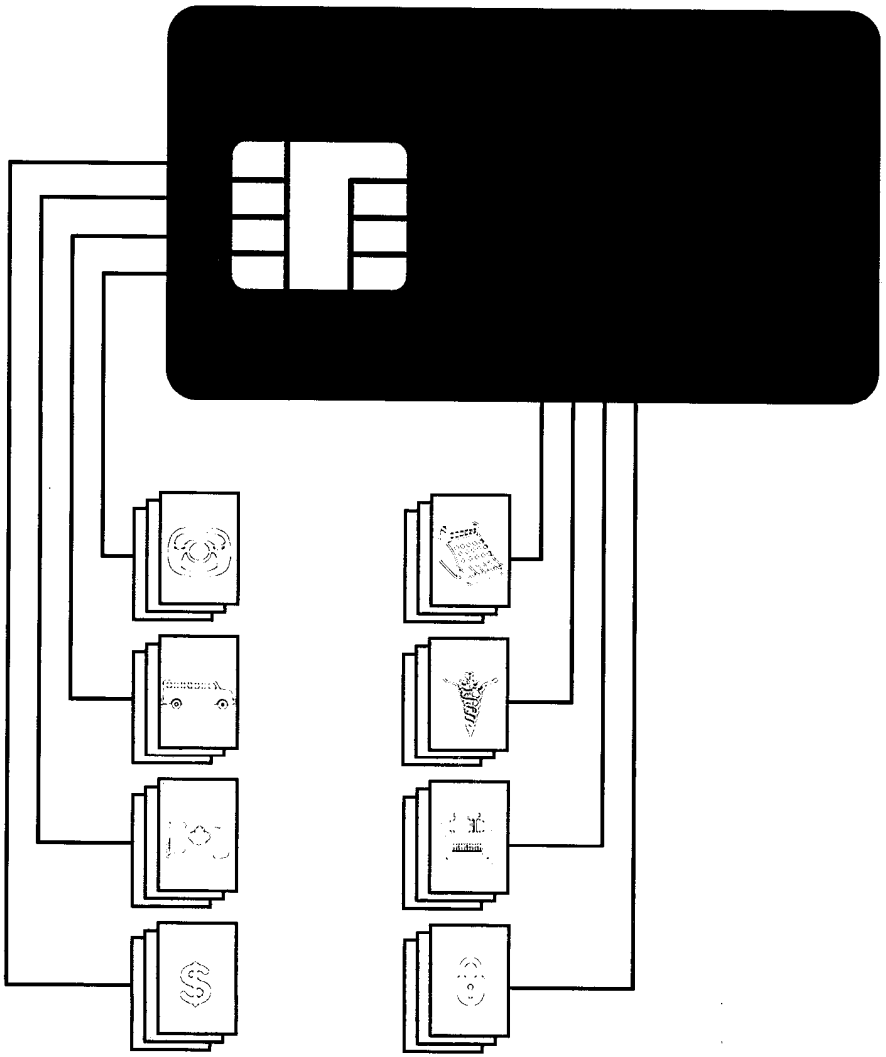
Privacy Commissioner

Annual Report 1991 - 92



Annual Report
Privacy Commissioner
1991-92

Front Cover: The new "smart cards" look like bank or credit cards but there is an essential difference. Imbedded in the card is a computer chip to process and store data and to identify the owner. The symbols illustrate the range of services and personal information that may soon be stored on one small piece of plastic. They are:

- Telephone calling card
- Bus pass
- Federal benefits
- Banking services
- Retail purchases
- Medical records
- Computer system access
- Residence and workplace access

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

© Minister of Supply and Services Canada 1992

Cat. No. IP30-1/1992

ISBN 0-662-59183-6

The Honourable Guy Charbonneau
The Speaker
The Senate
Ottawa

August 12, 1992

Dear Mr. Charbonneau:

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

This report covers the period from April 1, 1991 to March 31, 1992.

Yours sincerely,

Bruce Phillips
Privacy Commissioner

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

August 12, 1992

Dear Mr. Fraser:

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

This report covers the period from April 1, 1991 to March 31, 1992.

Yours sincerely,

Bruce Phillips
Privacy Commissioner

Table of Contents

Mandate

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

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

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

Anyone in Canada may complain to the Privacy Commissioner if:

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

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

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

The Act also gives the Privacy Commissioner the power to audit the way government institutions are collecting, using and disposing of personal information.

The End of the Beginning?

It may be tempting fate beyond prudent limits. Nevertheless, with crystal ball and reputation in hand, the author is willing to venture the opinion that the privacy picture is getting a little better.

Not yet the sunlit uplands, to be sure: disaster areas abound, and the rubble of many a previous privacy defeat remains untouched.

But, carrying Churchillian paraphrase to unreasonable limits, one senses that, while we are a long way from the beginning of the end to privacy problems, we may be close to the end of the beginning.

In plain talk, we seem to be getting somewhere.

During the year under review, there were a number of developments on several fronts which suggest the slow-gathering defences of privacy are starting to make themselves felt.

Both inside and outside of government there were hopeful signs of greater recognition of the problems affecting privacy, and a greater willingness to seek remedies. To itemize a few of the more outstanding ones:

• Two more provinces, British Columbia and Saskatchewan, are in the process of creating privacy protection schemes. A third, Alberta, is considering similar action. Inclusion of these three provinces would extend some form of data and privacy protection at provincial levels from Quebec to the Pacific Coast.

• Federal legislative activity in the fields of telecommunications and financial institutions stimulated refreshingly intense focus on their privacy implications, both by the government and in Parliament. Some of the proposed responses, still under study as this report goes to press, could point the way to a breakthrough in the difficult problem of achieving higher levels of privacy protection in the private sector.

• Some of the major players in the commercial field are responding more energetically to the rising level of public concern about the way business handles personal information under its control. Notable in this respect are Canada's direct marketers, who are working on a code of practice which, if adopted, offers promise that those among us who do not wish to receive unsolicited mail and telephonic sales pitches will be provided with a convenient and well-publicized method of avoiding them.

• Though technically not within the year, there was a landmark decision by the Canadian Radio and Telecommunications Commission (CRTC) in the case of "Caller ID". It established a critical precedent by ruling that telephone subscribers who wished to preserve the anonymity of their telephone numbers would not have to pay a special charge. This ruling clearly recognized that in telecommunications, privacy is recognized as a consumer's right, and not merely as a commodity for sale.

Some of these developments will be discussed in more detail later in this report. They do not constitute in any way a comprehensive account of all that has happened in the many areas of life and commerce which had an impact on privacy during the year. They are presented as examples of a hopeful trend. Taken singly or together, they represent something considerably less than dazzling victories, but something considerably more than deadlock.

However, they must be viewed in the context of the larger problem. For example, all the earnest jawboning of privacy advocates so far has had almost no impact on the biggest and most serious privacy issue of all, which is the vast and unregulated traffic in personal information, a business whose monetary value in North America runs into the billions of dollars. A society which casually accepts the existence of dossiers of unknown accuracy in unknown hands on millions of individuals, and with no rights of access and correction, is a society which is recklessly indifferent to preserving that most basic privacy right: the right to some control over what others know about you. Yet this is the situation as it now stands. There is scarcely one among us whose name is not to be found in one, and probably more of those dossiers in the computer banks of the list-makers and the list-marketers.

It is, though, an indifference born largely of ignorance. There is ample and heartening evidence that wherever and whenever the public at large clearly understands the issues and is given an opportunity to influence them, whole armies rise up to mount privacy's barricades, sometimes with dramatic results.

Item: a couple of years ago, a telephone company in the United States asked its subscribers whether they objected to their information in the company files being sold off to other companies. Eight hundred thousand of them so objected, and the idea was dropped. Likewise, a scheme involving one of the major software companies in the United States to market a machine-readable disc containing information on eighty million persons provoked such a storm of controversy that it too was discarded.

Public reaction — often angry — to the explosion of direct marketing illustrates the critical importance of wider knowledge about the issues. While not implying that marketers are devoid of a sense of responsibility, it would be naive not to acknowledge that it is public concern about the means by which these firms acquire their information which is injecting fresh impetus into the industry's efforts to develop an improved privacy code.

Thus greater public understanding of privacy issues in the modern technological context is a desperate necessity. What simpler and more graphic proof is required than our recent experience with cellular telephones?

Many people were surprised to learn from our last annual report that conversations over cellular telephones could be monitored with easily-obtained scanning equipment. The revelation has not lessened the public affection or appetite for these extremely useful inventions, but we're willing to wager it has made many people considerably more sophisticated or guarded in their use of them.

All that was ever missing in the cellular phone revelation was adequate information. Mass media coverage of the observations of this office helped to fill the information gap. But one would never have been created in the first place had industry been required to ensure that its clientele was provided with all the information needed to make informed decisions about the equipment.

The obligation to inform rests upon both the private and public sectors. In the latter area, the only national agency which seeks to maintain an overview of the entire privacy field is the Office of the Privacy Commissioner. It is, therefore, the natural body to play a lead role in the area of public education and communication. Yet it is a fact (which even some parliamentarians are surprised to discover) that the office has no public education mandate. We do what we can, with almost no resources for the purpose, largely through the medium of this report, speeches and conferences as time permits, and of course the attentions of the media.

None of these factors is to be discounted, particularly the last. Yet much more can and should be done. Forgotten, perhaps, is the government's commitment in 1987 to seek a *Privacy Act* amendment to give the office an education mandate. Let us hope this reminder stimulates action.

Over the years, both the incumbent and previous commissioners have discussed the merits or otherwise of extending the reach of the *Privacy Act* to include federally-regulated private businesses such as banks and transportation companies. In the case of the present Commissioner, this option was regarded not as the best thing to be done, but as possibly the only thing that could be done in the face of apparent failure to obtain good privacy protection in the private sector any other way. The urgency of this question is somewhat diluted by the current examination by Parliament of the privacy problems posed by financial and telecommunications legislation. We must await results to determine whether this case-by-case approach is better. But there are distinct advantages in the sectoral approach made possible by the *Bank Act*, in which

privacy rules for specific industries or services could be developed. This approach is now being adopted in the Netherlands. In the case of Canadian banks, both the Canadian Bankers Association and several of its members already have developed privacy codes which with some improvements and modifications, could well form the basis of a set of regulations governing their handling of personal information. The principal element missing from the codes as they now stand is a system of independent oversight and dispute resolution, which the Commissioner feels is essential to ensure compliance and public confidence. In any event, efforts to produce a more alert and informed body politic is a more urgent priority. An informed public is the best defence against abuse. That holds true for privacy as much as it does for democracy as a whole. It is certainly a pre-requisite to any kind of effective defence.

Charter privacy protection

The value of an aware public must also be considered in the context of a nation which still has no constitutional right to privacy. Although there are various laws such as the federal *Privacy Act*, which give citizens some protection in specific areas of information gathering, and although the Supreme Court has defined a privacy right in some cases—principally involving criminal laws—the acceptance of privacy as a basic human right has not yet found its way into our statutes.

This office has sought to correct this oversight by appearing before the Special Joint Committee on a Renewed Canada to urge that a right to privacy be included among its recommendations.

The submission pointed out that a privacy right was included in almost the very first draft proposed by the federal government when it unveiled its *Charter of Rights and Freedoms*, that it is already included in a number of similar documents such as the *Quebec Charter of Rights*, the *Universal Declaration of Human Rights*, the *European Covenant of Human Rights*, and the constitutions of several states of the American union, to name just a few. Moreover, the proposal has already been favorably viewed by the Commons justice committee (in 1987), and had the support of such important Canadian groups as the Canadian Bar Association.

