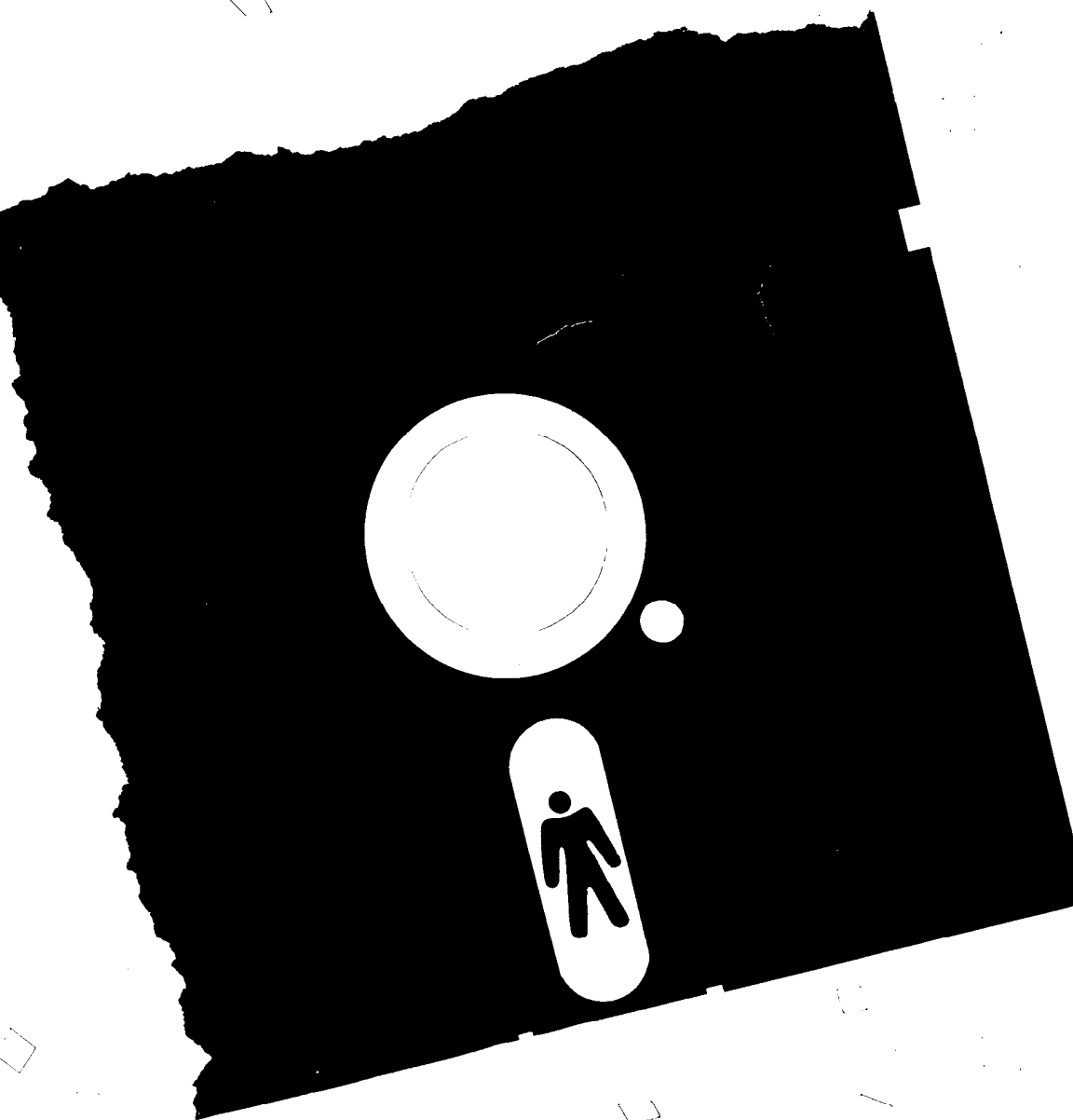




Privacy Commissioner

Annual Report 1989-90



**Annual Report
Privacy Commissioner
1989-90**



The Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3
(613) 995-2410, 1-800-267-0441
Fax (613) 995-1501

© Minister of Supply and Services Canada 1990

Cat. No. IP30-1/1990

ISBN 0-662-57525-3

The Honourable Guy Charbonneau
The Speaker
The Senate
Ottawa

May 22, 1990

Dear Mr. Charbonneau:

I have the honour to submit to Parliament my annual report. This report covers the period from April 1, 1989 to March 31, 1990.

