly occurring developments in genetic testing and their impact on privacy. Although our 1992 report, *Genetic Testing and Privacy*, has received national and

international praise, genetic privacy concerns have fallen behind other public issues. The immediacy of the dangers of unregulated genetic testing risks being overlooked.

Genetic technology will not wait for us to catch our breath. Genetic discoveries are breaking at an ever-increasing rate. Scientists and biotechnologists will continue to develop new, cheaper and more accurate genetic tests to identify physical and behavioral traits. Some traits, if revealed to employers, insurers and governments, will almost certainly stigmatize individuals or precipitate discrimination against them simply on the basis of their genes.

By waiting, we come ever closer to losing control over our own genetic information—information about the very essence of our beings. The Commissioner urges Parliament to take up this issue before a post-Orwellian genetics free-for-all engulfs us.

...Here and There

Regular readers of these reports will know that the Office monitors privacy protection elsewhere in this increasingly interconnected world. The past year has seen progress both at home and abroad.

In the provinces: Quebec

In December 1992, the Quebec government introduced Bill 68, an act to extend privacy protection to the private sector.

If passed, this will be the first legislation in North America to regulate private sector collection, use and disclosure of client and employee personal data.

The legislation would require businesses to limit collection of personal information to specific stated purposes. Clients could not be denied goods or services for refusing to provide personal information unless the details were required by law or to fulfil contractual obligations.

The bill would also require businesses to tell clients what information is held about them, to keep the data accurate, up-to-date and complete, and to obtain the subject's consent for any disclosures to third parties that are inconsistent with the stated purpose (unless specifically allowed by the legislation).

Consumers will be able to opt out of telemarketing or mail solicitation and to find out where the business got their personal information. And companies must have appropriate security measures in place to protect the confidentiality of personal information.

Specific provisions deal with credit reporting companies which must register with the provincial access and privacy commission and publish their activities in the newspapers. The bill sets out fines for non-compliance ranging from $1,000 to $10,000, depending on the offence.

The Quebec privacy commission will play a lead role in overseeing administration of the act. It will investigate complaints and issue binding decisions (although questions of law and jurisdiction may be appealed to the courts). The Commission will also have an education mandate and can encourage and help business develop internal privacy codes.

A legislative commission held public hearings and is now reviewing the bill and considering specific amendments.

At least one question remains to be answered: will the legislation apply to federally regulated businesses such as banking, transportation and communications? If so, will these sectors provide the same level of privacy protection to other Canadians?

British Columbia

In June 1993, British Columbia's legislature passed the province's first *Freedom of Information and Protection of Privacy Act.*

The act (which takes effect in October 1993) is broadly similar to other provincial legislation and will apply to BC government bodies. However, before even taking effect, the act is being amended to extend its provisions in October 1994 to local government bodies such as school boards, hospitals and municipalities. Other amendments would see self-governing professional bodies covered by Spring 1995.

Complaints will be handled by a commissioner—part ombudsman, part tribunal—allowing for both mediation and (if it fails) enforceable orders. Unlike the federal ombudsman, the commissioner will have access to Cabinet confidences to assess the validity of exemption claims. He or she has a specific mandate to carry on education and research. However, the commissioner too must live with time limits; reviews must be completed in 90 days. There are some undeniable benefits to having order

powers—they will allow the commissioner to impose deadlines on reluctant government agencies.

Overseas: the European Community Draft Directive

Of course, privacy developments can have implications well beyond national or regional boundaries.

The most obvious illustration is the European Community's (EC) draft directive on protecting personal data. Earlier reports have cautioned Canadian governments and business about the potential implications of strict European privacy rules on transfer of personal data in and out of the community—particularly to North America.

During the past year, the EC directive came under intense pressure from business, particularly the direct marketing and financial sectors. Business identified several problems: the directive's restriction on transfer of personal data to non-EC countries without "adequate" protection; the need for the subjects' express consent before their data is processed or transferred; "unnecessarily burdensome" obligations to notify the data protection authorities; and lack of flexibility for member states to use various kinds of regulation or codes to implement the data protection principles.

The lobbying had some effect and, in October 1992, the EC issued an amended directive. The revised version continues to require "adequate" protection in non-EC countries receiving EC residents' data. And it has dropped any formal distinction between the public and private sectors—the rules are the same. However, there is added flexibility. The directive now allows transfers if the subjects consent, if the data is needed to satisfy a contract between subject and controller (notice must be given to the subject), and if an important public interest or the vital interests of the subject are at stake.

The amended directive will also allow EC countries to consider the type of data, the reason for processing, any sectoral codes, as well as legislative provisions, and even "professional rules" when assessing the "adequacy" of non-EC countries privacy protection.

It is not clear how Canada's patchwork of public sector legislation and private sector codes (or statements of good intent) will measure up.

OECD Experts Privacy Briefing

Technology is usually blamed for eroding rather than enhancing privacy. But a November 1992 meeting of the OECD (Organization for Economic Cooperation and Development) turned the problem on its head and looked at the potential of technology to protect personal data. The OECD invited several experts to brief government participants on using new technologies and processes to protect personal data in electronic systems.

Some of the technical possibilities include encryption (coding), trusted systems (specially designed to meet specific security objectives), blind signatures and electronic cash (verifying financial transactions without tracing the individual) and networks which allow transmissions between parties without their being "observed." It is unlikely that any system will be foolproof but these meetings are an important step in building controls into the systems themselves. The group expects to meet again.

As well, the OECD passed its new Guidelines on Information Security Systems which will soon be released.

Privacy in Hong Kong...

The Hong Kong government recently issued a discussion document examining the Crown Colony's current privacy protections and outlining a framework for a privacy protection bill. The draft was produced by a Law Reform Commission

sub-committee, representing academia, law, telecommunications, banking, trade, police and the media.

The draft contains the eight OECD principles and much of the spirit of the latest EC draft directive. There is a comprehensive description of what constitutes personal information and its jurisdiction will include both the public and private sectors. The draft also deals with sectoral codes, data matching, direct marketing, personal identifiers, and transborder data flow. Two of its strengths appear to be provisions for ensuring that data subjects consent to uses and disclosures, and allowing individuals to opt out of direct marketing activities.

With Hong Kong's reversion to mainland Chinese control in 1997, the future of the proposed bill is uncertain.

...and New Zealand

New Zealand is in the midst of considering a comprehensive privacy act to replace a number of statutes, each with limited jurisdiction. The bill contains 12 privacy principles, expanding on those contained in the OECD principles and the EC directive. It will cover both the public and private sectors and it tackles such subjects as private sector codes of practice, public registers (for example, electoral lists) and data matching.

The bill would allow the privacy commissioner to issue emergency codes of practice. It also sets out comprehensive data matching requirements for the public sector, requires users to verify the accuracy of personal data before processing, and establishes a broad scheme of damages to compensate those whose privacy is breached.

There are, however, some notable omissions: organizations have substantial discretion to determine what are "trivial" demands and they may charge fees to process access, correction and notation

requests. And it appears that criminal offenders will have no access and correction rights.

The bill is awaiting second reading and is expected to take effect on July 1, 1993.

...In the Private Sector

The CSA model code

Last year we reported the Canadian Standards Association's initiative in developing a model privacy code to serve as a minimum standard for private sector handling of personal information. The model code holds promise for some meaningful privacy protection without resort to legislation.

CSA formed a committee whose goal is to develop and then promote a model code based on the OECD guidelines. The members (including this Office) represent finance, insurance, direct marketing, telecommunications, information technology, utilities, credit reporting, consumers and federal and provincial governments.

Work continues apace. Committee working groups have prepared documents explaining each of the OECD principles in everyday language and identifying the issues that must be dealt with to implement each principle. A drafting committee will now amalgamate and edit all the material into a single draft model code which is expected to be ready for committee review later this year.

One important aspect of any code is the oversight mechanism. The committee expects to make specific recommendations on several possible options for registering or certifying industry specific codes.

Privacy staff were also resources for CSA's consumer advisory panels which provide input and public review of the standards. Recommendations from these panels will help the committee reflect the privacy concerns of the wide range of interests and occupations beyond its immediate membership.

Canadian Direct Marketing Association

Also reported last year was the CDMA's decision to develop its own specific privacy code (CDMA is also a member of the CSA group).

The CDMA has done it. The code, released in January 93, was developed following two years of research and consultation with consumers, industry and privacy experts. Prior to the code, CDMA had offered consumers the option of removing their names from all CDMA members' lists. But the new code goes further. It gives consumers a means of controlling the transfer of marketing information about them by allowing them

- to decline to have their names used;
- to know the source of their information, what information it holds and to request correction of errors;
- to control the subsequent use of their information by third parties;
- to be reassured about the security of their information;
- to benefit from more stringent protection for sensitive information, and
- to complain to the CDMA if a member breaches the code.