Unfortunately, the proposal did not command majority support of the committee. Although this office of course was not privy to the committee's *in camera* deliberations, we understand some members expressed concern that inclusion of a privacy right might have an adverse impact on other freedoms or rights, such as speech or access to information. It should be pointed out that a privacy right would be subjected to the same test of balancing the private and public well-being that applies to all rights and freedoms now in the *Charter*. The *Charter* expressly directs that these rights are to be exercised in a manner that is reasonable in a free and democratic society, thereby imposing on the courts the duty to seek a balance between competing or conflicting claims.

The fate of this initiative was particularly disappointing in view of the constitutional exhaustion that is likely to ensue when the current round of negotiations concludes, with the dim prospect of re-opening the *Charter* any time soon. All the same, this is unfinished business on the Commissioner's agenda, and the office will continue to press the case.

Privacy in banking and telecommunications

At the federal level, some kind of Great Divide may have been traversed, with the inclusion of language in two important pieces of legislation which makes it possible to accommodate privacy concerns. The first of these is the revised *Bank Act* and associated statutes, which will make possible the cross-ownership of banks, insurance and trust companies. Given the huge holdings of personal information in financial institutions, this office naturally is concerned by the degree to which these data might be shared in future, and to what extent the consent and control by clients and customers will be involved in the process.

The legislation gives the government authority to make regulations covering such personal information exchanges. In April, the Commissioner appeared before the Senate banking committee to urge that Parliament take advantage of this authority and draft such regulations.

The committee evinced considerable degree of interest in this recommendation, and indicated that the Commissioner might be invited to discuss the subject further. At the same time, the Commissioner understands the Department of Finance is also examining the issue.

A telecommunications bill now before Parliament is even more explicit in recognizing protection of privacy as one of its objectives, the first such example known to the Privacy Commissioner apart from the *Privacy Act* itself.

As of this writing, the outcome of these initiatives is still to be determined. However, the Commissioner must record his satisfaction with this evidence of growing understanding of the privacy issue both in the councils of government and in the federal bureaucracy.

In fact, the Commissioner sees in the above developments a possible answer, or the beginnings of an answer, to the oft-debated issue of regulating information practices in the private sector.
Also on the legislative front, the Commissioner notes with great satisfaction the proclamation of Saskatchewan's *Freedom of Information and Protection of Privacy Act* and the intention of the government of British Columbia to proceed with the introduction of similar legislation. B.C. has engaged the services of Professor F. Murray Rankin as principal consultant, thereby ensuring the process will be favored with both enormous commitment and immense knowledge.

The extension of privacy protection to Canada's third most populous province means that more than 60 per cent of Canadians would enjoy the benefits of privacy oversight at the provincial level (joint Quebec and Ontario). The Commissioner is pleased to report that he has had consultations with officials of one other province now considering similar legislation.

All these developments must be regarded in a highly positive light. They constitute hard evidence that governments more and more are recognizing privacy not only as a right to which all citizens are entitled, but one which in the face of increasingly intrusive technology needs to be supported by its own set of laws and regulations.

The Private Sector: Voluntary Action

As previously mentioned, much of the Canadian banking industry now is covered by voluntary privacy codes. Following the promulgation of a model code by the Canadian Bankers Association, a number of the largest chartered banks have developed their own individual codes. While these codes differ in detail, and while they fall short of what the Commissioner would consider ideal, they share one important characteristic—the recognition that clients and customers have a vested interest in the fate of the personal information which they provide to the banks, and are entitled to some measure of consent and control.

As of this writing, for reasons mentioned earlier, these encouraging if less-than-perfect measures may be overtaken by the revised *Bank Act*. Even so, they provide an important starting point in what should be a joint government-industry effort. If *Bank Act* revisions do not occur, the Commissioner remains convinced that while the banks are to be commended for the progress made so far, their codes will still need to be strengthened.

Also heartening are signs of progress in the direct marketing field, which in recent years and as noted earlier has been the target of much public concern and complaint. The Commissioner commented previously and favorably upon a decision by the Canadian Direct Marketing Association to create a system by which Canadians could have their names removed from marketing lists held by the association's member companies. The association continues to work on an expanded code. It is unpublished as of this writing, but it is the fervent hope of the Commissioner that it will enlarge significantly the role of consumers, at least to the extent that prior consent becomes a condition of inclusion on such marketing lists.

Another promising initiative was undertaken during the year by the Canadian Standards Association (CSA) an organization whose primary responsibility is to ensure the safety and reliability of products marketed in Canada. CSA is most familiar to Canadians from its logo on products which conform to industry standards.

Shortly after the Commissioner's last annual report appeared with its news on the European draft privacy directives, the CSA contacted this office to offer a novel suggestion. CSA proposed formation of a committee to develop a model privacy code, one which would serve as a minimum national standard for private sector organizations handling personal information.

The CSA is ideally placed to develop such a code. It is an independent service organization of business, industry, labour, academia and regulators. This new proposal is a natural extension of the organization's involvement in international technology standards and its interest in technology's impact on consumers, business and industry.

A workable model code for the private sector would balance trade and business interests with consumers' inherent right to privacy. It would also demonstrate Canadian industry's commitment to the privacy principles contained in the OECD guidelines—and thus respond to the EC's requirement for "equivalent or adequate" protection.

The CSA code's committee (of which the office is a member) has drafted a proposal and has already received indications of interest and funding from AMEX, Readers' Digest, Bell Canada, Equifax and the federal departments of Consumer and Corporate Affairs and Communications.

If necessary, CSA will hire an experienced consultant to conduct research and work with the committee to develop the code. Once consensus is reached, the code will serve as the foundation, to be supported by various technical standards. It will become the cornerstone of a national compliance framework to help different business sectors establish privacy codes suitable for their particular environments.

The Commissioner strongly endorses CSA's approach and has committed the office's support. Private sector organizations interested in workable privacy solutions might find CSA's approach just what they are looking for.

Privacy At Work

Privacy in the workplace is an issue of rising concern, highlighted by the decision during the year of two major companies (Toronto-Dominion Bank and Exxon Canada) to introduce drug testing programs. Previous studies by the Office of the Privacy Commissioner have stressed the very limited utility of drug testing programs, and have concluded that the results to be gained do not justify the intrusive methods required. Developments in the past year suggest that the time has come to consider means by which individual privacy rights can be accommodated in areas of industrial activity which have special safety or other problems. It is not the Commissioner's view that no case can ever be made for testing programs; it is decidedly his view that such programs must meet demonstrated tests of both need and effectiveness.

Fine-tuning the Act

The *Privacy Act* has been part of the landscape for nine years, long enough for observers to form at least some interim judgments about its effectiveness. It is entitled to high marks.

The doctrine of fair information practices which is the heart of the *Privacy Act* has proved highly adaptable to a wide variety of situations in a rapidly-changing environment, and gives every sign of long life expectancy. Certainly, a better set of principles has yet to be devised.

The chief limitation of the Act is that it applies only to records in the custody of the Government of Canada and some of its agencies. Fair information practices have found their way into the laws of only a few other jurisdictions, and hardly at all into the private sector. So by far the largest part of personal information holdings in Canada continues to be unprotected.

Unless and until that situation changes, the *Privacy Act* will continue to be the most important piece of privacy legislation in the country, both for the immense holdings of personal information it covers in the Government of Canada, and for the benchmark against which data protection standards in other areas can be measured.

Thus, while the Act has weathered well, it needs to be constantly re-assessed, not in the sense of major overhaul but, if the phrase may be used, of "polishing the jewel". One comprehensive parliamentary review took place in 1986-87, as required by subsection 75(1) of the Act. But six years of added experience suggest it may be time for another.

Surprisingly though, we advise fine-tuning the Act's strengths: the definition of personal information (section 3), the fair information practices code (sections 4 to 8) and the access to personal records protocol (sections 12 to 28).

Redefining "personal information"

The *Privacy Act* architects could not have foreseen today's new technologies when they defined personal information. Advances in the science of genetics, for example, give added meaning to the words "information about an identifiable individual recorded in any form" (section 3—definition of personal information).

Locked in the smallest drop of body fluid or speck of tissue is a mountain of information that defines in minute detail the characteristics not only of individuals but also those of their forbears. Though paragraphs 3(b) and 3(d) refer to medical information and blood type, it is not clear that information recorded in biological samples about an identifiable individual falls within the scope of section 3. While it is clear the office would argue it does, any controversy regarding its inclusion could be eliminated by amending section 3. What is sought here is a clear statement that information contained in a genetic sample is personal information for purposes of the Act.

Some may argue that such an amendment is unnecessary tampering with an already elegant definition. But the genetic key is potentially so damaging to our privacy that a specific reference in the Act is needed.

Tightening up disclosures

Sections 7 and 8 of the Act are the foundation upon which are built our confidentiality rights. Its cornerstone is the principle of informed consent. Personal information cannot be used or disclosed without the concerned individual's knowledge and consent.

The *Privacy Act* demonstrates the truism that rules often need exceptions. Exceptions are necessary to strike a balance between an individual's right to confidentiality and the government's responsibility to manage the affairs of state. It is, for example, reasonable for personal information to be disclosed without consent to meet legal requirements or for criminal investigation purposes.

Curiously, one of the strengths of the legislation is contained in one such exception—paragraph 8(2)(m), disclosures in the public interest. The Act does not prevent public interest disclosures nor does it attempt to substitute detailed written rules for the reasoned and considered judgment of the head of an institution. It simply provides a transparent framework which ensures all interested parties are informed and that discretion regarding disclosure is properly exercised. The head of the institution who, after all, knows the records best, must balance the benefit to the public against the harm it may cause the individual.

However, most disclosures without consent do not require the head to exercise discretion. This may be delegated to staff. In this respect, the section is deficient. Staff should not be delegated the responsibility for consistent use disclosures; exchanges of information with foreign states or with the provinces; disclosures to investigative bodies, to Members of Parliament, to researchers, to auditors or to associations of aboriginal people. Since they are serious derogations from the prior consent principle, the head of the institutions should be required to decide on these disclosures.

This process might also resolve another difficulty with consistent use disclosures. Subsection 9(1) requires government agencies to notify the Privacy Commissioner of new consistent uses not recorded in *Info Source*—the personal information index. The office has received and assessed only 18 such notifications in its entire history. Our complaint and audit experience shows clearly that new consistent use disclosures are happening routinely without proper notification of the Commissioner. Surely higher level accountability would produce a more diligent application of all of the Act's requirements.

The Commissioner would welcome some fine-tuning of sections 7 and 8. The major flaw in the fair information practices code is its failure to provide a mechanism for an individual to prevent the release of personal information pending a determination of the propriety of its release. As previous annual reports have stated, it is an anomaly that individuals denied access to their personal information may go to court for review of the decision, but they cannot seek a review of a department's decision to disclose their personal information to third parties.

The *Access to Information Act* provides a mechanism for alerting third parties, such as corporations, whose sensitive commercial information may be shared. Yet, the *Privacy Act* provides no similar rights to individuals whose sensitive personal information may be disclosed. Does not personal information deserve protection from abuse that is at least the equal of that afforded corporate information?

True, in matters of national security or criminal investigations it may not be possible, or wise, to provide an individual with prior notice before disclosing sensitive personal information. These disclosures can be properly documented for the Privacy Commissioner's review.

Broadening the injury test

While the *Privacy Act* gives Canadians an impressive array of access rights, it also gives government institutions a vast—cynics might say limitless—arsenal of exempting provisions to defeat them. These exemptions are not unreasonable if they can be supported by clear, strong rationale. Most of them are. Who, for example, would want terrorists to learn that law enforcement agencies were hot on their trail, simply by applying for their records?

But some exemptions go too far. For example, government agencies can or must withhold personal information under sections 19, 22(1)(a) and 22(2) without demonstrating that release would cause some injury. These provisions concern, respectively, information obtained from other governments, law enforcement information, and information obtained by the RCMP while providing policing services to a province or municipality. Solicitor-client information (section 27) can also be withheld without a requirement to demonstrate that its disclosure would be harmful.