Yours sincerely,



John W. Grace
Privacy Commissioner

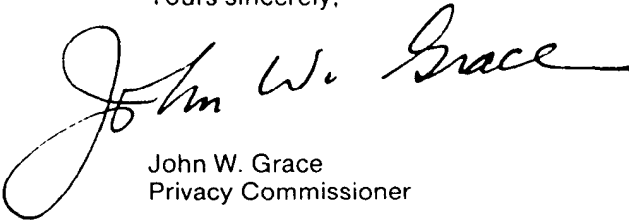
The Honourable John Fraser, P.C., Q.C., M.P.
The Speaker
The House of Commons
Ottawa

May 22, 1990

Dear Mr. Fraser,

I have the honour to submit to Parliament my annual report. This report covers the period from April 1, 1989 to March 31, 1990.

Yours sincerely,



John W. Grace
Privacy Commissioner

Table of Contents

| | |
|---|----|
| Mandate | 1 |
| The Sermon: An end of term report | 2 |
| During the Year | 16 |
| Public servants' hot line | 16 |
| Reviewing the CSIS act | 17 |
| SINning...again | 19 |
| Thanks to Mr. Statsman | 20 |
| Spreading the word | 21 |
| Drug testing—everybody's doing it | 22 |
| Genetic analysis | 23 |
| Police databases—CPIC | 24 |
| Ring, ring... Orwell calling | 26 |
| A new exempt bank | 27 |
| Complaints Directorate | 29 |
| Data-matching review | 31 |
| Notifying the Commissioner | 33 |
| Some cases | 36 |
| Inquiries | 50 |
| Compliance Directorate | 52 |
| A seven-year retrospective | 52 |
| What was found | 54 |
| Some incident investigations | 56 |
| Corporate Management | 57 |
| Appendices | 59 |
| I Organization chart | 59 |
| II Government institutions covered by the Act | 60 |

Mandate

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

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

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

Individuals in Canada may complain to the Privacy Commissioner if:

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

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

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

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

The Sermon

*"The future is not what it used to be."
—William McNeill, Professor of History
Emeritus, University of Chicago.*

An end-of-term report

An end-of-term report offers a once-in-seven-year opportunity to range beyond the arbitrary confines of 12 months in appraising the privacy state of the nation. Of course, there is some grandiosity (or threat?) to that promise. The *Privacy Act* requires, after all, only an annual accounting to Parliament and the legislation covers only the federal government, not the country.

Yet comments based upon seven years of observing privacy protection (or lack of it) should be better grounded than those based on the experience of the last 12 months. If the observations and judgments in this report sometimes reach beyond the narrow legal confines of the *Privacy Act*, that itself is because a privacy commissioner's office by 1990 has inevitably been drawn into the day's larger and newly-emerging privacy issues.

That does not mean that a privacy commissioner should try to impose his writ upon areas where he has no jurisdiction. But to stay out of the fray and ignore the privacy aspects of, say, AIDS or drug testing—two momentous issues of our time—would be to risk irrelevance and to preside over the diminishment of the office. Perhaps the most encouraging development in seven years has been the way in which the office of the Privacy Commissioner, like it or not and justified or not, has been used as a national privacy resource centre.

Inquiries from the public have increased from 1008 in 1984-85 to 3447 in 1989-90. The subject of the calls and letters range from queries on when a Social Insurance Number must be given (still the most frequent question) to media requests for comment on matters with potential privacy implications; from telephone gadgetry showing a caller's telephone number on a screen to an Auditor General's proposal for an anonymous fraud hot line to a proposal by a municipal council to circulate detailed profiles of released offenders.

Privacy moved from a peripheral social issue, from being a rather esoteric, rarefied—almost cult—concern into the main stream of public consciousness. That is the positive change of the past seven years, and the awareness continues to grow.