The code demonstrates what commitment to an idea can produce. CDMA members understand the importance of consumer confidence, control and consent for the health of their industry. The code is not perfect; there are no limits on collection (as envisaged by the OECD guidelines) and the oversight mechanism is not independent. Nevertheless, the effort deserves a round of applause from consumers and privacy commissioners alike.

Investigating Complaints

There were no surprises this year. The number of new complaints climbed to yet another record total of 1,579—a 13 per cent increase. However, investigators closed 1,440 cases during the year, almost double last year's productivity. Of the closed cases, 590 were well-founded, 757 not well-founded and 104 discontinued.

Complaints about time limits and denial of access made up 86 per cent of all complaints received. Many institutions have blamed their poor track record on staff cutbacks caused by the government's drive to reduce expenditures. The result is slower service to applicants.

How Institutions Measured Up

Here too there are few surprises. Over 85 per cent of the new complaints were against virtually the same departments as in previous years: Correctional Services (CSC), Revenue Canada, Taxation, Employment and Immigration Canada, Canada Post Corporation (CPC), Canadian Security Intelligence Service (CSIS), Royal Canadian Mounted Police (RCMP), Revenue Canada, Customs and Excise, and National Defence. New to this year's top ten are Transport and Health and Welfare Canada.

Health and Welfare Canada

New complaints against Health and Welfare climbed to 132 this year (90 access, 28 time limits and 14 others) from 40 in 1991-92. The vast majority concerned information held by Income Security Programs—Canada Pension Plan, Family Allowances and Old Age Security—programs that maintain files on virtually every Canadian. The department was also the subject of many complaints about tardy responses to requests—18 of 37 completed complaints concerned time limits, all but two of which were well-founded.

Canada Post Corporation

The number of new access and time limits complaints against Canada Post were similar to last year's—54 and 22 respectively. However, the corporation continues to be the target of many complaints about its collection, use, disclosure and retention of employee records. These 43 privacy rights complaints make up 36 per cent of Canada Post's total case load of 119—the highest number of any government agency.

Two years ago there was praise for Canada Post, despite having the questionable honour of the office's most important client. Almost 80 per cent of its complaints were not well-founded, many related to its administration of the employee attendance and leave policy and its modified duties program for employees unable to carry out their normal functions due to injury or illness.

This year more than half of the complaints against CPC focused on its inappropriate use of exemptions (half were well-founded), and delays in processing (22 of 24 well-founded).

All but a handful of complaints originated from CPC employees in Ontario (particularly in Metro Toronto and southern Ontario) who are involved in labour relations disputes. Some CPC labour relations officials see an inherent unfairness in allowing employees in labour disputes to use the *Privacy Act* to obtain documents germane to their grievance, while there is no parallel right for CPC management to obtain access to the unions' files.

This view that the *Act* is a pawn in labour relations disputes has made it very difficult to resolve some complaints. An illustration is the office's first case which asks the court to review Canada Post's refusal to disclose the identity of a witness who provided information in a grievance matter (see In the Courts).

Other departments

More than 100 of the 172 complaints investigated against Revenue Canada, Taxation were filed by one individual, all related

to time limits. Customs too had problems meeting the 30-day deadline: 36 of the 44 against that department were well-founded.

The RCMP is to be commended for its efforts to follow the letter and spirit of the access provisions of the *Act.* Of the 47 time limits, denial of access and corrections complaints investigated this year, none were well-founded. CSIS, too, responds promptly and properly. Only two of 89 complaints were well-founded, but both were resolved.

Still, it is discouraging to have to report that after ten years administering the act, many departments still have difficulty responding to requests properly and in a timely fashion.

Origin of Completed Complaints

Newfoundland	8
Prince Edward Island	3
Nova Scotia	27
New Brunswick	30
Quebec	153
National Capital Region Quebec	13
National Capital Region Ontario	156
Ontario	588
Manitoba	63
Saskatchewan	55
Alberta	101
British Columbia	216
Northwest Territories	2
Yukon	19
Outside Canada	6
TOTAL	1,440

Notifying the Commissioner

Although the *Privacy Act* generally prevents federal organizations from disclosing personal information without the person's consent, there are exceptions. Two of these oblige the organization to notify the Privacy Commissioner: a release in the "public interest" or one which would clearly benefit the person concerned. There were 48 notifications this year.

The *Act* requires the head of the organization to determine what is in the "public interest", not the Commissioner. The Commissioner's role is to review the proposal and to notify the individual concerned if that seems appropriate. The Commissioner has no power to prevent a release; however, if he strongly disagrees he may initiate his own complaint. The individual also has no avenue to block release but does have a right to complain to the Commissioner, albeit after the fact.

Staff examines these notifications, leaving the Commissioner free to consider any ensuing complaints.

Assessing the public interest can be a tough call for department heads, as some of this year's notifications illustrate.

HIV status disclosed

Correctional Service Canada (CSC) advised the Commissioner that it would disclose the HIV status of a man alleged to have sexually assaulted two young girls. The man, on parole at the time, had refused the fathers' request for the results of blood tests he took voluntarily when he was arrested.

Since the test results were negative, CSC wanted to assure the families that their children had not been exposed to the HIV virus. However, the Commissioner cautioned CSC that the negative test did not necessarily mean the children's health was no longer at risk. The HIV virus can remain undetected for years after the person is exposed. The Commissioner urged CSC to point this out

to the parents. CSC agreed and the Commissioner advised the man of the disclosure.

Nurse's name to professional association

In another HIV-related case, CSC advised it would give the Registered Nurses Association of British Columbia the name of a nurse who had left an HIV-contaminated syringe on the counter in a federal penitentiary. Another nurse then used the syringe to draw blood from a second inmate.

CSC's board of investigation recommended reporting the incident to the association. Nurses are obliged to report any breaches of their code of conduct to their association but the nurse's union had advised her to refuse. CSC considered it in the public interest to ensure professionals comply with their code of conduct and advised the association. The Commissioner wrote to the woman to ensure that she understood the government's obligations and her rights under the *Privacy Act*.

Team member's passport details to Olympic organizers

A last minute opportunity for the Canadian women's fencing team to compete in the Barcelona Olympics prompted an urgent call to External Affairs Canada for passport information on a team member.

The team had not qualified in the top 12 during preliminary competitions and members had dispersed. But when two qualifying countries failed to field complete teams, the Canadian women were invited. Organizers scrambled to re-assemble the team and to provide passport information immediately to Olympic officials for security and identification. When organizers could not reach one of the members, they asked External to provide the woman's passport number and expiry date.

External concluded that there was a public interest in having the team compete and a personal benefit to the team member. The department advised the Commissioner it would release the information. She was reached 12 hours later.

Electoral lists to political parties

A 1992 privacy compliance review of Elections Canada revealed that electoral lists were routinely being disclosed to political parties and candidates in the "public interest" without notifying the Commissioner. As a result of the review, the Commissioner received his first formal disclosure notice in January 1993.

The lists are assembled from door-to-door enumeration conducted during an election campaign. They contain the last and first names, sex and address of each eligible voter in the riding and are available in paper or electronic form. Political parties and candidates use them for promotional mailings, door-to-door canvassing and to solicit contributions. The current lists are particularly valuable since voters were enumerated recently for the Constitutional referendum.

Elections Canada receives many requests for the lists but provides them only to political requesters in the interest of candidates reaching constituents during an election campaign. The Commissioner is satisfied as long as the lists are used only for election purposes.

Nepotism allegations prompt release of personal details

A competition for customs inspectors in Winnipeg and Emerson, Manitoba led to allegations of favouritism in the *Winnipeg Free Press*. The Public Service Commission (PSC), which hires all federal public servants, advised the Commissioner that it had investigated the allegations and intended to release its report.

The PSC received more than 1,000 applications for the job openings at Revenue Canada, Customs and Excise. After an initial screening, customs officials interviewed 279 candidates who had passed the written test. The 20 qualified candidates were ranked in order of merit and 11 were offered positions.

Several unsuccessful candidates complained that at least three of those hired were relatives of Customs superintendents. Local media reported the allegations and other complaints surfaced—25 in all—including one from the Customs employees' union.

Given the seriousness of the allegations—and the PSC's mandate to uphold the merit principle in public service hiring—the PSC concluded that there was a clear public interest in a full accounting of the process. The report contained the names of all qualified candidates who were related to Customs employees, the position titles (but not the names) of the employees to whom they are related, and brief general summaries of the employment experience of a number of the applicants.