However, paragraph 22(1)(a) is certainly the most offensive. This section authorizes the government to deny access to personal information prepared "in the course of lawful investigations pertaining to the enforcement of any law of Canada or a province", provided the investigation was conducted by an "investigative body". There are nine such bodies listed in regulations to the *Privacy Act*. The exemption amounts to carte blanche to these bodies to deny Canadians access to their information for no reason whatever. No agency should be entitled to this kind of denial.

Generally this section has not been abused. The RCMP, for example, which has the right to use the exemption, rarely invokes it, preferring to use other sections of the Act. On the other hand, some cases demonstrate clearly how it can be misapplied.

One example concerned the Department of Consumer and Corporate Affairs (CCA). CCA's director of investigation and research investigated a complaint that the Parliamentary Press Gallery had violated federal competition rules when it denied an application for membership. CCA's investigation found no violation but, confronted with the complainant's subsequent privacy request for the opinions of Press Gallery members about his application, the department refused, taking refuge in paragraph 22(1)(a). Since CCA's investigation was complete, the Privacy Commissioner could find no valid basis for CCA denying the privacy request. However, the department was unyielding, and, given the blanket authority conferred by the section, he could do nothing more.

This kind of blanket exemption should be stricken from the Act. It has proved unnecessary even in such sensitive areas as police investigations. As it stands, it merely provides a convenient shield for bureaucrats not wanting to be troubled by the tiresome need to justify their decision. The following paragraph (22(1)(b)), with its injury test, provides a reasonable framework to allow government institutions to effectively manage their programs.

The scope of this exemption explains the Commissioner's reluctance to applaud additions to the list of investigative bodies. During the year, the Commissioner learned that three new bodies were being considered. The quarrel is not with the particular bodies being considered but rather with the concept of any investigative bodies at all. Other exemptions—subject to an injury test—provide all the latitude needed. The Commissioner's office is now part of a working group examining the exemption, its uses and some options for the future.

"Catch 22"

One final preoccupation about the Act needs addressing in this report.

Section 16 allows an institution to refuse to either confirm or deny the existence of personal information. To most of us at least, other exemptions provide a more than sufficient limitation to the general right of access. Section 16, though, goes far beyond the mere refusal to provide access.

The doctrine of refusing to confirm or deny is ingrained in Canadian security and policing psyches, and it would seem that section 16 is its statutory embodiment. As distasteful as the notion is in a free and democratic society, it may be necessary for us to tolerate its use in order to achieve a public good. But invoking this section with any exempting provision other than those concerned with security and policing (sections 21 and 22), would surely constitute an unacceptable encroachment on an already too highly encumbered and fragile right of access. The Act should be amended to limit this authority to national security and criminal investigations.

The threat to our privacy rights is compounded because though the Privacy Commissioner may investigate complaints about this section, he cannot reveal any information or even that there is no information!

Should the Privacy Commissioner be unable to resolve the complaint, he faces Catch 22. Simply by referring the matter to Federal Court he runs the risk of revealing the existence of information, thus breaching his own Act. The Act needs a mechanism to enable the Commissioner to refer these complaints to the Courts for adjudication.

Genetic Testing

It is easy to overlook the privacy implications of technologies many of us do not yet fully understand. Nowhere does this pose a greater danger than with genetic testing.

Advances in genetic technology promise to unravel medical mysteries, thus preventing many diseases and allowing treatment of others. The technology can already identify many genetic traits or disorders and, occasionally, accurately predict our genetic destinies. This news is good. But there is also the inevitable dark side. Genes can reveal deep secrets about individuals' physical and psychological being—secrets they may not want others to know, or may not want to know themselves. Stripping away the human being's very essence to the twisted strands of DNA molecules—the personal genetic building blocks — is an assault on privacy that few may want to endure.

Do governments or other organizations have a right to acquire personal genetic information "for the public good", with or without consent? Or should individuals be able to protect their genes from inspection by either the state or the private sector?

This year the office completed its report, *Genetic Testing and Privacy,* the third in a trilogy on biomedical testing. (The first two dealt with HIV/AIDS and drug testing.) The latest report examines the issues flowing from the rapid development of genetic testing technology, including several present or potential uses. These tests could be designed to select genetically fit employees or monitor the effects of workplace hazards on their health; determine eligibility for such benefits or services as insurance; diagnose or predict medical conditions during regular medical care or reproduction (pre-conception, prenatal and neonatal), and provide more accurate forensic evidence in criminal investigations.

To date, genetic testing in Canada appears to have been limited to three fields — reproductive technology, regular medical care, and criminal investigations. Still, the advent of cheaper, more informative tests will almost certainly stimulate further interest in testing. Governments will not be the only intruders. Private sector interests, such as employers and insurers, will become increasingly enthusiastic about the supposed ability of genetic testing to give them a competitive edge.

Governments may be tempted to override serious ethical concerns and apply genetic knowledge to promote eugenics. Certainly today's world is not free from pressures to thus create "better societies". In the private sector, genetics could be used to identify genetically "inferior" individuals. For these unfortunate members of the genetic "underclass", access to employment or services could be severely impaired.

In both environments—government and private sector—people could find genetic traits over which they have no control determining how they will be permitted to lead their lives, with little concern shown for the person behind the genes.

This office was chilled by the potential growth in the number and types of intrusions that may ensue as genetic technology advances. Accordingly, the report recommends against mandatory (and, in some cases, voluntary) genetic testing in several situations. It also calls on the federal government to study the extent of genetic testing in Canada, and the likely future uses of this technology.

Prominent recommendations of the report are:

- every person should have a reasonable expectation of genetic privacy;

- governments should collect personal genetic information only if specific statutory authority permits;

- neither government nor the private sector should compel persons to learn their genetic traits or disorders;

- employers should not require genetic testing in employment, whether to identify undesirable genetic traits in employees or applicants, or to identify genetic changes due to workplace exposures; only true voluntary testing would be allowed;

- service or benefit providers should not be permitted to use mandatory genetic testing to determine a person's eligibility for services or benefits;

- governments should not collect personal genetic information relating to the reproductive process;

- governments should not collect personal genetic information relating to ordinary medical care;

- governments should restrict forensic DNA analysis in criminal investigations to identifying offenders or exonerating suspects;

- governments should not establish personally identifiable genetic databases or banks of genetic materials from the general population for crime control.

The report merely scratches the surface of genetic testing. The Commissioner hopes it will stimulate thought and action before powerful public or private sector interests transform us all from human beings into the mere sum of our genetic parts.

Telecommunications toys—playing with privacy

Readers of these reports may recall the former Privacy Commissioner's concern about the privacy threats in new telecommunications technology (1989-90 report, p. 26). The Commissioner cited Bell Canada's new Call Management Services (CMS)—and Caller ID in particular. The CRTC has since approved Bell Canada's service and similar ones are now available from most telephone companies.

Caller ID is just one element of the new telephone technology. Many new phone services are not features of improved telephone sets but the product of powerful computers which handle telephone switching operations. However, users do need specially equipped telephones to allow them to see and record the caller's phone number before picking up the handset.

Seeing the caller's number before answering may provide protection against harassing calls. But it also trades away the rights of others who have an equally legitimate desire to avoid having their phone number known or recorded.

This desire—or need—for anonymity is obvious for those calling crisis hot lines or for volunteers who often return calls from home. Many professionals—from psychiatrists to probation officers, from politicians to undercover police officers—may now be unable to call from home, not wanting their numbers displayed and recorded.

Many are also concerned about commercial use of their phone numbers. Anyone calling a business with a casual inquiry now courts the risk of having their number recorded, only to be called back for marketing purposes. Reverse directories (which list subscribers sequentially by phone number) can then link the number to a person and address.

Trading away everone's privacy is a heavy cost for CMS' few benefits. Charging subscribers to **prevent** the display of their numbers means privacy is for sale and not everyone will be able to afford it.

These concerns are well-founded and workable solutions are elusive. CMS can vary from one phone company to another, making privacy protections a patchwork. Some companies allow callers to block the number display for all calls on their line—or just selected calls—but at a cost. Some charge nothing to block. Others offer a form of encryption which scrambles the number. Nearly all companies offer a solution for women's shelters.

One recent CMS decision comes from the Manitoba Public Utilities Board. The board approved Manitoba Telephone System's application for a trial run, providing that all subscribers benefitted from free call blocking. The board also demanded free line blocking for shelters and individual victims of abuse. However, the board did not approve Call Return—the option which traps the numbers of unanswered incoming calls and displays them later on command.

Of broader significance is the CRTC's recent announcement–well after the end of our reporting year–that phone companies under its jurisdiction must offer free per-call blocking.

Canada is not alone in its struggle to find appropriate solutions for technological advances. In the United States, the debate has raged since New Jersey introduced the service in 1987—a debate involving public utility commissions, state and federal legislatures and even the courts.

And the solutions range from New Jersey's, which offers no blocking at all, to Pennsylvania where CMS has been ruled illegal since it offends the state wiretap law.

Texas proposes that customers pay if they want to display and, most recently, an administrative law judge in California proposed that the state utilities commission prohibit Caller ID because it is not in the public interest and violates both the state and federal constitutional right to privacy.

Still other states offer free per-call blocking, pay-per-line, free per-call **and** per-line blocking. At the height of the debate, one company even offered a service to automatically refuse blocked calls. The options are dizzying.

The debate has focussed public attention on the privacy issue. Probably more disturbing is the knowledge that these services are only the beginning—an early feature of the ever-increasing intelligent network system. This system will soon offer personal communication networks with a lifetime personal phone number, dial-up services and picturephones. The technology is evolving so fast that neither engineers nor policy makers have time to consider the social impacts. Each new development affects or overrides the privacy protections so laboriously erected to defend against the last one.

Obviously the Privacy Commissioner's small office cannot keep abreast of each new technical marvel; it lacks the expertise and resources. Nevertheless, the Commissioner is eager to find enduring and workable solutions.

The New York State approach has substantial appeal. That state's public service commission took a broad policy approach to telecommunications privacy, approving eight privacy principles. They state, for example, that telecommunications companies should recognize clients' privacy explicitly and that customers should not pay extra to preserve their privacy status quo. Customers should be told of any proposed use of their information and be able to give informed consent to any further uses.

The office and the Department of Communications are both examining the broad issue of telecommunications impact on privacy and considering some remedies.

New Telecommunications Act

A step in the right direction may be the initiative in the proposed *Telecommunications Act* in which Parliament recognizes the privacy impact in telecommunications technology. The act includes as a policy objective

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

This act also allows the government and the CRTC to block such intrusions as unsolicited phone calls and junk faxes.

The office intends to monitor passage of this bill through the House to help ensure that the privacy protections are not eroded. At issue is whether its provisions go far enough. Either the act or its regulations should outline the privacy standards which telecommunications services must meet.

This year's SINs

Born without SIN

Resistance to demands for the Social Insurance Number (SIN) took an unusual turn this year when a Prince Edward Island couple refused to apply for a SIN for their newborn baby.

PEI's vital statistics department requires all newborns to be assigned a SIN for the province to use as identification numbers for its Health Service Payment Plan. The couple asked for an exemption and were denied. The health department responded by refusing all claims for the baby's medical care because she did not have a SIN.

The couple has taken the case to court, arguing that requiring the baby to have a SIN (and denying the medical claims) offends several provisions of the *Canadian Charter of Rights and Freedoms*. The parents maintain that their daughter has no legal obligation to obtain a SIN until she begins insurable employment. They argue further that denying the medical claims offends *Charter* protections against unreasonable search and seizure and denies the baby's right to equal benefit of the law, and requiring a baby to have a SIN breaches an individual's reasonable expectation of privacy.

The case is interesting to this office, although well outside the *Privacy Act*. But it does raise an important privacy question: what program or activity of Employment and Immigration Canada (the department responsible for issuing SINs) allows it to issue the numbers to newborns?