The awareness grows with each new intrusion upon private lives by the information society—and the information economy. Turning to privacy values is an instinctive human response to, and defence against, a prying, pervasive technology. The cry for privacy protection is a plea that human values—human dignity—should prevail against a computer-driven culture which would claim sovereignty over every recorded transaction. It is sometimes argued the massive information storage and retrieval capacities of the computer make possible a new Renaissance of learning, an age when machines can do what men could not do without unimaginable drudgery—and perhaps not even then. Comfort has been taken in the notion, as one commentator has put it, that "information is a renewable resource".

Unlike trees or oil, information can indeed be renewed: better computers linked to better communications systems can renew—and expand—information almost to infinity. But human privacy is not renewable. There's the rub. Once lost to an indiscreet computer, a person's privacy is gone forever. The computer never forgets.

In a laissez-faire information society, there is no control even over the uses of one's own name. As the American attorney and communications scholar Anne Branscomb has written, the only way to stop the trafficking in a person's personal information is to "become a hermit, have an unlisted telephone, never charge anything and stop buying any items from catalogues". Even such unnatural precautions may offer no real guarantee.

The consciences of the collectors of personal information are all that control the uses of private-sector databases. Voluntary codes of fair information practices are visible evidence of ethical intent. Here there is some reason for encouragement, as is discussed later. But should one choose not to share one's own information with the marketplace, there is negligible legal protection in the now open season on personal information.

The dark side

Too many Canadians continue to remain unaware of the *Privacy Act* and the important rights it confers. The fact that 300,000 individuals have used the Act to apply for their information in federal government files shows, however, that the legislation is becoming better known and, when known, it is used. More and more Canadians are increasingly, if vaguely, aware of the dark side of new technologies which can transform persons into "data subjects" and develop profiles of greater or lesser accuracy based upon personal information winkled out of proliferating data bases.

These gloomy observations are not simply the subjective judgment of a professional privacy advocate. Public opinion poll after another show that protection of privacy ranks high among the most pressing issues facing modern society.

What chance does privacy have when satellites can conduct surveillance from more than 300 kilometres in the sky? Audio eavesdropping no longer demands physical access to a building in order to plant listening devices. And, of course, most of us carry in our wallets or purses the key to vast amounts of highly sensitive personal information. Our ubiquitous bank and credit cards leave a trail of where we travel, eat, shop and sleep—perhaps by matching records—even with whom! George Orwell could not have imagined the new possibilities of Big Brother.

Professor David Flaherty of the University of Western Ontario is an internationally recognized authority on data protection. He served as consultant to the Justice and Solicitor General Committee's review of the *Privacy Act* and he has been quoted before in these reports. His recent book, called *Protecting Privacy in Surveillance Societies* (University of North Carolina Press), argues with chilling persuasiveness that individuals "are increasingly subject to surveillance through the uses of data bases in the public and private sectors and that these developments have negative implications for the quality of life in our societies and for the protection of human rights."

What can be left of the right to be left alone (and courts are defining precisely such a right), he asks, when credit bureaus monitor the credit information of millions of Canadians and the names of perhaps 10 per cent of this country's adult population may be contained in the national police computer known as the Canadian Police Information Centre?

Add to these, burgeoning federal and provincial government data bases holding personal data of greater or lesser sensitivity on everyone who has ever breathed the air of the country. Seven years ago, the federal government held, on average, 10 to 12 files on each person in Canada. Today, the number is closer to 20. The sheer magnitude of such data bases goes a long way to demonstrate Professor Flaherty's thesis that western industrial societies run the increasing risk of becoming, if they are not already, surveillance societies.

"There has to be some consideration for individual rights. We can't be running around testing anybody at any time."

—Pat Bowlen, owner of the Denver Broncos.

Privacy and the Charter

There is, however, some room for encouragement, though certainly not smugness, in the knowledge that Canadians are better defended against uncontrolled surveillance than other societies. In addition to the protection and rights provided by the *Privacy Act*, the *Charter of Rights and Freedoms* is proving to be an unexpected and surprisingly effective defender of privacy values.