Unfortunately, the Privacy Commissioner was not notified until the day after the report was released to the newspaper, giving him no opportunity to alert the individuals to the probable publicity. PSC acknowledged the error but felt pressured to deal with the continuing media inquiries. The Commissioner decided to write to all those involved to explain the process and their rights under the *Privacy Act*.

Petro Can shareholders not disclosed

Supply and Services Canada (SSC) advised the Privacy Commissioner that the Information Commissioner had recommended it release the names and last known addresses of shareholders of Petro Canada Enterprises Inc. to an "investigative accountant."

The department denied the accountant's Access to Information request because the information was personal and therefore exempt. The accountant complained to the Information Commissioner, arguing that it would benefit the shareholders if he could use the SSC lists to find them and—for a fee—obtain the moneys owing.

SSC holds the lists because the company was dissolved in 1983 and the value of the unredeemed shares ($120.14 each) was paid into general government revenues. Registered owners may claim the money from SSC.

Apparently SSC had written to each shareholder at the wind-up of the company explaining the arrangement for cashing the shares. It also placed advertisements in major Canadian and foreign newspapers. Approximately 80 per cent of the shares have been redeemed and the department continues to receive claims from individuals on its lists. Following the complaint, the department mailed another reminder to shareholders. It argued that any shareholder who is unsure how to obtain the money need only contact Petro Canada or any stock broker.

There is a public interest in ensuring that the government makes reasonable efforts to locate those for whom it holds money. However, the Privacy Commissioner had reservations. He questioned whether that interest was best served by disclosing the information, without shareholders' consent, to a third party who intends charging a finder's fee of 15 to 40 per cent of the shares' face value. The disclosure seemed to served the accountant's interests more than the shareholders'.

Nor would the disclosure guarantee that all shareholders' interests would be served. The Commissioner doubted that it would make economic sense for the accountant to attempt to find at least half of the shareholders who hold three or fewer shares. As well, 60 per cent of all those on the list live outside Canada.

A second concern was how SSC would protect shareholders from subsequent use or sale of the lists. Once released, there is no legal means for the government to prevent third parties from duplicating, selling or otherwise using the information.

Finally, the Commissioner wondered how the accountant expected to find the shareholders using the same addresses as SSC. If there was a way, he encouraged SSC to use it and save the shareholders the third party's fees. Both Commissioners agreed that SSC needed to be more aggressive in communicating with shareholders—however the Privacy Commissioner was unconvinced that disclosure to a third party was the best remedy.

Although the accountant did not get the lists he wanted, his access complaint prompted the department to write again to all shareholders and to consider other ways of reaching those who do not respond.

Inquiries

Inquiries also increased again this year—by 10 per cent to 5,183. Of these, 4,865 were telephone calls, 274 letters and 44 personal visits.

Almost 55 per cent dealt with individuals' rights under the *Act* but about 20 per cent concerned privacy matters over which the Privacy Commissioner has no jurisdiction—other public sector organizations or private businesses. The remainder had been mis-directed or had nothing to do with privacy. Although many of the questions are outside the office's mandate, inquiries officers redirect callers to the appropriate organization or department.

Several callers were concerned about postal employees recording their identification card numbers when they received parcels and registered mail. The office reviewed Canada Post's procedure which requires anyone picking up parcels or registered mail to produce acceptable identification, and the postal employee to record the details in a ledger.

The Commissioner agreed that Canada Post must check identification to ensure that the person claiming the parcel is the intended recipient. The information is logged to provide a trail in case valuable goods or documents go astray. Privacy staff also confirmed that delivery registers are kept in an area not accessible to the public.

Inquiries officers continue dealing with many calls concerning the collection, use and disclosure of personal information by financial institutions. Since the banks are not subject to the *Privacy Act*, and the Office of the Superintendent of Financial Institutions does not deal with complaints about information practices, privacy staff must refer callers back to the financial institution—each of which has its own policy on management and use of personal information.

Inquiries officers often must explain that the *Act* deals with just one facet of privacy. For example, a man returning recently from

an overseas assignment, complained to the Commissioner about customs officials' rudeness and of their searching his personal files and belongings. He wanted to know his rights under the *Privacy Act*. Privacy staff explained that the *Customs Act* authorizes customs officers to examine goods and mail, and their rudeness is not covered by the *Privacy Act*.

Sometimes callers ask that their complaint be handled informally. An employee of a company participating in a work sharing program with Employment and Immigration Canada (EIC) was concerned that EIC sent documentation to the employees through the employer.

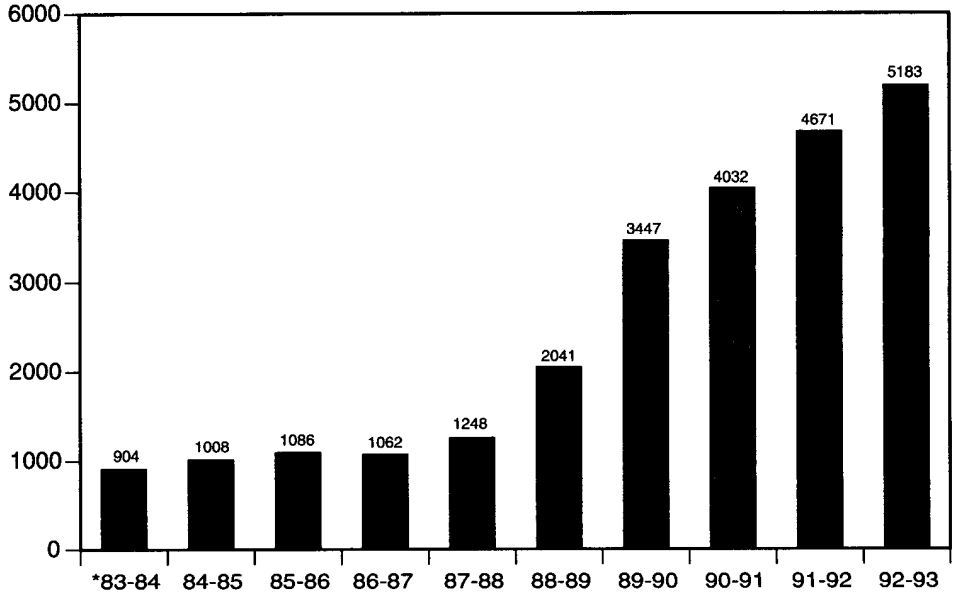
Although the company needed to examine employees' benefit statements to make the proper wage adjustments, the caller did not think it needed to see the employees' Telephone Access Code (TAC). This is a personal identification number which gives UI recipients access to information about their benefits over the telephone. EIC looked into the problem and agreed to remove the access code from the documents. It advised employees to change their TAC number.

Three callers asked whether a Moneymart, a video store and a large appliance store were allowed to take identification pictures of them. There is no legislation covering this situation. Is picture taking a new fad?

Inquiries about the SIN continue—549 this year. The Office's advice to anyone not wanting to provide their SIN to private businesses, landlords, or organizations not subject to any legislation covering the SIN, is to ask:

- Do you need my SIN to comply with a legal statute or regulation?
- Why do you need it and how will you use it?
- Will you keep it confidential?
- What are the consequences if I refuse?
- Would you accept another ID?

Inquiries 1983-93



* 9 Months

Job competition notes accessible

A complaint against the Department of Justice established an important precedent for access to handwritten notes taken by board members during job competitions.

A man asked the department for copies of all material gathered during his job interview. He complained to the Commissioner when Justice could not find the interviewers' notes.

The investigator found that all the selection board members took handwritten notes to help rate the candidates during the interviews. The notes taken by three board members were destroyed once the hiring process was completed. The fourth member (a staffing officer) recalls including her notes with the documents transferred to personnel when she left the department shortly after the interviews. However, a search of the department's staffing files found nothing. The department assumed the notes were inadvertently lost or destroyed.

While the Commissioner was prepared to concede that all employees occasionally make personal notes which cannot be considered "under the control" of their department, he was not persuaded that this was such a case. In his view, selection board members' notes are made to choose a candidate—an administrative purpose—and should become part of the staffing file. This means they are accessible under the *Privacy Act*.

After extensive consultations, Justice finally accepted the Commissioner's position. The department was unable to establish the exact content of the notes made about the complainant. However, it admitted that since the selection board considered the notes in reaching its decision, they had been used for an administrative purpose and should have been retained and made available to the complainant. Since they had not been kept, the Commissioner considered the complaint well-founded.