SINs were created for unemployment insurance and Canada Pension Plan, and later authorized for use by Revenue Canada for individual income tax reporting. Recent federal government policy—applauded by the Privacy Commissioner—has reined in many unrelated federal government uses of the numbers. However, apparently EIC still relies on a 1970 federal-provincial agreement concluded well before any federal privacy protection was in place.

The Commissioner has asked Employment and Immigration to identify a direct relationship between assigning SINs for birth registration and EIC programs. If none can be shown, he will urge EIC to reconsider its arrangement with PEI in light of both the *Privacy Act* and the federal government's policy to restrict SIN use to a short list of social programs.

Casting the first stone—
renumbering the public service

One significant impact of the federal policy to restrict its own use of SIN is the need to re-number some 310,000 public servants, members of the military and RCMP.

Supply and Services Canada (which controls the pay and records data bases) will begin assigning new Personal Record Identifiers (PINs) by January 1993. Each employee will receive two numbers: the PIN and a second number to be given to third parties such as banks, insurance companies and the employees' unions. This second number will ensure that employees' PINs remain private but allow the employer to link third party transactions to the correct employee.

There remains some confusion about what constitutes a proper request for a person's SIN. For example, the Public Service Commission's language testing programs still ask employees to volunteer their SIN and public service unions continue to use SINs for membership purposes. These are legitimate requests. But once the renumbering is completed, the Commissioner urges federal employees to keep their new PIN to themselves.

SIN or else

The Commissioner's office was alerted to what seemed to be an unnecessary use of SIN in Employment and Immigration Canada's new automated Job Information Bank in St. John's, Newfoundland. The pilot project allowed job seekers to scan a computerized listing of available positions and select those that matched their interests and skills. The system gives applicants greater opportunity and frees up EIC staff for other duties.

However, a caller complained that he could not even look at the list without first providing his SIN. Since any casual passer-by can scan the paper notices of jobs available, he thought demanding a SIN for a computer listing was excessive and—since he was not claiming unemployment insurance—unneccessary.

Apparently EIC asked for the SIN to measure both the effectiveness of the system and its ability to place UI claimants. Responding to the office's enquiries, EIC acknowledged that the system should also accommodate non-UI claimants.

The system has now been modified. The opening screen advises users that access to the system is unrestricted. Those receiving unemployment insurance have the option of entering their SINs so that the Canada Employment Centre has a record of their job search. This change will become part of the new nationwide job-bank system.

Technology update

Last year the Commissioner reported on Employment and Immigration Canada's (EIC) plans to harness new information technology to handle the department's huge client load. EIC had pilot projects underway using smart cards and an automated telephone answering service (AVRES).

EIC is not the only federal department considering using new information technology to improve service. Veterans' Affairs has already tested smart cards as a method of improving its delivery and billing of prescription drugs to veterans. Revenue Canada is looking at the possibility of having travellers use the cards to declare goods or pay fees at customs points.

Several departments are jointly developing smart cards which would allow remote access to government computers. This would permit someone working at a home personal computer to communicate with a government agency's computer over the telephone.

As with much of the new communication technology, there are privacy implications.

The smart card is like a conventional bank or credit card—but with an essential difference. Smart cards are imbedded with an integrated circuit chip which gives the card intelligence for processing and memory for storing data. Chips and digitized information also make it possible for the cards to carry an invisible photograph or even a fingerprint of the bearer. The cards could be used to provide banking, telephone and medical services, giving the user access to a network of computers.

Privacy needs

Clearly smart cards are an important technical advance which can improve service to clients and control costs for departments—particularly those like EIC which must track, credit deductions for and pay benefits to such large numbers.

Yet government agencies and their clients should be able to enjoy the benefits of progress without sacrificing individuals' control over their personal information. In effect smart cards could become that universal identity card that North Americans so fiercely resist. Their development invites a profound shift in the relationship between the individual and the state.

This can be avoided, first, by making the systems transparent to the clients. Card bearers must know their inherent rights when using the card, what information the card contains, how it will be used, and what risks that use implies.

Individuals should be free to refuse the card without jeopardizing their access to the service. And similarly, holding a card should not confer advantages unavailable to those who opt out.

Finally, the systems and their participants must respect both privacy laws and basic ethical principles on collection, handling and disclosure of personal data.

Because of the Commissioner's concern about the security aspects of the pilot projects, his staff were invited to join two federal government working groups: one dealing with applications of the technology and the other developing standards for remote access to computer systems.

The applications group—whose ultimate goal is to establish standards and guidelines for all government smart card applications—will identify how government might use the cards and the framework in which they should operate. Its membership includes such federal agencies as Health and Welfare Canada, Supply and Services Canada, the RCMP and Veterans' Affairs, as well as the Quebec and Ontario health ministries.

The office is also a member of a special interest group working on the development of remote access to computer systems. Since many government agencies have a common interest in access, they are sharing research and development costs and contributing to shared standards.

The AVRES Project

Last year's report (p.53) described a privacy flaw in EIC's automated telephone inquiry system being tested in Quebec City. The story ended unsatisfactorily since the project seemed too far advanced to change. However, EIC has re-written the ending and the Commissioner could not be more pleased.

The system allowed claimants with touch-tone telephones to call into a computer for routine information about their own unemployment insurance claims. For example, a caller could confirm that his or her claim had been accepted and when benefits would begin. Callers identified themselves by their Social Insurance Number (SIN) and birthdate. The office heard about the service when a local radio station questioned this use of SIN.

There was no question that EIC could use SINs to identify UI claimants—the numbers were devised for this purpose. But the Commissioner was concerned about the lack of security of the SIN-birthdate combination. The office discussed the problem with EIC staff who agreed that both pieces of personal data are widely available and therefore not a secure access code. However, the test project had already expanded to London and Peterborough and it seemed too late for changes.

Nevertheless, aware of the Commissioner's concern, EIC systems designers used the Peterborough project to test a new four-digit telephone access code similar to a bank number.

Apparently the test was successful and the new code will be a feature of the national program. EIC will assign claimants the number to identify themselves when making telephone inquiries. Claimants may also choose their own numbers.

The Commissioner applauds EIC's quick response and its sensitivity to client security.

Data Matching

Probably the most important data matching news this year is what did not happen—apparently data matching did not happen. The Commissioner received just three notifications during the entire year—all from Agriculture Canada.

The Commissioner wishes not to appear suspicious. Yet it would be credulous to accept that of more than 150 federal agencies subject to the government's data matching policy, only one began any new matches of discrete sets of files during 1991-92.

The matching policy restricts linkages between computer data bases that could produce detailed dossiers—or "super files" on individuals. It also requires federal agencies to submit matching proposals to the Commissioner 60 days in advance. He then assesses the match against a set of criteria and acts as an advocate for the subjects of the files. The intent is to prevent government efficiency from trampling individuals' personal information rights.

The policy, while admirable, may not be working. Only 22 federal agencies describe anything remotely resembling a data match in their listings in *Info Source*—the federal information directory. Some departments couch matches under more benign headings like "use" or "disclosure". And others only recognize a match when it links with data from an outside agency, contrary to the policy which also controls matches of different program files within an agency.

Everything the Commissioner has seen leads him to conclude that computer data matching is common in government—particularly with social programs, law enforcement and intelligence operations and the criminal justice system. Do government staff recognize a data match? Are they unaware of the policy? Or do they simply see the policy as a nuisance to be avoided?

The Commissioner urges the Treasury Board to investigate. In the meantime, the Commissioner's compliance auditing teams have added data matches to their list of audit criteria.

Agriculture Matches

In fairness, Agriculture Canada has been scrupulous in observing the data matching policy. Its first notice advised that the new *Farm Income Protection Act* would allow Agriculture to match farmers' information from the income stabilization account with income information from Revenue Canada.

The match will ensure that the benefits farmers receive from these programs are based on correct information about their revenue, expenses and production. The act gives Agriculture legal authority for the match and allows it to use the Social Insurance Number.

Garnishees for Family Support: Agriculture also advised the Commissioner that it would match information from the Western Grain Stabilization Program with the Department of Justice to allow garnishee of program payments from farmers who had defaulted on their family support. In fact, the submission was unnecessary because Parliament had passed a regulation under the *Family Orders Agreements Enforcement Assistance Act* authorizing deductions from the stabilization program.

More Information Needed: Finally, the Office was notified of a match between Farm Debt Review Board files and Quebec agriculture department records. The match supports a new program to subsidize beef feed lot operators and to mediate with farmers' creditors. The Office has not received sufficient detail to assess this match.

Complaints Directorate

The office received 1,402 new complaints this year compared with 1,239 last year—an increase of 13 per cent. This increase is consistent with the pattern established since the office opened in 1983. Not consistent is the drop in the number of completed cases—782 cases were closed, 269 of which were well-founded, 448 not well-founded and 65 discontinued.

The 1991 Census

During the past year, one issue has consumed considerable time—investigating 34 complaints against the 1991 census. Several complainants were concerned about Statistics Canada's collection of personal information and had refused to respond to census questions they considered an unacceptable invasion of their privacy.

Others cited the guarantee (or lack) of confidentiality of their census responses. The most frequent complaint was that census workers who gathered the results were neighbours or acquaintances of the complainants. Complainants believed that their completed questionnaires would be sent directly to Statistics Canada in Ottawa to be reviewed by some anonymous bureaucrat, not by someone from their neighbourhood. The investigation is now in its final stages and its results will soon be shared with Statistics Canada.

This is the first time this office has undertaken such a complicated and time-consuming investigation, and it has taken its toll. The nearly six months spent by three senior privacy officers who spearheaded the investigation took time away from other cases. This is the main reason that the number of completed cases is lower than last year. Staff turnover (and subsequent training) has also contributed, thus exacerbating a growing backlog.

A New CPIC Policy

The Canadian Police Information Centre (CPIC) continues to be the target of complaints and inquiries about the collection, use and disclosure of personal information held in its databases. CPIC is a collection of police databases, federally funded and administered by the RCMP. However, it is governed by an advisory committee of major municipal and provincial police forces who contribute and have access to the information.

We often hear from individuals who cannot get access to their own information in CPIC because various police forces cannot disclose information contributed by others. For example, CPIC may not disclose personal information contributed to it by the Ottawa City Police.

This office has discussed its concerns about CPIC's administration in earlier reports and recommended that the RCMP consult other CPIC users about introducing voluntary privacy controls over its databases. This would provide comprehensive protection for CPIC's collection, use and disclosure of personal information, and allow individuals to access and correct their personal data.

Congratulations are in order. CPIC approved and implemented a CPIC Code of Ethics in November 1991, one which generally addresses the Commissioner's concerns—particularly those dealing with access rights. It entitles individuals to request access to their personal information maintained on CPIC and to correct it, when necessary.

Top Ten

Last year, for the first time the office listed its top ten clients—a group which accounted for 80 per cent of the total caseload. Eight of those ten departments made the list again this year: Correctional Service Canada (CSC), Canada Post Corporation, Employment and Immigration Canada, Revenue Canada-Taxation, National Defence, Canadian Security Intelligence Service(CSIS), RCMP and National Archives.

Joining the top ten is the Immigration and Refugee Board (IRB) with 68 complaints received—the first privacy complaints received against IRB. However, 67 of those were made by one person, including 33 time limit complaints which were considered well-founded. Investigation of the 33 access complaints continues.

Completed Complaints by Grounds and Results

		Disposition				
Grounds		Well-founded	Well-founded: Resolved	Not Well-founded	Discontinued	TOTAL
Access		5	102	260	41	408
	Access	5	100	228	41	374
	Correction/Notation	0	0	29	0	29
	Index	0	0	3	0	3
	Language	0	2	0	0	2
Privacy		5	12	92	13	122
	Collection	1	2	35	4	42
	Retention & Disposal	1	1	6	6	14
	Use & Disclosure	3	9	51	3	66
Time Limits		142	3	96	11	252
	Time Limits	138	3	90	11	242
	Extension Notice	4	0	6	0	10
TOTAL		152	117	448	65	782

Another significant increase occurred at Revenue Canada-Customs and Excise. Their 72 complaints constitute a five-fold increase over last year's figures.