Privacy is not mentioned as a specific right guaranteed by the Charter. Yet the Supreme Court of Canada has interpreted sections of the Charter unambiguously and vigorously as statements of privacy protection. Attention has been called in earlier of these reports to previous Supreme Court decisions which established that the "right to be secure against unreasonable search and seizure" (section 8 of the Charter) protected individuals from unjustified intrusions upon their privacy. On January 25 this year, in *Mario Duarte v. Her Majesty The Queen*, that reading of the Charter was spectacularly re-affirmed in the decision concurred in by six of seven Justices.

The case turned on whether it was legal, under the Charter, for the police to have an informer record, surreptitiously and without a judicial warrant, his conversation with a suspected drug dealer. The Supreme Court of Ontario had held that the police (though not private citizens) were free, without judicial warrant, to “bug” private conversations as long as they had the co-operation of one of the parties.

In writing for the majority, Mr. Justice La Forest built upon the Supreme Court’s earlier decisions (his own among them) that “the primary value served by section 8 of the Charter is privacy”. The following paragraph should end any doubt of how effectively the Court and the Charter can respond to technology threats to personal privacy:

“The very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to annihilate any expectation that our communications will remain private. A society which exposed us, at the whim of the state, to the risk of having a permanent electronic recording made every time we opened our mouths might be superbly equipped to fight crime, but it would be one in which privacy no longer had any meaning”.

The importance of this judgment can hardly be over-estimated and it is deserving of more attention than it has received.

The good news is that the case lays down rules restricting the use of electronic surveillance by police authorities. The Supreme Court decision makes the country at least a more private place than it might have been.

The *Criminal Code*, however, does not prevent private citizens from intercepting the conversations of others as long as one of the parties to the conversation consents. Through this loophole the surreptitious use of microphones hidden in briefcases and umbrellas, parabolic dishes and the widely-advertised “whisper 2000” directional microphones continue to proliferate.

The criminal law should make the surreptitious interception of all private communications unlawful by requiring the consent of all parties to the communication to any recording or interception.

“When a reporter enters the room, your privacy ends, and his freedom begins.”
— Warren Beatty.

Privacy and the media

Another recent Supreme Court judgment compels equal attention.

In this case, *Edmonton Journal v. Alberta*, a majority of the Court held that intrusions upon the personal privacy of individuals were justified by the higher public good in the freedom of the press to report court cases.

But the dissent of Mr. Justice La Forest, writing for Madame Justice L'Heureux-Dubé and Mr. Justice Sopinka was, for a privacy advocate, more significant than the view of the majority. Earlier Court decisions placed limitations upon *governmental* intrusions; the dissent would protect individual privacy from assault from non-governmental sources. In this case, Mr. Justice La Forest was willing to extend the Court's protection because, he wrote, "in our society the privacy of the individual is as often threatened by other powerful or influential entities against which the individual is powerless".

Other entities, indeed. Three Supreme Court Justices concurred in the following: "The protection from intrusion on the privacy of the individual, the family and witnesses . . . in itself affords a sufficiently compelling objective to warrant some curtailment of the freedom of the press in the present context." (The context was a matrimonial dispute.)

No state secrets here to protect. No threat to the privacy of ordinary citizens from government. In an almost trivial matter, so far as the state is concerned, the minority was ready to extend existing prohibitions upon publishing personal information. They would go considerably beyond restrictions pertaining to victims of assault or to young offenders. The dissenting judges were willing to place new limits upon press freedom because the disclosure "of personal information about an individual by the mass media can do incalculable harm to the individual and his/her family".

The view of the majority, which held that there should be no restrictions placed upon the reporting of matrimonial cases, has received all the media

attention. The dissent has been all but ignored. In the long term, however, it may be shown that the balance, that anguishingly difficult balance, between privacy and press rights which has been struck in the *Edmonton Journal* case is not good enough. It will need fine tuning and Mr. Justice La Forest, Mr. Justice Sopinka and Madame Justice L'Heureux-Dubé may yet be proved right.

The threats posed in this case to a free press were, after all, theoretical. The invalidated law respected the principle of open courts. Access by those having serious interest in court proceedings or family law is permitted. All the general information about the nature of the case may be published. Moreover, the *Edmonton Journal* presented no evidence that, throughout its 50 years, there was a single instance where the rejected provision forbade it from reporting on a matter of public interest.