As a result of this investigation, Justice assured the Commissioner that it would require future selection boards to retain "notes made by members and used in the decision-making process." The handwritten notes will be given to the personnel representative and become part of the final board report (unless they are incorporated verbatim). The Commissioner agreed with the department's observations that the ramifications of the case were important enough to mitigate the delay.

Disciplinary notice not for union

An employee of Employment and Immigration Canada (EIC) complained to the Commissioner that his manager improperly disclosed disciplinary information about him to another employee during the October 1991 strike of the Public Service Alliance of Canada (PSAC).

The investigation revealed that the complainant was a "designated employee", meaning he was required to work during the strike. However, one morning he failed to report for work and was seen later on the picket line. His manager wrote a letter reprimanding him for being absent without authorized leave, and attempted to give it to the complainant. He refused to accept it.

After advising him to report to work immediately (and the financial implications of refusing), the manager put the letter on the complainant's desk. He also gave a copy to the PSAC union strike coordinator, who was the complainant's local steward.

The Commissioner agreed that an employer has the right to tell the union official that a member is engaged in an unlawful strike but it did not have the right to give her a copy of the written reprimand, showing what disciplinary action would be taken. The Commissioner considered the complaint well-founded.

No medical details during reference checks

Another EIC employee complained to the Commissioner that the department improperly collected confidential and inaccurate medical information about her during a reference check with a supervisor, then used it to eliminate her from the list of qualified candidates.

The investigation confirmed that during a job competition in one of its employment centres, EIC staff conducted telephone reference checks with qualifying candidates' most recent supervisor. Asked if the complainant's attendance and punctuality were satisfactory during the past year, her supervisor provided specific medical details which were then recorded on the file.

Collecting information about illnesses or injuries during reference checks poses potentially serious privacy problems. It can harm the individuals by revealing gratuitous details about the person's health or life. The Commissioner was concerned about the accuracy of any medical information collected during the process, as well as the validity of any conclusions that staff might draw based on such medical data.

The *Privacy Act* prohibits collecting personal information unless it "relates directly to an operating program or activity" of the department. EIC conducts literally hundreds of staffing actions every year so it is inevitable that it will occasionally be offered unsolicited medical information during reference checks. Nevertheless, the Commissioner considers it the department's responsibility to ensure that it does not collect more personal details than it needs simply to assess a candidate's record for attendance and punctuality.

The Commissioner concluded that the medical information was not required for the staffing action and that the complaint was well-founded. However, he dismissed a second complaint that EIC had misused the information when it became apparent that it was

the complainant's attendance record (which was relevant) that made her unsuitable for the job.

EIC removed all the supervisor's references to her illness from the files. In addition, it agreed to publish guidelines to remind managers about the proper way to conduct reference checks in keeping with both the *Privacy Act* and the *Canadian Human Rights Act*. The Commissioner considered the matter resolved.

Need court order for disclosure

An employee of Correctional Service Canada (CSC) complained to the Commissioner that her director disclosed to a third party a copy of a security investigation report containing personal information about her.

The director confirmed that he had given a copy of the woman's report to the director of an after-care agency under contract to CSC. He had provided the report at the agency's request because the complainant had filed a lawsuit against the organization.

The Privacy Commissioner concluded that none of the disclosure provisions of the *Privacy Act* justified this release. The *Act* allows personal information to be released in response to a subpoena or court order but the outside agency had obtained neither. The Commissioner concluded that the disclosure was unwarranted and considered the complaint well-founded.

Legal guardian must consent for minor

A man complained to the Commissioner that External Affairs denied him access to his son's passport records. The father felt that since his son was a minor, he was entitled to see the records.

The Commissioner was satisfied that the passport information was personal information about the son. The *Act* allows personal information to be disclosed only to the subject of the information

unless he or she consents to release to a third party (there are some specific exceptions). Since the son is a minor, the *Privacy Regulations* require the consent of the individual's legal guardian—in this case, the complainant's former wife.

The Commissioner believed that External Affairs had acted properly in refusing the complainant's request and considered the complaint not well-founded.

SIN optional for job-seekers

A man's complaint that Employment and Immigration Canada (EIC) misused his social insurance number (SIN) has led to a change in the way EIC registers clients seeking employment.

The complainant refused to provide his SIN when registering for summer employment and wanted to know why it was necessary. He alleged that his question was referred to a manager who then retrieved the man's SIN from departmental files before talking to him.

EIC claimed that it is reasonable for a CEC manager, before returning a client's phone call, to use the client's SIN to retrieve the file and thus be better prepared to respond to the client. The Commissioner was satisfied with the explanation and found the complaint to be without merit.

However, EIC officials were asked why clients must provide the SIN when simply registering for employment. They assured the Commissioner that the intent is simply to provide the broadest range of services EIC has to offer its clients. The SIN is the only practical means for identifying and referring clients with particular skills to suitable job openings.

Nevertheless, EIC did agree to dispense with collecting the SIN when the client objects. However, staff will caution those clients that not having their SIN will limit the services EIC can provide

and could mean lost job referrals. The choice of providing the SIN will rest with the client.

HIV poster display "careless"

The Privacy Commissioner received a complaint from the B.C. AIDS Network that the RCMP had posted photographs and descriptive details about five HIV-positive individuals on a bulletin board in the local detachment. Someone had seen the information and told one of the individuals who complained to a local AIDS support group.

The Commissioner investigated to determine whether the RCMP should have collected the information that the individuals were HIV-positive, and to assess how the Force was using it and whether the disclosure was proper.

The investigation established that the photographs and details were collected from the detachment's own operational files. Police files identified all five individuals as known repeat offenders with a propensity to violence. They were considered to pose a threat to police and guards and all had volunteered that they were carriers of the HIV virus.

Although the individuals were well known to the detachment's full-time guards, staff suggested posting the information in the guards' office where 10 casual guards (who replace full-time staff who are on leave or sick) would see it.

The investigator found that prisoners and the public do not enter the guards' office. In fact, even police officers do not normally have access. However, the office is frequently left unoccupied when guards are busy elsewhere in the cell area.

It was evident that the photographs and documents were too small to be discernible from the open counter at the front of the office, or even from the doorway. Given that the bulletin board is

mounted on the same wall as the door and counter, someone would have had to enter the office and approach it to read the details. The investigator was unable to determine who had seen the material.

The information has since been removed from the bulletin board and placed in one of the desks. The RCMP is drafting a policy to control the display of identifying information about detainees who are HIV-positive or who have developed AIDS.

The Commissioner considered it reasonable for the RCMP to inform guards about individuals who pose a risk to employees and other prisoners. He concluded that the display did not breach the *Act*. However, while the Commissioner remains concerned about organizations assembling inventories of people identified as HIV-positive, he appreciates the quick action of both AIDS organizations, and the RCMP's immediate response.

Doing the bureaucratic shuffle

The man looking for information about his participation in EIC job training programs in 1975 complained to the Commissioner when all he got was a run-around.

First he went to his local Canada Employment Centre where he was told that the department did not keep the information as far back as 1975. He consulted *Info Source* (the directory of government information holdings) which confirmed that the training files were indeed kept for 25 years. Reassured he went to EIC's Toronto regional office and tried once again.

The regional office referred him back to his local CEC who repeated that the information did not exist. This time his request was referred to the National Archives.

During the shuffle, the complainant was given several inconsistent explanations. He was told the material was kept for only two

years, then seven years. The *Info Source* listing describes the retention period of one bank as indefinite; the second as two years for paper and 25 years for machine readable records.

The first thing the investigator needed to establish was just how long EIC kept the information in the two banks. Officials explained that the information is indeed kept for two years in individual Canada Employment centres, then it is transferred to a departmental archive where it is kept for a further five years. The information is then destroyed. Only statistical and program evaluation material (not personal information) is transferred to computer tapes and kept for 25 years.

The Commissioner concluded that the information had not been improperly destroyed and that complaint was not well-founded. However, he was concerned about the confusion, the repeated re-routing of the complainant's request and the inconsistent explanations about why the information did not exist. He asked EIC to clarify its explanation of the retention periods in *Info Source*—the tool on which the public depends to gain access to their records.

Improper Collection of Medical Information

An employee of the St. Lawrence Seaway Authority (SLSA) complained to the Commissioner when he was refused pay for two days sick leave because he would not disclose the nature of his illness to his supervisor.

SLSA policy required all employees claiming sick leave to supply the medical details on the "Application for Leave" form. The information was then reviewed by the employee's immediate supervisor who determined whether the condition warranted payment of sick leave.

SLSA staff argued that supervisors must collect and assess the information because occupational health and safety rules require

SLSA to ensure returning employees will not endanger themselves or colleagues. They also argued that collecting the medical details kept employees honest and was an important factor in controlling absenteeism and reducing costs.