Last year's report applauded CSC for its efforts to conquer its delay problem. Unfortunately CSC's delay complaints more than tripled this year—160 (compared with 50 last year). These delays account for 34 per cent of the year's time limit complaints. However, this warrants an explanation. CSC has changed the way it processes information about inmates that it receives from provincial and municipal governments and police forces. CSC routinely used to exempt information received in confidence from another government. However, after years of urging from this office, CSC now asks the originator whether it will agree to disclose.

This causes delays for applicants. With heavy caseload and shrinking resources, CSC has to choose between two evils: providing a less than complete response in time—or go the extra mile, risk exceeding the time limits but provide the applicant more information.

Other departments also continue struggling to meet time limits: National Archives, Revenue Canada-Taxation and National Defence.

Toward the end of the reporting year, the office changed the way it reported time limits complaints. Frequently, complainants question departments' claims of a time extension either to consult other organizations or because operational requirements prevent them from responding within 30 days. The office did not count the number of complaints specifically questioning the notice. But time limits complaints have now been divided into two categories: time limits and extension notices. The change acknowledges the distinction between the two issues. It also identifies departments which continue to neglect their responsibilities to respond in time.

At a time of government restraint it is difficult to chastise departments for not respecting the time limits. Budgets and staff have been slashed in most government departments with the result that service to the public suffers.

While the number of time limits and access complaints received increased by 31 per cent from 855 last year to 1118 in 91-92—the number of complaints about improper collection, use and disclosure dropped by 26 per cent—from 384 in 90-91 to 284 in 91-92.

How Institutions Measured Up

The RCMP continues to carry the banner for maintaining its high regard for the letter and spirit of the Act. Only one of its complaints was well-founded, resolved; 40 were not well-founded, while three were discontinued. CSIS too must be commended; of the 56 complaints completed last year, only five were considered well-founded, and all were resolved.

Last year CSC had the highest ratio of well-founded complaints, with EIC, Taxation and DND not far behind. This year, despite continuing to head the list of complaints received (a total of 287), only 27 per cent of all CSC's complaints were well-founded. Approximately one-half of the complaints against EIC and Taxation, and 32 per cent against DND were well-founded.

This year's number of discontinued findings is high—65 represents eight per cent of completed cases. However, the majority were discontinued when the office's initial notice to the departments prompted them to resolve the problem. Of course, that's what the ombudsman's role is all about—resolving problems, not counting complaints.

Top Ten Departments by Complaints Received

		Grounds		
Department	TOTAL	Access	Time Limits	Other
Correctional Service Canada	287	92	160	35
Canada Post Corporation	143	101	3	39
Employment and Immigration Canada	135	72	26	37
Revenue Canada, Taxation	107	27	59	21
National Defence	99	20	63	16
Canadian Security Intelligence Service	87	77	10	0
Royal Canadian Mounted Police	84	67	4	13
Revenue Canada, Customs & Excise	72	29	31	12
Immigration and Refugee Board	68	33	33	2
National Archives of Canada	47	14	23	10
OTHER	273	119	55	99
TOTAL	1,402	651	467	284

Proposals for New Exempt Banks

The office was consulted twice during the year on proposals to create new exempt banks. The RCMP advised the Commissioner that it intended to seek Cabinet approval to create an exempt bank for its National Security Investigation Records. CSIS also notified the Commissioner of its proposal to seek an exempt bank for its Investigation Records.

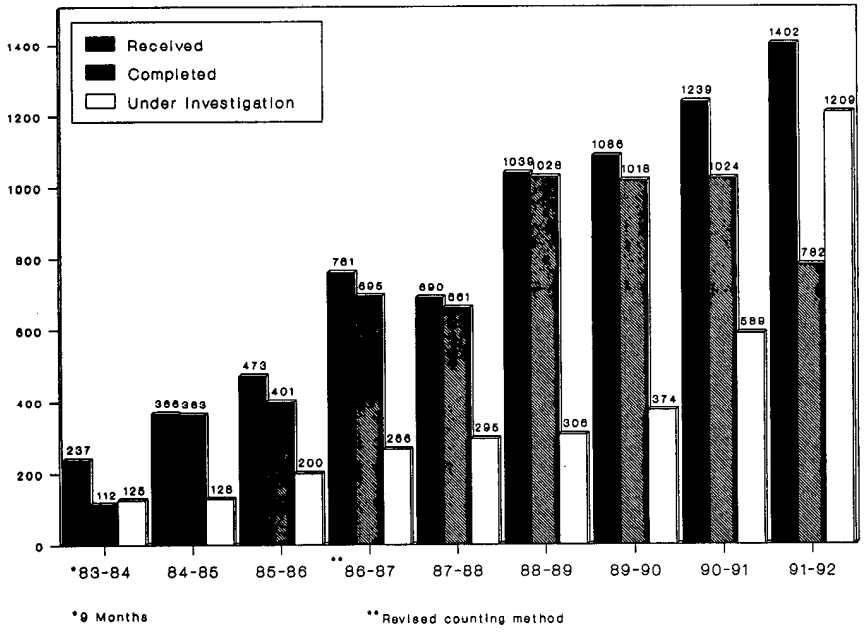
A staff review of both banks determined that they consist predominantly of personal information obtained or prepared during criminal investigations or whose release could damage the conduct of Canada's international affairs or defence (sections 21 and 22 of the *Privacy Act*). The Commissioner would not comment personally on the validity of the exemptions in order to avoid any conflict of interest should he receive a complaint about information contained in the files.

The Constant Plea for More Resources

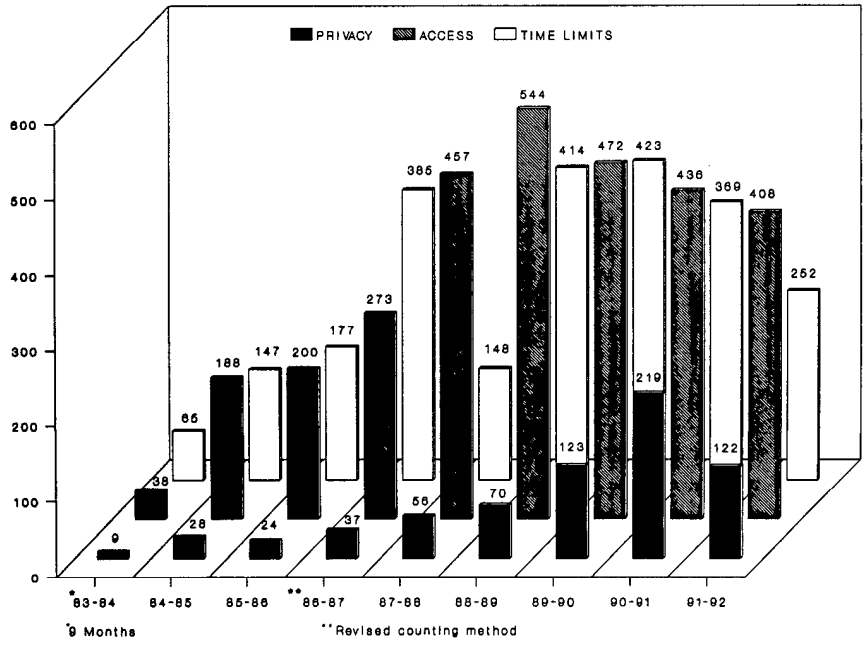
The 13 per cent increase in new complaints has put the office behind by almost a full year's caseload—1209 cases pending at year end. As predicted in last year's annual report, the backlog increased investigators' workloads to 200 each. Thus clients are now kept waiting sometimes months longer than they should to receive the Commissioner's finding.

Treasury Board allotted the office two additional person years to hire more privacy officers. But if new complaints continue to arrive at last year's pace, the office faces the spectre of more than 2000 open cases. This risks becoming unmanageable.

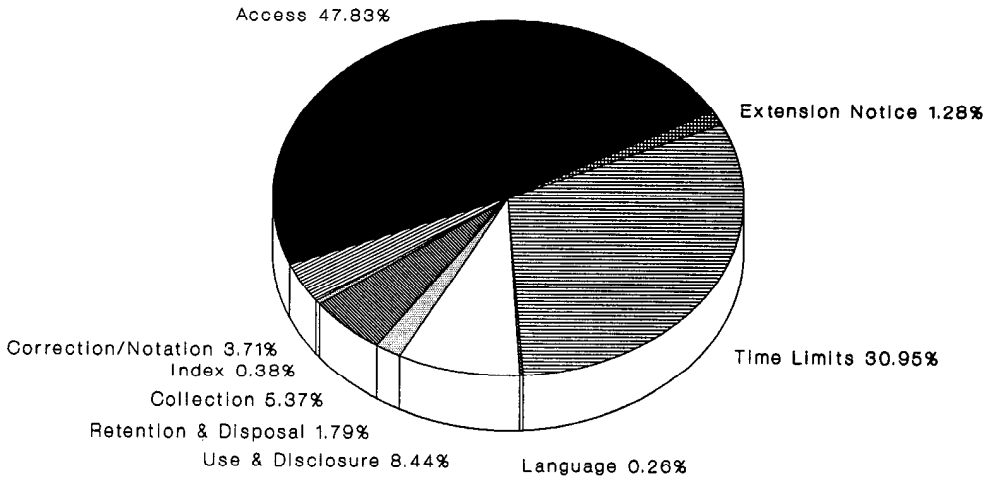
Completed Complaints 1983-92



Completed Complaints and Grounds 1983-92



Complaints Completed by Grounds 1991-91



Origin of Completed Complaints

Newfoundland	5
Prince Edward Island	4
Nova Scotia	43
New Brunswick	20
Quebec	48
National Capital Region Quebec	17
National Capital Region Ontario	114
Ontario	226
Manitoba	28
Saskatchewan	30
Alberta	94
British Columbia	144
Northwest Territories	4
Yukon	2
Outside Canada	3
TOTAL	782

Completed Complaints by Department and Result

Department	Dispositions				
	Total	Well-founded	Well-founded; Resolved	Not Well-founded	Discontinued
Agriculture Canada	3	0	2	1	0
Atomic Energy Control Board	1	0	1	0	0
Bank of Canada	2	0	1	1	0
Canada Post Corporation	67	2	9	55	1
Canadian Human Rights Commission	2	0	0	2	0
Canadian Radio-Television and Telecommunications Commission	1	0	0	1	0
Canadian Security Intelligence Service	56	0	5	42	9
Commissioner of Official Languages	1	0	1	0	0
Communications	1	0	0	1	0
Consumer and Corporate Affairs Canada	9	0	0	3	6
Correctional Service Canada	130	10	25	76	19
Employment and Immigration Canada	71	11	22	30	8
External Affairs Canada	13	0	7	6	0
Farm Credit Corporation Canada	1	0	1	0	0
Fisheries and Oceans	10	1	1	8	0
Forestry Canada	1	0	0	1	0
Health and Welfare Canada	7	2	0	5	0
Immigration and Refugee Board	34	33	0	0	1
Indian and Northern Affairs Canada	11	7	0	4	0
Justice Canada	8	0	1	7	0
Labour Canada	3	2	0	1	0

Completed Complaints by Department and Result

Department	Dispositions				
	Total	Well-founded	Well-founded; Resolved	Not Well-founded	Discontinued
National Archives of Canada	10	2	1	6	1
National Capital Commission	1	0	0	1	0
National Defence	110	25	10	65	10
National Parole Board	35	6	5	23	1
Office of the Superintendant of Financial Institutions Canada	3	2	1	0	0
Privy Council Office	1	0	0	1	0
Public Service Commission of Canada	6	0	3	2	1
Public Service Staff Relations Board	1	0	0	1	0
Public Works Canada	2	0	0	2	0
Revenue Canada, Customs and Excise	25	15	4	5	1
Revenue Canada, Taxation	67	31	4	31	1
Royal Canadian Mint	1	0	0	1	0
Royal Canadian Mounted Police	44	0	1	40	3
Secretary of State of Canada	2	0	0	1	1
Solicitor General Canada	5	0	0	5	0
Statistics Canada	3	0	0	1	2
Supply and Services Canada	7	1	0	6	0
Transport Canada	20	2	12	6	0
Veterans Affairs Canada	7	0	0	7	0
TOTAL	782	152	117	448	65

Some Cases

CPIC limits AIDS identifiers

A group of community organizations in Vancouver asked the Privacy Commissioner to look into allegations that Canadian Police Information Centre (CPIC) databases identified individuals as HIV positive.