Little wonder that the dissenting judges expressed scepticism of the significance of the negative impact of the legislation on freedom of the press and media, and the public's right to be informed of matters of public interest.

But, on the other side, the harm is real and present.

In Justice La Forest's words:

"In matrimonial cases, the individual is forced to reveal many aspects of his or her private life in order to comply with the demands of the state in ordering his or her life. This necessary intrusion on family privacy, we saw, may have serious impact not only on the litigants themselves but on witnesses and, even more important, children."

The far greater threat to freedom of the press today comes from some of the media's own excesses in intruding, shamelessly and aggressively, into private lives in matters where there is no public interest, only public curiosity or, even, prurience. In the United Kingdom, a reaction to such excess brought about the introduction of legislation which would have restricted, in the name of privacy protection, the publication of personal information. That legislation has been withdrawn, wisely; it was dangerously drafted. But the fact that it was a near thing in Britain—and the closeness of the Supreme Court's decision in Canada—should cause the media to examine their collective conscience (is there such a thing?), if only from the point of view of enlightened self-interest.

Justice La Forest's observation that "privacy ranks high in the hierarchy of values meriting protection in a free and democratic society" is a message more than an aphorism. The message is that privacy is a value which the courts—and the public—may be increasingly willing to place higher than even that of a free press.

Real progress

If there is truth to the proposition that Canada is doing better than most societies in holding back the intrusions of the new, aggressive technologies which would treat human beings as mere data subjects, the credit must not only go to a vigilant Supreme Court, but to Parliament and, yes, the government.

The most significant privacy happenings in the past seven years were, perhaps in this order, the review of the *Privacy Act* by the Justice and Solicitor General Committee, the government's generally positive response to that committee's recommendations in *The Steps Ahead* and two government policy initiatives: the first, reining in the Social Insurance Number (the now infamous SIN), the second, imposing controls over computer matching or linkage.

These achievements have been commended in earlier reports and must be singled out again in this retrospective. Without the enthusiastic and unanimous re-affirmation of the *Privacy Act* by the Parliamentary committee and the government's acceptance of the committee's principal recommendations, atrophy might have set in.

It was enormously important that the Parliamentary review found that the *Privacy Act* had struck the proper balance between the public interest and private rights. There had been some scepticism from both sides—from chiefs of police and civil libertarians—over that balance. Parliament must have had it right because, on review, not a whimper of complaint was heard from either side of the ideological barrier.

"... aspiring bureaucrats are constantly inventing new ways to use existing data for other administrative purposes."

David Flaherty, Protecting Privacy in Surveillance Societies.

As a result of support from the top, privacy as an issue in Canada has developed considerably beyond awareness, however necessary that is for the beginning of reform. Seven years ago, privacy rights and the need for privacy protection remained largely abstractions. Today the talk is of specifics: bringing the use of the Social Insurance Number under better control (Why do banks demand a SIN? Must I give my SIN in opening a new account?); controlling the use of compulsory tests in the search for the "perfect" employee; limiting the traffic in personal information that reveals individual's spending choices—from goods purchased to charity donations; and questioning the intrusiveness of market surveys, political polling, and census-taking (Do they ask too much and what do they do with the information?).

Even those who are not computer literate are aware of the ability of small and cheap computers to mix, match and massage data bases. Techno-peasants, data protectors included, are aware of the downside of efficiency. The claimed benefits from linkages (tracking down cheaters or debtors, for example) may come at the unacceptable cost of systematic population monitoring. In Canada, computer matching by federal government institutions is now covered by strict rules under which the Privacy Commissioner's office plays a role. The Americans have even encased their matching controls in federal legislation.

"We are travelling in the fast lane without side-view or rear-view mirrors."
—Henry Wiseman, Chairman, World Conference on Ethics and Technology, University of Guelph.

The "what" act?