The Privacy Commissioner recognizes that employers have a right to satisfy themselves that an employee's absence is justified, and there may be occasions when it will need to collect medical information from employees before endorsing sick leave requests. However, he does not agree with unqualified personnel collecting and assessing medical information. The Commissioner considered the complaint well-founded since the right to collect medical details to assess an employee's fitness should be reserved only for a qualified medical practitioner.

SLSA officials responded by changing their sick leave collection procedures, in place since the 1960s. The nature of illness is no longer disclosed to supervisors. When needed, it is collected and reviewed only by qualified medical practitioners.

Locator information unnecessary

An inmate asked for access to his Offender Grievance Files at Correctional Services Canada (CSC). He complained to the Commissioner when CSC refused to process the request, claiming he had not provided them with all the locator information needed to find the files.

The investigator found that every CSC institution keeps either a computer or manual log of all grievances submitted by inmates in their institution. Any CSC institution could easily identify and locate an inmate's grievance file in that institution just by using the inmate's name. The additional locator information was not necessary. CSC admitted that it could retrieve the file using the name and agreed to change its requirements for access to this information.

The complaint was well-founded.

Public interest release prompts complaint

Last year the Office reported receiving a complaint against the Privy Council Office (PCO) following its disclosure of personal information about two members to their professional body.

The case illustrates the limitations on the Commissioner's powers and the individual's rights in these "public interest" disclosures. It also demonstrates why staff examine the disclosure notices: the Commissioner must not have pre-judged the release and be prevented from ruling on a subsequent complaint.

The material was produced during a federal commission of inquiry. The commission report recommended the professional body review its members' conduct and PCO (the custodian) agreed to the body's subsequent request for the records. PCO advised the Commissioner, arguing there was a public interest in the body maintaining its professional standards.

The Office recommended notifying the two members (and their clients whose information would also be disclosed as evidence) and PCO agreed. One of the two then complained to the Commissioner.

The Commissioner reviewed PCO's procedure, the inquiry commission's recommendation, the material released and the powers of the professional body to compel evidence and conduct investigations.

He concluded that the disclosure did not violate the *Privacy Act*. He also pointed out that the professional body's powers were sufficient to compel PCO to produce the material under another provision of the *Act*.

Access to consent of "other parent"

An estranged husband asked External Affairs' passport office to provide him with a copy of his declaration, signature and consent contained in his wife's application to include their children on her passport.

The passport office replied that since the application belonged to his wife, he would need her authorization to obtain a copy.

The investigator examined the material and disagreed, pointing out that the information belonged to the husband since it refers to the "other parent", not the parent completing the passport application. The passport office was unconvinced and very reluctant. After much debate, it finally released the disputed information. The Commissioner considered the complaint well-founded and resolved.

Parole Board fine tunes process

The National Parole Board often has to consult other organizations such as provincial government agencies or police forces before completing an access request. In one case, the Board wrote to several organizations asking for consent to release information they had provided about the applicant.

All but one responded in time for the board to process the request within the required 60 days. However, the PEI Crown Prosecutor did not respond to several letters. After many months, the board finally reached him and he agreed to release the information.

Given the time it took to get a response (and the well-founded complaint to the Commissioner), NPB decided to change its consultation process. Consultation letters now state that if the board does not receive a reply by a specific date, it will process the information in accordance with the federal *Privacy Act*. The onus has now shifted; an organization must respond quickly if it

wants to refuse to disclose information. And applicants are not kept waiting needlessly for months.

Questionnaires need own bank

Several Employment and Immigration Canada (EIC) employees complained through their union that a questionnaire collecting personal information for the department's Human Resource Inventory Program (HRPIP) violated their rights under the *Privacy Act*.

They complained that they had not been told the purpose for the collection. They also alleged that managers had ordered them to complete the supposedly voluntary questionnaire, requiring them to consent to all subsequent uses and disclosures of the information. They argued that this was a de facto avoidance of the use and disclosure provisions of the *Privacy Act*. Finally, they complained that the information being collected was not described in *Info Source*, as required by the *Privacy Act*.

EIC was sensitive to the employees' privacy concerns. Although it had tried to ensure full compliance with the *Privacy Act* in carrying out the project, some details had to be addressed.

The investigator found no evidence to substantiate the claim that employees had been ordered to complete the questionnaire. Although the language was not entirely clear, on second reading it was possible to determine that completing it was voluntary. However, EIC officials agreed to clarify the opening statement.

It was true that the collected information was not described in *Info Source*. EIC officials explained that all the separate pieces of information were described in the various standard employee banks, so it was unnecessary to develop a new bank. The Commissioner disagreed, viewing this as a distinct bank of personal information collected for a specific purpose.

Since many departments have similar programs (and there is no standard employee bank for this information), the Commissioner decided to accept EIC's explanation, close the complaint file, and work with Treasury Board to develop a new government-wide standard bank for these records.

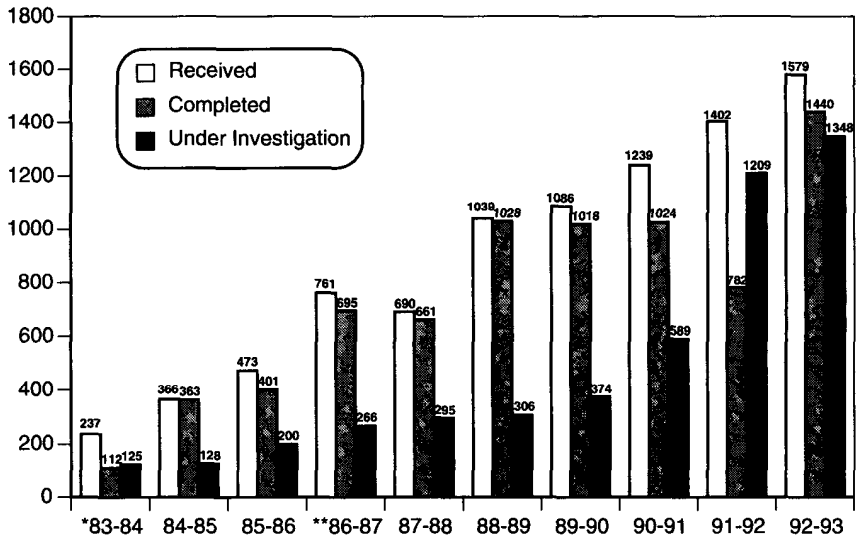
Inmates receive each other's records

Two inmates in a federal penitentiary complained that the personal information of each inmate had been improperly disclosed to the other. Both had requested their own records but when they were delivered, each envelope was found to contain the others' files, despite being properly addressed.

Staff at the institution confirmed that the incident happened substantially as reported. However, the files had arrived at the institution in sealed envelopes so the investigation focused on the privacy coordinator's office in headquarters where the envelopes had originated.

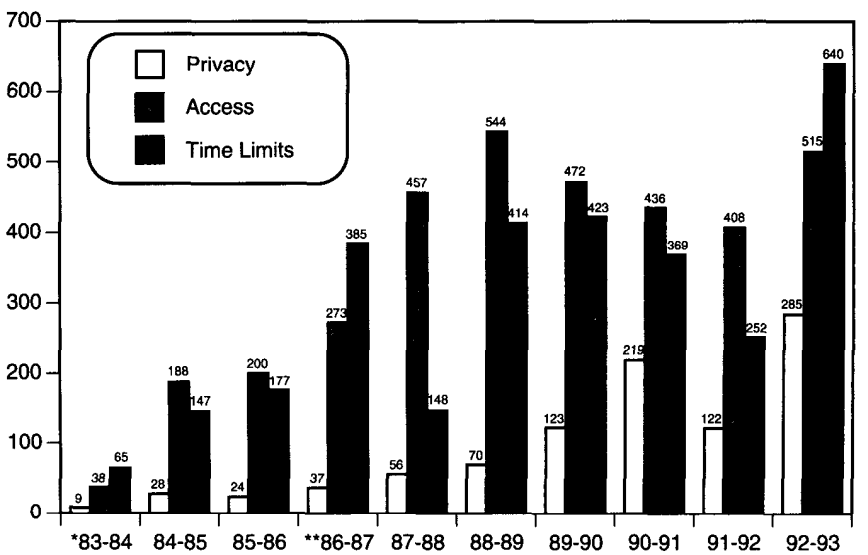
The investigator confirmed that controls are in place to prevent such incidents. However, the sheer volume of files handled by CSC headquarters, combined with shortages of trained staff to cope with that volume, made it almost inevitable that a mistake would happen. The Commissioner concluded that the two complaints were well-founded but made no recommendation that CSC institute further controls. The mix-up was probably attributable to human error.