Although no one could point the finger at a specific incident—and the office's jurisdiction over CPIC is questionable—the Commissioner decided to inquire informally.

The RCMP (which administers CPIC) explained that individual CPIC files could contain a "C" flag to indicate that the person has a contagious disease. The flag helps police find individuals with communicable diseases who have escaped from penitentiaries or wandered away from hospitals. It also helps police inform those who may have been exposed to disease.

The CPIC advisory committee asked for a legal opinion on identifying HIV/AIDS carriers. As a result, CPIC policy now forbids identification of carriers unless they have threatened to transmit the condition using physical violence or, for example, if a carrier has violated the public health act by willfully spreading the virus.

CPIC contacted all CPIC users to explain the new policy and a subsequent audit identified 96 "C" entries (not necessarily HIV/AIDS). Since then CPIC has reminded users and done yet another audit which found fewer than 40 "C" files remaining—all for *bona fide* law enforcement reasons.

Finally, an RCMP member and the privacy investigator met the coalition members in Vancouver to brief them and answer questions. The coalition appeared satisfied with the outcome. The Commissioner is particularly grateful that CPIC and the RCMP were willing to listen and respond to the group's real concerns.

Respondent should see entire file

A complaint about the Public Service Commission's handling of an application to see a personal harassment investigation file revealed what seemed to be inconsistent treatment.

The applicant (the respondent in the harassment case) was given only those parts of the file that PSC considered his personal information. The investigation revealed that PSC processes harassment files differently, depending on who is the applicant. When the applicant is also the complainant, PSC considers the entire file that individual's personal information and discloses everything except that which may be exempted under the *Privacy Act*.

However, when the applicant is someone else—for example, witnesses or the respondent—PSC processes only those records considered to be the applicant's personal information.

The privacy investigator considered that since the applicant was also the alleged harasser and lone respondent—and the entire file dealt with the investigation of a complaint against him—PSC should process the entire file.

PSC officials have agreed that when the respondent is an individual (rather than the department), it will process privacy applications from both complainants and respondents in the same way. This means that all information on the PSC investigation file will be disclosed unless it may be exempted under other provisions.

Since the applicant had not been denied access to any of his own personal information, his complaint was not well-founded. However, his complaint prompted PSC to disclose the remainder of the file which did not qualify for exemption and to change its processing methodology.

New spouses get equal treatment

An employee of the Communications Security Establishment (CSE) told his supervisors of his pending marriage, a requirement of all federal employees holding a secret or top secret security clearance. The employee provided his bride's name, birthdate, address and name of present employer—as required by the government's Personnel Security Clearance Questionnaire.

However, CSE also requested details of the new spouse's residence and employment from the previous five years. At that point, the woman complained to the Privacy Commissioner that CSE's demands for more information invaded her privacy. She also held that CSE should have asked her directly for the information and not collect it from a third party.

The investigation revealed that CSE's policy on security reliability checks was inconsistent with most other federal government departments which rely on the information on the employee's security questionnaire. As well, new CSE employees are not required to provide the more detailed information about spouses. Only established employees who change their marital status must provide their new mate's residence and employment history.

DND was the only other department found to demand this supplementary information in similar circumstances, asking for details of residence and employment over the previous ten years.

Without question, details of relatives' personal history is needed to conduct background checks on those in a position to influence employees with access to national security secrets. However, it was difficult to understand why CSE needed more personal history of new mates of its established employees than of spouses of new employees.

CSE officials were persuaded to bring their policy in line with other departments. Ironically, before the Commissioner's office pursued the matter with DND, its policy had already been amended.

The complaint was well-founded but resolved.

Bulletin boards no place for grievance responses

A National Defence employee complained to the Commissioner that his supervisor had posted on a bulletin board DND's response to his formal grievance about smoking in the workplace. The department's letter included his name, address and comments on DND's policing of its anti-smoking policy.

The investigation found that indeed the letter had been posted in the room where the complainant worked, in full view of other civilian and military employees. Apparently a manager had told the man's supervisor to post the letter as a reminder to personnel to comply with the anti-smoking policy.

Following the investigation, DND agreed that the personal letter should never have been the mechanism for reminding employees not to smoke in DND buildings. DND has ensured this will not happen again.

The Commissioner considered the complaint well-founded.

Employees' personal papers not for disclosure

During its investigation of a harassment complaint Revenue Canada-Customs searched the office of an employee it suspected of writing an anonymous note found on a colleague's desk. Revenue Canada investigators photocopied the employee's personal phone directory and took documents from his personal files to have analyzed by handwriting experts.

Discovering this, the employee complained to the Privacy Commissioner that Revenue Canada had improperly disclosed his personal information. The Commissioner's investigation established that personal documents had been taken; used during the harassment investigation, and disclosed outside the department without the complainant's consent.

The documents included employee benefit statements—including some medical information—and his completed personal record form which lists education, previous employment, personal references and identifies family members, their occupations and addresses. The Commissioner concluded that the use of this type of personal documentation during an internal investigation could hardly be "consistent" with the original collection purpose. He considered the complaint well-founded.

Revenue Canada-Customs has apologized to the complainant for disclosing the documents and has amended its investigation manual to prevent investigators from using such personal information without the individual's consent.

Anonymous tipster not EIC

A complainant alleged that Employment and Immigration Canada (EIC) had disclosed to his ex-wife information about his earnings from his unemployment insurance file. She then used this information in a court application to increase his support payments.

The investigator interviewed the two EIC employees who dealt with the complainant, both of whom denied disclosing any of his personal information to any unauthorized persons. The ex-wife and her current husband were also interviewed. They too denied having obtained the information from EIC, saying that the tip-off came from an anonymous caller.

The Commissioner concluded that there was no evidence to support the man's allegation that EIC staff were the source of the information and he dismissed the complaint.

Complainant revealed identity himself

A man complained to the Commissioner that Employment and Immigration Canada (EIC) officials had identified him to an EIC-funded organization as the applicant seeking information about it under the *Access to Information Act*. The complainant correctly observed that identifying him as the applicant was an improper disclosure of personal information.

The investigation established that the complainant had had a dispute with the managers of the organization which provides on-the-job training to otherwise unemployable individuals. The complainant then made annual access requests to EIC for information about the organization. He was well known to its staff and is alleged to have spoken openly about his requests for the centre's records.

When the latest request arrived, the manager simply assumed it was from the same person. As he said: "it didn't take a rocket-scientist to figure it out".

Without evidence to support the allegation that EIC revealed the source, the Commissioner concluded that the complaint was not well-founded.

Can mail blind persons' audio tapes "sealed"

A blind person complained that Canada Post's requirement that letter and talking book tapes be mailed unsealed violated his privacy rights.

The investigator found that blind persons can mail audio tapes free of charge. However, the material must be packaged so that Canada Post personnel can open it easily to ensure that it meets the regulations.

The complainant agreed to have the investigator discuss the matter with the Canadian National Institute for the Blind (CNIB). CNIB explained during the meeting that its free postage privilege amounts to an almost $3 million a year subsidy, which CNIB is reluctant to jeopardize.

Cassette tapes must be sent in special padded mailers. For talking books (the bulk of its mailings) CNIB has developed a re-usable plastic pouch with a Velcro closure. According to CNIB, this is as much for convenience as for ease of inspection. For other mailings, small padded envelopes are used and are either taped or stapled shut. Canada Post does not object to taping or stapling and the CNIB had never heard of a blind person being challenged on this type of closure.

CNIB pointed out that the regulations require that the closure permit easy inspection of the contents. It does not forbid sealing the envelopes. He suggested that the complainant simply staple his envelopes shut so that it would be relatively easy to tell if the envelope had been opened.

CNIB illustrated Canada Post's flexibility on the use of the free mailing privilege with anecdotes of blind individuals mailing back their cassette players to CNIB for repairs, claiming (and receiving) the free mailing privilege. According to CNIB, these mailings are definitely not covered by this privilege.

The investigator explained the entire procedure, as well as the CNIB's position, to the complainant. He was satisfied that Canada Post was not unnecessarily violating his privacy rights. The Commissioner concluded that the complaint was not well-founded.

Disclosure an error—but whose?

A complaint against the RCMP illustrated that sometimes it is impossible to get to the root a problem.

A man complained to the Commissioner when he learned that the RCMP had sent an unsolicited copy of his fingerprints and criminal records to Canada Post. There was no apparent reason for this disclosure since the man had received a pardon for his conviction. The records should have been sealed.

The investigator was unable to get a satisfactory explanation—audit trails were unclear and eventually the Privacy Commissioner's decision had to be based on "best available" information.

The investigation showed that in early 1991, Canada Post security received a copy of the complainant's criminal history record from the RCMP. Although this is normal procedure when its employees or candidates undergo security screening, security staff had no record of requesting the information. The complainant was not a employee, nor was he an applicant for a position. The record was put in a "pending" file.

At the investigator's request, the RCMP examined its records and found the distribution notation "Post Office, Ottawa" next to the man's criminal conviction listing. However, this did not explain why it had sent an apparently unsolicited copy of the record to Canada Post.

Further inquiries showed that the man had been briefly employed by Canada Post more than 10 years before. A reliability check (including fingerprinting) was done at that time. This explained the original distribution reference to the post office. Once he left the position, his personnel records—including his fingerprints—would normally have been transferred to the National Personnel Records Centre.

The complainant, once again a federal government employee, recently underwent a periodic review of his security clearance. This required the RCMP to process his criminal history record. Since no-one had removed the distribution notation on the old record, the updated record was sent to Canada Post.

This explanation is largely a reconstruction of events based on probabilities; it is not definitive. The Privacy Commissioner concluded that there had been an improper distribution of the information but, given the lack of detail, he could not say who was responsible.

However, he was able to reassure the man that Canada Post no longer possessed either the fingerprints or criminal history record and that the information had been well-protected for the brief period it was in Canada Post hands. The RCMP no longer has the fingerprints.

Denial "legal" but unnecessary

An Ottawa man asked the Commissioner to investigate his complaints against Consumer and Corporate Affairs (CCA), including one that alleged it had improperly denied him access to his personal information. He had lodged a complaint with CCA under the *Competition Act* and, unhappy with the investigation, wanted to see the comments about him in the file.

The Commissioner's investigation confirmed that CCA had withheld some information collected by its Director of Investigation and Research (DIR), claiming that it had been collected during a lawful investigation. Since the directorate is one of those units identified as "investigative bodies" in the *Privacy Act*, paragraph 22(1)(a) allows it to refuse to disclose information obtained in the course of its investigations.

The information requested was collected while DIR was investigating a complaint under the *Competition Act*. Thus it was lawful to refuse disclosure. However, the Commissioner observed that the exempted information was relatively innocuous and the complainant probably already knew its substance. Yet, representations and reasoning failed to persuade CCA to disclose the information. It clung steadfastly to its right to refuse, despite there being no reasonable probability that giving the man the information would harm the investigation or any person.

Since section 22(1)(a) does not require CCA to satisfy an injury test, the Privacy Commissioner had to tell the complainant that—much as he disagreed with CCA's stand—it complied with the letter of the law. He had to find the complaint not well-founded.

Ontario Workers' Compensation files no longer "confidential"

A lawyer complained that Health and Welfare Canada denied him access to 20 pages from his client's Canada Pension Plan disability medical file which had originated with the Ontario Workers' Compensation Board (WCB).

At Health and Welfare's suggestion, the lawyer applied directly to the WCB and received more material than Health and Welfare had exempted, leaving him unable to determine which documents Health and Welfare had used to deny his client's application. He argued that he could not properly represent his client in a pension appeal without knowing exactly which documents the department had received from the WCB.

The investigator found that Health and Welfare had withheld 20 pages using section 19(1)(c) of the *Privacy Act*. This section requires federal institutions to exempt information supplied "in confidence" by provincial governments or their institutions. There is no flexibility or discretion.

Thus, once a provincial or municipal government claims confidentiality, federal agencies may not disclose the information regardless of how innocuous it may be.

The investigation confirmed that a December 14, 1983, agreement provided that all information from the Ontario Workers' Compensation Board to Health and Welfare Canada was confidential and not to be disclosed except by the WCB itself.

Despite the agreement, the investigator persuaded Health and Welfare to ask WCB officials for permission to release the material. Health and Welfare did so and, as a result, WCB changed its policy, authorizing Health and Welfare to release its information directly to applicants. Health and Welfare then disclosed the client's material to the lawyer.

This is an important policy change which should simplify the procedure for many applicants.

The Commissioner concluded that the complaint was not well-founded because Health and Welfare previously had no authority to release the WCB's records. He applauded the change of position.

Notifying the Commissioner

Forty-three times this year the office was notified by government agencies that they intended to release personal information "in the public interest" or to "benefit" an individual. The Commissioner's role in this process is simply to notify the person if he considers it appropriate. He may advise against—but not prevent—the release.

Staff examine these notices so that the Commissioner remains free to consider any complaints without having prejudged the disclosure.

Although section 8(2)(m) of the Act is intended for exceptional disclosures, many notifications have become repetitive and something of an administrative burden for both the department and the Commissioner's office.

For example, Multiculturalism and Citizenship routinely notifies the Commissioner when confirming the Canadian citizenship of nominees for the Order of Canada. Since this was a recurrent and routine use of citizenship documents, the office suggested the department acknowledge this publicly and change its listing in *Info Source* to describe this use of citizenship documents. The department agreed, eliminating paperwork for itself and providing the public a clearer picture of how citizenship information may be used.

Correctional Services disclosures—a reprise

Last year the Commissioner reported on the difficult balance between individuals' privacy and the public interest—particularly on the release of reports on two prison escapes during which three persons were murdered (see Annual Report 1990-91).

The solicitor general refused to give the Justice and Solicitor General Committee uncensored versions of the investigation reports, maintaining that the *Privacy Act* prohibited the disclosure.

His refusal became the subject of a question of privilege in the House of Commons and the then-acting Privacy Commissioner was called to testify before the Privileges and Elections Committee. The acting Commissioner saw no difficulty with the solicitor general providing uncensored reports to an *in camera* committee hearing.

The privileges committee report concluded "that there is nothing in the *Privacy Act* to prevent the House of Commons from issuing an order for the production of unexpurgated versions of the two reports. Accordingly, we do not believe that an amendment to the *Privacy Act* to permit such production is either necessary or desirable".

The report suggested making copies available to the Justice committee at an *in camera* meeting.

The following are samples of other public interest notices received during the year.

Release prompts complaint to Commissioner

The Privy Council Office (PCO) advised the office that it intended to disclose personal information about several individuals to a professional body inquiring into the conduct of two of its members. The documents had been produced in evidence before a federal commission of inquiry.

PCO had obtained the consent of one individual (who was not under investigation) but considered it impractical to obtain everyone's consent. The Commissioner's office believed that the individuals should be notified of the impending release but suggested that it would be less disturbing coming directly from PCO. Privy Council agreed and wrote to each person, setting out the reasons for disclosure and citing the permissive section in the *Privacy Act*.

One of the professionals under investigation objected and has since complained to the Privacy Commissioner.

Details released for possible bravery award

The RCMP advised the Commissioner's office that the Chancellery of Canadian Orders and Decorations (in the Governor-General's Office) had asked the Force for information on one victim of a 1972 Arctic plane crash. The Chancellery was considering awarding a posthumous bravery decoration to a young Inuit man who survived the crash and kept the injured pilot alive but died before both could be rescued.

The Chancellery was reconsidering the award following publication of a second book on the accident which detailed the young man's role in the pilot's survival.

The privacy investigator examined the material that the RCMP proposed to release and found it contained less personal detail than the transcripts of a coroner's inquest or either book on the crash. The proposed disclosure did verify the accuracy of some of the details in the book.

The office did not object to the release and concluded it need not notify the sole survivor since the information was already public.

Pilots and engineers list not released

National Defence (DND) asked Transport Canada for a list of helicopter pilots and maintenance engineers in the Ottawa area to notify them of job opportunities at DND.

The Commissioner's office is reluctant to support this type of wide-scale list disclosure when there are other means of communicating with the individuals. Disclosure might "benefit" those who got jobs, but not the other several hundred who did not. The office suggested Transport Canada mail notices for DND, or that DND simply place advertisements in local newspapers and professional journals.

Transport Canada decided not to provide the list.

Post-mortem to family doctor

A doctor asked National Defence for the post-mortem of a military member who died suddenly while jogging. The doctor was treating a member of the man's family and wanted to determine whether the officer had the same condition which could contribute to a heart attack. Since the condition is suspected of being hereditary, the doctor wanted to begin immediate treatment of other family members.

DND released the post-mortem, then notified the Commissioner's Office. Although the Office prefers to be notified in advance, the request arrived during the public service strike when DND had no office staff. There was no objection to the disclosure.

Korean veterans' list to Rideau Hall

The Governor General's Office was the source of another request for personal information, this time about Korean War veterans. This notice provided a good example of how easily communications can become muddied over the telephone.

The Chancellery asked Veterans Affairs Canada for access to its computer database containing personal information about veterans eligible for the Canadian Volunteer Service Medal for Korea. The personal details—names and addresses, language, service number and confirmation of eligibility—would speed processing of applications for the new Korean War medal. The Governor General's office wanted to present the awards in November 1991.

Veterans Affairs staff telephoned the Commissioner's office to discuss the request and were left with the impression that they would need written consent from each veteran. (In fact, consent was just one of the avenues suggested.) This message was conveyed to Chancellery staff who, understandably frustrated, called the offices directly.

Privacy staff asked to see a written notification and sample of the information to be taken from the database. Once they had examined material, it was apparent that everyone on the list had indicated an interest in the medal and therefore would benefit. Staff also suggested Veterans Affairs obtain a written undertaking that the Chancellery would use the data only for this purpose, then destroy it or return it to Veterans Affairs.

The misunderstanding was cleared up quickly and the Governor General presented the first of the medals at a ceremony in Ottawa on November 10, 1991.

False claim to Canadian citizenship

External Affairs advised the Commissioner's Office that it proposed to tell a foreign government that a man arrested overseas on drug-related charges was not a Canadian citizen, even though he carried a Canadian passport.

The foreign government had seized the passport and given it to External Affairs on the understanding that if indeed he were Canadian, Canada would issue travel documents once the man was released. Since he was not a citizen, the Canadian embassy would not provide consular services or travel documents.

The Commissioner's Office agreed to the disclosure because there is a significant public interest in the integrity of Canadian passports. And it is important that Canadians not be alarmed by reports of consular services being denied to "citizens" whose claims are actually false.

Inquiries—the Public Talks Back

Inquiries officers continue to respond to an ever-mounting tide of letters and telephone calls—4,671 of them during the year. The offices' national toll-free line (shared with the Information Commissioner) is the only nation-wide access and privacy information service.

Canadians are becoming more aware of existing privacy protection, as well as new or proposed legislation governing provincial and municipal governments. Saskatchewan has just proclaimed its *Freedom of Information and Privacy Act*, and both British Columbia and Alberta have promised similar legislation in their latest throne speeches.

However, callers are shocked to discover that the private sector remains totally unregulated. The office handles many calls from individuals faced with difficulties in examining or protecting their information held by private organizations. It is frustrating to confess that there is nothing the office can do since our jurisdiction is limited to the federal government. Even worse is being unable to suggest a route to solve many callers' problems.

Although the *Privacy Act* is a federal law, hundreds of federally-regulated agencies and companies, and most Crown corporations, are "unregulated"—including Canadian National Railways, Via Rail, Air Canada, Atomic Energy of Canada Limited, various ports corporations, telephone companies and financial institutions such as banks and insurance companies.

The office has also answered calls about handling personal information in MPs' offices and at the Royal Commission on the New Reproductive Technologies. Employees and clients are dismayed to hear that we cannot intervene nor can they use provincial or municipal laws.

A substantial part of the inquiries officers' time is spent explaining the limited controls on use of Social Insurance Numbers (SIN). Most believe SIN use was restricted by the legislation which created unemployment and pension programs in the 1960s. Despite promises made at the time, that is not so. Many callers find it difficult to accept that only the federal government limits its use of SINs.

Individuals too often must choose between protecting their SIN or getting the goods and services they want. Given our limited mandate, staff now encourage callers to write to their MPs in the hope that if more MPs hear the complaints, they might act to control unnecessary uses of the SIN.

But the SIN story is not all gloom. Several organizations **are** interested in the SIN issue. During the past year, we sent background information to the Regional Municipality of Waterloo, the Ontario Ministry of Revenue, the Universities of Saskatchewan and Quebec, Nova Corporation and Maritime Telegraph and Telephone Company Ltd.

And there are kudos for the Quebec access and privacy commissioner's office for investigating SIN abuses in Quebec government agencies. Unlike most provinces which avoid the issue because SIN is a federal number, the Quebec commission seized the initiative and intervened under its own access and privacy legislation. For example, Quebec no longer demands a SIN to get a fishing permit for provincially controlled areas. As well, the automobile insurance industry has informally agreed to stop forcing clients to provide their SIN.

And the Quebec commission is now examining other provincial uses of the SIN including:

- Hydro-Québec's authority to use the SIN to identify both employees and subscribers;
- the Université de Laval's collection of SIN from students; and
- SIN use by hospitals, nursing homes and housing authorities.

It is encouraging to find that the federal government's efforts have had some impact outside its immediate jurisdiction.

Despite efforts to fine-tune listings in the blue (government) pages of telephone directories, more than half of the calls on the national toll-free line are unrelated to access or privacy. The receptionist re-directed 9343 callers to Reference Canada, the federal government's central information service. The office will make another attempt now that Bell Canada and the government telephone authority are working to improve the blue pages.