Completed Complaints 1983-93



* 9 Months
** Revised counting method

Completed Complaints and Grounds 1983-93



* 9 Months
** Revised counting method

Top Ten Departments by Complaints Received

Institution	TOTAL	Grounds		
		Access	Time Limits	Other
Correctional Service Canada	417	161	215	41
Revenue Canada - Taxation	158	34	111	13
Employment and Immigration Canada	133	51	51	31
Health and Welfare Canada	132	90	28	14
Canada Post Corporation	119	54	22	43
Canadian Security Intelligence Service	95	86	9	0
Royal Canadian Mounted Police	92	62	12	18
Revenue Canada - Customs & Excise	92	24	60	8
National Defence	72	34	22	16
Transport Canada	48	40	4	4
OTHER	221	107	68	46
TOTAL	1,579	743	602	234

Completed Complaints by Grounds and Results

Grounds		Disposition				
		Well-founded	Well-founded; Resolved	Not Well-founded	Discontinued	TOTAL
Access		10	114	351	40	515
	Access	9	96	334	38	477
	Correction/Notation	1	4	14	2	21
	Index	0	14	0	0	14
	Language	0	0	3	0	3
Privacy		28	25	204	28	285
	Collection	2	4	95	10	111
	Retention & Disposal	6	5	4	0	15
	Use & Disclosure	20	16	105	18	159
Time Limits		403	0	202	35	640
	Time Limits	339	0	93	30	462
	Extension Notice	64	0	109	5	178
TOTAL		441	139	757	103	1,440

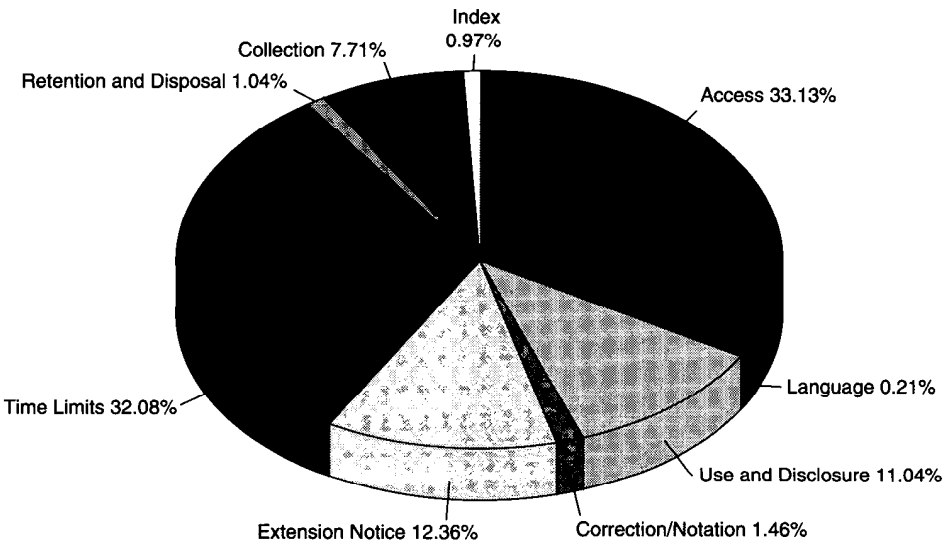
Completed Complaints by Department and Result

Department	TOTAL	Disposition			
		Well-founded	Well-founded; Resolved	Not Well-founded	Discon-tinued
Agriculture Canada	11		1	9	1
Canada Labour Relations Board	1			1	
Canada Mortgage and Housing Corp.	2			2	
Canada Post Corporation	73	30	10	30	3
Canadian Security Intelligence Service	89		2	85	2
Communications, Department of	8	8			
Correctional Service Canada	388	161	40	142	45
Employment and Immigration Canada	147	26	33	74	14
Energy, Mines and Resources Canada	8		6	2	
Environment Canada	9	5	2	2	
External Affairs Canada	14	1	3	10	
Farm Credit Corporation Canada	2		2		
Fisheries and Oceans	2		1		1
Health and Welfare Canada	37	19	5	10	3
Immigration and Refugee Board	36		2	34	
Indian and Northern Affairs Canada	3			3	
Justice Canada, Department of	20	5	3	12	
Labour Canada	4	1		3	
National Archives of Canada	45	21		24	
National Defence	112	26	6	77	3

Completed Complaints by Department and Result

Department	TOTAL	Disposition			
		Well-founded	Well-founded; Resolved	Not Well-founded	Discon-tinued
National Film Board	2			2	
National Parole Board	22	2	1	15	
Pension Appeals Board Canada	3	1	1	1	
Privy Council Office	19	2	2	15	
Public Service Commission of Canada	6		1	3	2
Public Service Staff Relations Board	1				1
Public Works Canada	1			1	
RCMP Public Complaints Commission	3	1		1	1
Revenue Canada, Customs and Excise	53	38	3	12	
Revenue Canada, Taxation	172	86	4	75	7
Royal Canadian Mint	4				4
Royal Canadian Mounted Police	60		2	53	5
Secretary of State of Canada	13	4	2	6	1
Solicitor General Canada	11		1	10	
St. Lawrence Seaway, The	1		1		
Statistics Canada	7			3	4
Supply and Services Canada	1				1
Transport Canada	30	2	5	22	1
Transportation Safety Board of Canada	1			1	
Treasury Board of Canada Secretariat	7			7	
Veterans Affairs Canada	12	2		10	
TOTAL	1440	441	139	757	103

Complaints Completed by Grounds 1992-93



Assessing Compliance

This has been a year of change and adjustment for the Compliance Directorate. In addition to a full workload (nine compliance audits, two special investigations, 12 follow-up audits and a study of information technology from a privacy perspective), the unit became the focal point for an Office-wide operational renewal.

The directorate was originally envisaged as an audit unit which would conduct systematic independent reviews of the 160-odd federal institutions subject to the *Privacy Act*. The workload this generated, combined with the need to examine emerging privacy issues, have proved simply beyond the limited resources available. However, the Office is unwilling to abandon this goal and simply react to complaints.

To meet this challenge, the operations and structure of the directorate have been redesigned. The result is a fresh approach to audit selection (who we audit), audit scoping (what we look at) and methodology (how we investigate). Investigators are shifting emphasis away from physical security and information bank descriptions. They now give more attention to determining whether agencies are collecting only personal information that meets operational requirements, and properly using, sharing and disclosing information. These changes should enhance our ability to investigate privacy issues and reinforce our ability to inform Parliament on privacy matters.

Special Investigations

This year the Compliance Directorate completed two special investigations of potential violations of the *Privacy Act*.

Computer stolen from Veterans Affairs

Last year's annual report reported the theft of a portable computer from an office of Veterans Affairs (VA). Again this year VA

reported a computer containing personal information had been stolen from an employee's home. The employee had the authority to use the computer at home and had taken reasonable measures to secure it and the information it contained. Since our last report, VA has improved security measures to protect personal information stored in portable computers. As a result, the Commissioner decided not to notify the individuals concerned.

Personal computer use has increased dramatically in the public sector during the past decade and not just at the office. With the advent of work-at-home programs (telework) and light, powerful portables, personal information is leaving the workplace. However, our review of departmental practices this year reveals that departments are unable to account for the number, location and use of their personal computers.

It is passing curious that this latest theft at Veterans Affairs is only the second ever reported to this office. Have other computers gone astray but departments either do not have the proper controls in place to identify the losses or to report the incidents to our office?

Personal information found in surplus file cabinets

The office received a call that used filing cabinets being sold at a warehouse surplus store still contained personal documents. Only a remarkable coincidence led to the office hearing about the incident—the caller once worked for the Privacy Commissioner's office. Investigators retrieved the documents and confirmed that they had originated in two federal departments.

The first group of documents included more than a dozen Transport Canada files, one of which was an employee travel expense claim file (the rest were not personal). This file contained substantial detail from the employee's transfer including utility bills, mortgage documents and even a cancelled cheque with his bank account number.

The second group originated with Health and Welfare Canada and was far more sensitive. It contained approximately 370 index cards documenting the lab tests undergone by each individual (but not the results). Investigators immediately notified the two departments and returned the documents.

Both departments investigated and reported back that they have procedures for ensuring that all documents are removed from any equipment declared surplus. Both acknowledged that they had been lax and began briefing staff and improving physical security. Although this office has no evidence to suggest that personal information is regularly being left in equipment declared surplus, the company reported it frequently finds documents in old cabinets.

The incident, while embarrassing for the departments involved, should remind all federal institutions to review their procedures and communicate them to staff.

Audits of Institutions

The Directorate completed audits of nine institutions this year: the Canadian International Trade Tribunal, Elections Canada, the National Library of Canada, the Canadian Transportation Accident Investigation and Safety Board, National Research Council Canada, Veterans Affairs Canada, Bureau of Pensions Advocates Canada, the Canadian Pension Commission and Veterans Appeal Board Canada.

The audit of Labour Canada, begun in 1992, is nearing completion. In addition, Indian and Northern Affairs Canada and the Bank of Canada are currently conducting their own internal privacy audits. Privacy staff will review the results of these audits in the coming year.

Common themes

One summary observation from this year's audits is the improved information management practices and better handling of personal information. This is particularly true in the area of information security and data maintenance. Despite this, audits continue to reveal a general lack of understanding of the *Privacy Act* and the role of this Office, particularly at the operational level.

We found several broad areas of concern during our audits.

Contracting out

Budget cuts and staffing freezes are causing more federal government institutions to contract to the private sector work involving personal information. Prime targets are Employee Assistance Programs, management consulting, computer programming and, in some cases, the day-to-day functioning of entire programs. Our audits continue to reveal that many contracts do not require contractors to comply with the *Privacy Act* and its code of fair information practices. Where investigators did find provisions about handling personal information in contracts, they were so general as to render them virtually ineffective for privacy protection.

Retention and disposal

Investigators continue to find instances of institutions not applying retention and disposal schedules and even of not developing these schedules. Retaining personal information beyond its approved period could harm an individual should staff make decisions about the person on the basis of invalid or out-of-date information.

Info Source descriptions

In six of the nine institutions audited, investigators found information holdings that were not described in the *Info Source* directory or whose descriptions were incomplete or inaccurate. Since the right of access to personal information is one of the cornerstones of the *Act*, accurate descriptions of all personal information holdings are critical.

Access to personnel files

In most institutions audited, managers and supervisors can get access to the complete personnel files of their employees. This provides them access to sensitive personal information beyond their operational needs. This could include information such as divorce documents, support payments and designation of beneficiaries.

Regular readers of these reports will find many of these findings depressingly familiar; evidence the need to educate public servants.

Some Specific Observations

Office of the Chief Electoral Officer

This audit identified two key findings concerning the release of personal information from electoral lists. In the first case, investigators found that information was frequently being released under section 8(2)(m) of the *Privacy Act* to third parties (see Notifying the Commissioner). These disclosures were mainly to individuals to help confirm that they met residency requirements for pension or other legal claims.

However, the electoral office had never notified the Privacy Commissioner of these releases as the *Act* requires. When

investigators pointed this out, electoral staff agreed to notify the Commissioner in future.

The second finding concerned the electoral office's sharing of information from the federal electors list with municipalities to help them prepare for local elections. This disclosure did not appear to be a consistent use and electoral office staff agreed to either stop the practice or conclude formal agreements with individual municipalities to share this information and describe the new use in *Info Source*.

Veterans Affairs Canada

Veterans Affairs is an excellent example of an institution that complies with the *Privacy Act* and the code of fair information practices. Their commitment to training staff in privacy matters is encouraging and greatly facilitates proper management of personal information in the department.

A contract with Atlantic Blue Cross covering the administration of the Treatment Accounts Processing System, reviewed during the audit, could serve as a model for other departments that administer similar programs. Investigators also noted that privacy concerns are automatically considered in the design of the department's EDP systems.

One concern meriting specific mention concerns disposal of documents in the paper recycling bins. Like most departments, Veterans Affairs has an active paper recycling program. Despite instructions to the contrary, periodic inspections by VA security staff (and a sampling by the audit team) revealed personal information in the bins.

Following Up

To support this year's retrospective, investigators reviewed the outcome of several privacy compliance audits and complaints investigations conducted between 1984 and December 1989.

In order to determine whether departments had acted on the Office's recommendations, staff selected 20 audits and 116 recommendations stemming from complaint investigations.

Twelve institutions were examined in the past year: Agriculture Canada, Canada Post Corporation, Correctional Services Canada, Environment Canada, Fisheries and Oceans, Health and Welfare Canada, International Development Research Centre, Solicitor General Canada (Ministry Secretariat), Pension Appeals Board, Public Service Staff Relations Board, Supply and Services Canada and Transport Canada.

Investigators found about 74 per cent of all audit recommendations had been implemented, 16 per cent were partially completed or underway and the remaining 10 per cent had not been addressed.

Summary Observations

Overall, departments have responded positively to the Office's recommendations. Many recommendations have led to departments developing new policies and procedures at the corporate level. Unfortunately, this has not led to similar adjustments in the programs or regions. The reverse is also true; field offices have changed their practices to reflect the audit findings despite the absence of a change in corporate policy.

In general, investigators observed an overall improvement in attitude towards privacy. Government staff (particularly at the working level) are more aware of privacy concerns yet there is still minimal knowledge of the *Act* and its impact on federal

government operations. There is also little understanding of the role and functions of this Office.

These follow-ups also identified the difficulty experienced by some institutions in responding to recommendations involving the retention and disposal of personal information. Employee and client personal information are sometimes retained well beyond approved retention schedules and some schedules have not been approved at all. Departments cited budget constraints and delays at National Archives Canada as the cause.

Highlights by Institution

Agriculture Canada has acted on about half of the recommendations made in the Office's 1988 audit. Agriculture's treatment of personnel files is uneven; regional supervisors in some locations now have access only to relevant employee personal documents as recommended. However, in other locations, they see the entire employee record. Investigators found that 40 per cent of personnel files examined contained outdated employee performance appraisals and one general personnel file included a complete human rights investigation report containing very sensitive personal information.

Canada Post Corporation has acted on many of the recommendations from the 1988 compliance audit and follow-up from individual complaints. Investigators noted improved information bank descriptions, data security and policy development. However, they also found that regions were inconsistent in implementing some of the changes. For example, supervisors' access to employee files has been restricted at headquarters by splitting the files, removing third party information and fingerprints. Unfortunately, this has not been completed in most regional offices visited.

Correctional Service Canada has addressed many of the audit recommendations concerning access to personal information and

improved listings in *Info Source.* In addition, investigators reviewed several complaint investigations concerning disclosure of inmate personal information and confirmed that the recommended controls are now in place.

Environment Canada has not responded adequately to many of the Privacy Commissioner's recommendations. In fact, the Commissioner has not received a formal response to the 1988 audit report. Staff blamed centralization, decentralization and staff changes in the ATIP section for not completing the recommendations. The review found that some locations acted independently to improve protection of personal information and staff awareness. However, the corporate response has been disappointing.

Fisheries and Oceans was the first institution audited by the Office in 1985, serving as a test run for new auditors. Fisheries has complied with recommendations to stop collecting the social insurance number on fishing applications and cease publishing the Fishing Licence Directory containing personal information. However, the department continues maintaining indefinitely the personal records in the Atlantic Commercial Fishing Licence Database (PU-010) formerly Commercial Fishermen's and Vessel Registration bank.

Health and Welfare Canada has amended most of their personal information bank descriptions as recommended in the 1990 audit. The department has had less success disposing of outdated personal information at national headquarters and in one of the regions surveyed.

International Development Research Centre has dealt with most of the audit recommendations and is improving its protection of personal information while negotiating with National Archives Canada for an approved retention and disposal schedule.

Solicitor General Canada (SGC) has acted on most of the eight recommendations for improvement. Its request for an approved retention and disposal schedule from National Archives Canada is still outstanding. Although SGC has not purged staff personal records as recommended, its new automated Resource Management Information System (RMIS) will address this concern.

Supply and Services Canada responded positively to most of the concerns identified, restricting supervisors' access to employee personal records and registering all its personal information holdings in *Info Source.*

Transport Canada has responded to about 70 per cent of the recommendations made in the 1988 audit. Transport must be commended for its disposal of duplicate records containing highly sensitive personal information. However, the department has not yet amended the bank descriptions of its Aviation Licensing Database bank and Vehicle, Ship, Boat and Aircraft Accident bank. In addition, medical examination reports remain part of the Aviation Licensing Database rather than in the medical files, as recommended.

Both the **Pension Appeals Board** and **Public Service Staff Relations Board** have dealt with all our audit recommendations, resulting in proper identification of personal information holdings, better protection of information and an increased privacy awareness.

It's 1993 – Do you know where your information is?

Governments have always been massive collectors of personal data—but the growth of social programs and demand for government services, coupled with governments' vast technical ability to collect, manipulate and share information, make it vital for Canadians to know what governments know about them.