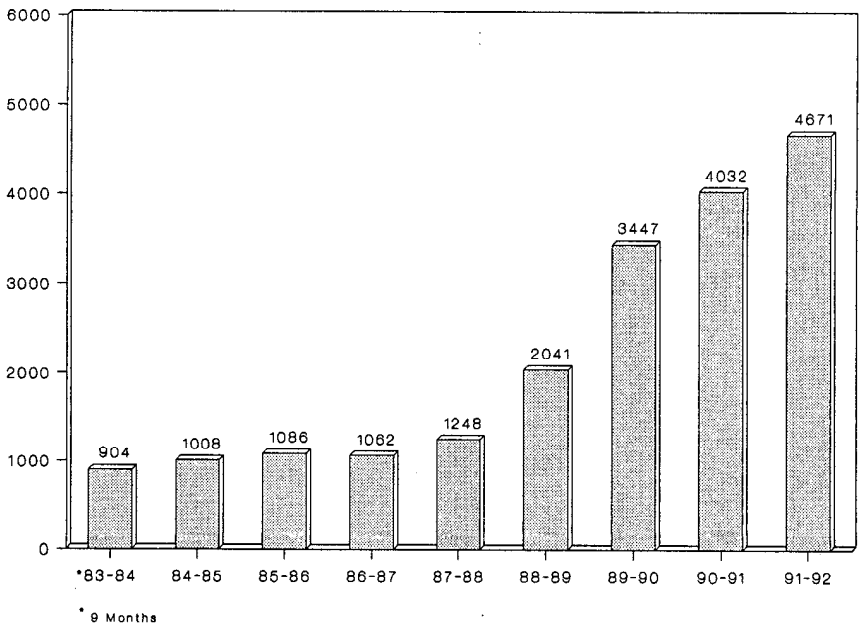
Finally, the office installed a device to communicate with callers with hearing or speech impediments (TDD).

The following two tables illustrate inquiries statistics. The first breaks out this year's inquiries by subject and the second compares numbers with previous years.

INQUIRIES 1991-92

What is the *Privacy Act* and How Can I Use It?	2420 (52%)
No Jurisdiction/Outside *Privacy Act* (Federal, Provincial, Municipal & Private Sectors)	808 (17%)
Use & Abuse of the Social Insurance Number (SIN)	588 (13%)
Misdirected Applications & Unrelated Matters	855 (18%)
TOTAL	4671

Inquiries 1983-92



Compliance Directorate

The directorate had two objectives for 1991-92. The first was to focus on a complex national organization—Canada Mortgage and Housing—with significant electronic data processing and communications components. Auditing CMHC permitted staff to examine distributed data processing and electronic communication issues and to further develop our EDP audit methodology.

The second objective was to review several smaller agencies dealing with women's and minority rights. Most of these organizations have large personal information collections, often because they investigate complaints. We selected Status of Women Canada, Canadian Advisory Council on the Status of Women, the Canadian Human Rights Commission and the Immigration and Refugee Board.

Audits were also completed on several other institutions such as National Defence, the National Capital Commission, Canadian Film Development Corporation, the Standards Council of Canada and various pilotage authorities. Work at 13 other organizations will carry over to 1992-93. Staff also

- investigated five incidents of lost or stolen files;
- audited three existing data-matches at Employment and Immigration Canada; and
- conducted a government-wide survey on the use of upward or reverse appraisals in federal institutions.

Trends and Problems

The past year's audits revealed some emerging trends in government information handling that demand attention. Foremost perhaps is the federal government's increasing use of private sector companies to provide services which handle personal information.

Contracting out—who's minding the data?

Budget pressures on government agencies have led many to use private industry for some of the services once performed in-house. For example, services such as Employee Assistance Programs, payroll applications and credit checking—and the personal information that goes with them—are now frequently handled by private companies under contract to the responsable government agencies.

The office has no quarrel with private companies performing services. However, unlike the federal government, the private sector is not covered by the *Privacy Act*. Thus, personal files handed over to private firms get no formal privacy protection unless specific clauses are written into the contracts. Since some departments use standard Supply and Services Canada contract forms and others draft their own, there is little consistency. Nevertheless, almost without exception, the contracts are deficient.

For example, contracts fail to:

- define ownership of the information;
- ensure employee access to the files;
- restrict further use of the personal data;
- protect against unauthorized disclosure;
- ensure proper disposal of files at contract end;
- establish retention and disposal criteria; and
- ensure the department's ability to audit compliance.

Our office is now working with Supply and Services Canada and Treasury Board to develop a standard contract. This should remedy many of the problems.

Checking employee credit ratings

Compliance auditors have found collection problems during examinations of personnel files. All permanent government employees—and many of those transferred or promoted—must undergo reliability checks. The department or agency obtains candidates' permission to check their credit ratings. Ratings are a combination of letters and numbers which describe the person's relative debt load and repayment behaviour.

The staff also found many of the same contracting problems described earlier. However, the credit checking process revealed other potential problems. For example, such large organizations as the RCMP, Canada Mortgage and Housing and National Defence often have direct on-line access to credit bureaus, allowing them to obtain substantially more personal financial data than a simple credit rating. There appears to be potential for abuse and nothing to prevent institutions from going on fishing expeditions.

In fact, most audited institutions tended to collect much more financial information than they needed. Details such as credit limits and account balances were found in files where only a simple credit rating was required. As well, the staff found credit reports containing not only the employee's information but also data on spouses. Credit bureaus often send out a work history and credit rating on the spouse, linking the information with the employee by Social Insurance Numbers and dates of birth.

Once in the hands of the government agency, credit information is often not kept secure. In some instances privacy staff found the information was transmitted by fax. In others, it was stored on the hard disk of desktop computers without adequate security protection.

Finally, much credit information is unreliable and therefore government institutions may be relying on incorrect data. Independent studies reveal a high error rate in credit files. Updates and corrections are made slowly and—sometimes—not at all. The onus rests entirely with individuals, even though stores and banks transmit the information to the credit bureaus.

Electronic transmission of personal information

Privacy audits have also found that government institutions routinely fax personal information. This courts the risks of having the transmission intercepted or sent to the wrong location. For example, an employee at the Canada Employment Centre in Sarnia, Ontario, sent four individuals' unemployment insurance queries to the local newspaper instead of the Employment and Immigration Canada office in London, Ontario. The employee had mistakenly punched the adjacent speed dial button which was programmed with the newspaper's number.

The incident was simple human error but it demonstrated the possible consequences of faxing personal information—a procedure auditors found in almost every institution visited. Fax is one type of technology where policies and procedures are not keeping pace. Little thought is given to what information should or should not be sent by fax. Employees transmit personal information from the most innocuous (lists of participants at meetings) to the most sensitive (medical records and credit checks).

Similar difficulties arise with the new electronic mail (E-mail) systems now being widely implemented. E-mail programs allow users of computer networks to communicate and transfer data within the network. Yet there are few policies or procedures to ensure that the data are shared only with those who need to know, or that it all remains secure.

Who's minding the computer?

One disturbing trend is that government seems not to be applying the same standards of management and control to its EDP resources as it does its paper records. Large complex government institutions appear not to know what hardware and software they own, let alone who has access and how the systems are being used. Increasingly, major collections of personal records are being automated but without formal controls. Electronic files lend themselves easily to improper collection, use and disclosure but, because the data are out of sight, they appear to be out of mind.

Portable computers: Automation of the federal government has seen the computer shrink from yesterday's roomful of equipment to today's notebook-sized units (with as much or more power) tucked into a briefcase. And already being tested is integrated chip technology which makes the plastic card "smart"—a mini-computer capable of storing and processing information.

However, these personal computing devices demand new management and control systems. Users often forget that these are not merely miniature typewriters. Computers remember what they process. Their loss or theft means not only lost valuable equipment but also lost information.

The office investigation this year of the theft of a personal computer from the Montreal office of Veterans Affairs illustrates the seriousness of such an incident. The computer was part of a new system on trial. It had been loaded with tombstone data on the office's entire 20,000 client base. Fortunately the personal details were very limited and the Commissioner decided not to notify the individuals concerned.

The investigation made it clear that Veterans Affairs staff had not followed the department's procedures for protecting valuable property. More important, however, investigators found no policies and procedures covering the storage and protection of the personal data in the computer memory. The Commissioner recommended that Veterans Affairs develop those policies and consider restricting storage of personal data to diskettes which could be removed and stored separately. Alternatively, personal data on personal computers could be encrypted to make it inaccessible to unauthorized users.

Controlling access in networks: The marriage of microcomputers and local or wide area networks poses another privacy challenge: determining which users should have access to what data. Auditors often find that authorized system users frequently can access information they do not need. The physical premises and the computer system may be secure from external threats but, once into the system, authorized users may access any data. Systems are needed to restrict users to the information they need to know.

Ending the pack rat syndrome: Auditors find few retention and disposal schedules for EDP files and those that do exist often do not correspond to the schedules for the paper files. Government may be shredding its paper but much of that paper was generated electronically. The data are replicated on hard and soft disks that seem to be kept indefinitely. Government agencies managing the retention and disposal of personal files need also to examine the electronic versions.

Describing information holdings

The description of government information holdings in *Info Source* continues to concern the Commissioner. Lack of resources may be a contributing factor but auditors find that *Info Source* is an incomplete and sometimes inaccurate catalogue of personal information held by government institutions. Some departments seem not to have a clear understanding of what they should list or how to change listings.

A common problem is the failure to list such federal employee standard banks as leave and attendance, travel and relocation, and training and development. The reverse is sometimes true—standard banks are listed but the institution holds no information. In fact, the bank is empty. And occasionally auditors and complaints investigators stumble upon information that seems not to be listed at all.

It may be time for Treasury Board to set out more clearly what institutions should describe and how to make changes. Also needed is a more rigorous review of the input government institutions provide to *Info Source.*

Upward appraisals

In earlier reports, the Privacy Commissioner expressed concern about the anonymity feature of upward or reverse appraisal processes being conducted in some departments. This process allows employees to rate and comment on their manager's performance, often anonymously.

In an effort to establish just how widespread the upward appraisal process has become and how it is being done, the Compliance Directorate polled 148 departments and agencies covered by the *Privacy Act*. At this writing it had received 141 responses (eight from one department), 27 of which were using or planning to use the process within the next 12 months. Of these 27, 24 promise employees anonymity and 18 use private consultants to analyze the results.

So fewer than 20 per cent of government agencies have embraced the idea. Nevertheless, one questions Canada's public service lending itself to a personnel relations process which relies upon the use of anonymous informants.

Corporate Management Branch

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

The following are the offices' expenditures for the period April 1, 1991, to March 31, 1992.*

	Information	Privacy	Corporate Management	Total
Salaries	1,670,069	1,911,442	658,825	4,240,336
Employee Benefit Plan Contributions	285,600	307,020	121,380	714,000
Transportation and Communication	75,621	59,500	124,875	259,996
Information	21,005	55,261	3,109	79,375
Professional and Special Services	209,028	190,237	81,059	480,324
Rentals	4,391	3,276	11,945	19,612
Purchased Repair and Maintenance	6,688	6,358	7,199	20,245
Utilities, Materials and Supplies	18,692	9,814	29,070	57,576
Acquisition of Machinery and Equipment	109,474	44,361	12,959	166,794
Other Payments	2,970	1,873	250	5,093
TOTAL	2,403,538	2,589,142	1,050,671	6,043,351

* Expenditure figures do not incorporate final year-end adjustments reflected in the offices' 1991-92 Public Accounts.

Finance

The offices' total resources for the 1991-92 fiscal year were $6,691,000 and 82 person-years, an increase of $367,000 and four person-years over 1990-91. Personnel costs of $4,954,336 and professional and special services expenditures of $480,324 accounted for more than 90 per cent of expenditures. The remaining $608,691 covered all other expenses.

Personnel

In the spirit of PS 2000, the unit made several improvements to the offices' personnel management practices by recruiting a management trainee, developing incentive awards and an orientation program for new employees, and streamlining some of its personnel procedures. In addition, the unit conducted a triennial classification audit, followed up the 1987 official languages audit and signed a letter of understanding on official languages with the Treasury Board.

Administration

The unit made continued progress on a retention and disposal schedule for records and also on an automated inventory of assets. As well, it evaluated the offices' telephone system to improve service to the public.

Informatics

This year the unit completed three studies for a new case management system, office automation and using a computer network in a secure environment.

Library

The library provides interlibrary loan services, manual and automated reference and research, and subject-oriented media monitoring files. In addition to acquiring 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 (which is open to the public) handled 1,298 publication requests and answered 1,084 reference questions during the year.

Organization Chart