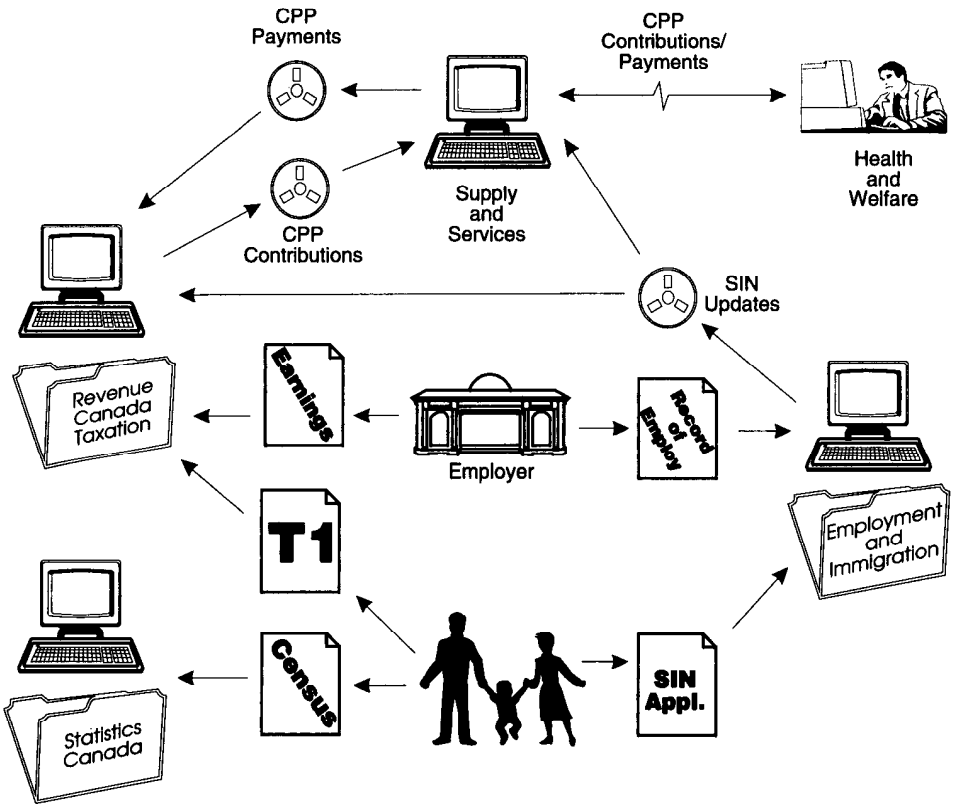
What personal data does the federal government hold? Although far from complete, most readers will recognize themselves somewhere in the following.

A key group of departments holds financial information on most Canadians. **Revenue Canada, Taxation** collects individual tax returns (approximately 17.5 million tax forms) which can contain everything from bank account numbers and charitable contributions to alimony payments and physical disabilities. **Health and Welfare Canada** manages the Canada Pension Plan (CPP) and Old Age Security programs, recording earnings and contributions. **Employment and Immigration** controls the Unemployment Insurance program which includes earnings, work history, benefits payed, and the Social Insurance Number (SIN) master list.

These main departments share information among themselves, primarily for financial checks and balances. For example, each year Revenue Canada gives Health and Welfare (through Supply and Services' computers) information on individuals' contributions to CPP, while Health and Welfare tells Revenue Canada about the CPP payments they make to individuals.

Chart 1 shows how the government collects some of its information from individuals and transfers it to other agencies.

Chart 1: Key Transfers of Personal Information in the Federal Government



Statistics Canada holds information about more Canadians (27.3 million) than any other agency, most of it drawn from the census. Everyone provides basic personal data, as well as their marital status, language, whether they own or rent their housing and who pays the household bills. One in five households provide more details, including ethnic origin, religion, physical and mental limitations, employment and income. Although this information is very personal, Statistics Canada uses it only for statistical purposes. Individuals' names are not entered into the computer (but the paper copies are kept).

Statistics Canada also conducts surveys such as those on consumer finances, health and work history. As well, the agency maintains long term databases on cancer and tuberculosis patients, dental hygienists, registered nurses and elementary and secondary school teachers.

Other agencies gather data from operational programs dealing with immigrants, native peoples, homeowners, Canada Savings Bonds purchasers, students, farmers, people who have changed addresses, and criminals. Some people's dealings with the government necessarily mean providing more details. For example:

- **Immigrants and Refugees**
  Some 6,670,000 individuals have immigrated to Canada since the Second World War. Their files can contain information about education, work history, financial situation, physical and mental health, social and political involvements, criminal activities and family situation. As well, the government collects data about the immigrant's sponsors or hosts.

- **Native Peoples**
  The government has a master index of approximately 530,000 registered status indians, as well as paylists (including family members) for those receiving treaty payments. There are also nominal roles of students living on reserves, attendance records

and grades of those attending federal schools and case files of reserve children and families who receive various social services. As well, there are trust fund accounts, a land registry, small business loan funds and artist and prospectors' programs containing a range of personal and financial information.

- **Pensioners**
  Pensioners' information falls into both financial and medical categories. There are Canada Pension Plan, Guaranteed Income Supplement and Spouse's Allowances files, all containing earnings and payments information. The Old Age Security Program alone has approximately 3,250,000 accounts. Pensioners receiving disability pensions also supplied detailed medical information to support their applications.

  Veterans Affairs also maintains 550,000 accounts for veterans' pensions and benefits. These files can contain sensitive medical information, including complete medical and drug histories on patients in veterans' hospitals. And since some veterans programs impose a means test to determine benefits, some files contain financial information.

- **Armed Forces Members**
  The dictates of their profession mean government has substantial information on current and former armed forces members. All members provide fingerprints, undergo security assessments and medical examinations. Since the forces provide members with ongoing medical care, there are detailed medical and dental files, and occasionally hospital reports. Inevitably members have training and education files, the latter particularly if the member attended a military college. There will also be personnel records, including performance evaluations, awards records, social services or disciplinary records. As well, the forces collect information on family members, particularly when the family lives on a military base or is posted with the member.

- **Inmates and Parolees**
  Current inmates and parolees will have a wide range of personal data in the files of the RCMP, Correctional Services Canada and the National Parole Board. These can include criminal history and court records, medical and psychiatric reports, disciplinary measures imposed, intelligence reports, appraisals and recommendations from the parole board and victim impact statements.

Those who worry about Big Brother can be reassured—there is no one central file containing all these personal details. Some federal departments do share and match personal information but must respect policies and rules set out in various acts. Some federal agencies exchange information with provincial governments under formal agreements. For more details, see *Info Source*, the annual directory of the federal government's information holdings.

Corporate Management

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

Finance

The Offices' total resources for the 1992-93 fiscal year were $6,761,000 and 85 person-years, an increase of $70,000 and three person-years over 1991-92. Personnel costs of $5,351,077 and professional and special services expenditures of $642,835 accounted for more than 88 per cent of expenditures. The remaining $765,086 covered all other expenses.

The following are the Offices' expenditures for the period April 1, 1992 to March 31, 1993*

	Information	Privacy	Corporate Management	Total
Salaries	1,923,405	2,066,562	609,110	4,599,077
Employee Benefit Plan Contributions	306,000	342,000	104,000	752,000
Transportation and Communication	36,468	96,722	134,107	267,297
Information	26,954	69,435	2,242	98,631
Professional and Special Services	402,524	107,240	133,071	642,835
Rentals	9,275	66	12,107	21,448
Purchased Repair and Maintenance	14,758	790	25,511	41,059
Utilities, Materials and Supplies	18,887	11,762	36,841	67,490
Acquisition of Machinery and Equipment	86,709	47,680	130,192	264,581
Other Payments	2,434	1,475	671	4,580
TOTAL	**2,827,414**	**2,743,732**	**1,187,852**	**6,758,998**

* Expenditure figures do not incorporate final year-end adjustments reflected in the Offices' 1992-93 Public Accounts.

Personnel

The unit provided support for restructuring both Commissioners' offices and began implementing the government-wide classification simplification project. The Offices approved a new policy on leave and introduced an employee assistance program.

Administration

The branch reviewed office accommodation and made some improvements. In addition, it introduced new government initiatives to speed up the procurement of goods and services.

Informatics

The Offices received funds to update the case management system and have established a local network and introduced new office automation tools.

Library

The library provides interlibrary loan services, conducts manual and automated reference and research, and maintains subject-oriented media monitoring files. 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 ombudsmen's reports and departmental annual reports on the administration of the two acts. The library is open to the public.

During the year, the library acquired some 560 new publications and answered 1006 reference questions.

Organization Chart