Little has been static in the privacy business these past seven years, neither the threats nor the responses. The impact of the *Privacy Act* upon the public, the government and the public service is now irreversible. As noted earlier, by the end of seven years almost 300,000 individuals (the count is Treasury Board's, not the Privacy Commissioner's) will have used the *Privacy Act* to apply formally for their personal information held by the government. That is a surprising figure. What would the numbers be if the *Privacy Act* were more widely-known?

After all the speeches and reports by the Privacy Commissioner, not enough Canadians are aware of their privacy rights. Even public servants remain unaware both of their own rights and responsibilities under the legislation. The latter is not a subjective judgment: it is the most common single finding of the office's privacy auditing.

Yet ask any senior public service manager (or any public servant aspiring to be a senior manager) and he or she will be as aware of the *Privacy Act*, well, almost, as the *Official Languages Act*. Privacy is now part of the public service's psyche.

Note these three important initiatives in the past year alone:

Item: National Defence now gives members of the Canadian Forces access to their current evaluations and to their position on a merit list without a formal request under the *Privacy Act*.

Item: Supply and Services put in place a strict policy ensuring that government mailings comply with the *Privacy Act*. On its part, Treasury Board has published guidelines to all departments covering uses of their mailing lists.

Item: Employment and Immigration, Industry Science and Technology, the Canadian Security Intelligence Service, among others, conduct their own internal audits to determine compliance with the *Privacy Act*.

On the most senior levels, there is now an ethos of acceptance of and respect for privacy principles. The most striking reason for this perhaps surprising generalization is that in seven years the Privacy Commissioner has not been forced to his ultimate resort—to bring a case against a government institution before the Federal Court. There have been a few, but only a few, settlements at the court house door. The crucial point is that in the crunch no recommendation of the Privacy Commissioner has been defied.

Of course, the reason Parliament put a privacy ombudsman in place was precisely to negotiate disputes and avoid recourse to the courts. The courts would be the first to say that they are overburdened enough without being asked to settle privacy quarrels.

It is not unseemly to boast of that non-court record because it takes two to tango. In this end-of-term reckoning, nothing is more important for the Privacy Commissioner to do than to commend ministers, deputy ministers, privacy coordinators and managers alike for their sensitivity to the letter and spirit of the legislation.

The willingness to make the *Privacy Act* work has been demonstrated across the board: from the Royal Canadian Mounted Police and the Canadian Security and Intelligence Service, the holders of some of the most sensitive personal information, to Employment and Immigration Canada and Revenue Canada, the custodians of the largest holdings of information, to the smallest, the Yukon Territories Water Board with (at last count), its three files.

The coordinators... still

As important as court cases which didn't happen (and another reason for that) is the increasingly close rapport achieved over the years between departmental privacy coordinators and investigators from the Privacy Commissioner's office. The busiest privacy coordinators are now as expert in at least some aspects of the *Privacy Act* as privacy investigators. They share a growing body of knowledge and precedents; their expertise enhances their value to their own institutions, especially as cases become more complex.

Coordinators have in fact emerged, albeit mainly in larger institutions, as privacy professionals. Theirs is not an easy role, caught between natural loyalties to a department and to the *Privacy Act*. Sometimes the role calls for heroism.

Enlightened departments now give their coordinators the status the job deserves. Last year, the coordinator for Veterans Affairs conducted briefings at regional departmental offices across the country. Her teaching role (with a travel budget of \$17,000), was tangible testimony to her department's commitment to the *Privacy Act*.

“and miles to go...”

So much for the credit side of the ledger.

A balance sheet must also report debits, some of which run deeper than even that most spectacular of privacy breaches—that privacy Chernobyl—the theft of the tax information of some 16 million Canadians from a Toronto office of Revenue Canada. That incident more widely brought home the vulnerability of data holdings and showed the need for data protection than all the preachments of a privacy commissioner.

Yet, even after all the good things are said, too many rank-and-file federal public servants, as noted earlier, remain in blissful ignorance of privacy rights and privacy responsibilities. After seven years, there shouldn't be a federal government employee unaware of the *Privacy Act*. Yet each privacy audit by compliance investigators turns up the same dreary chronicle of pervading ignorance, not among senior managers, but at levels where it is by now inexcusable. This past year has seen Treasury Board privacy courses given to some 700 public servants. That is an important beginning—but only a beginning.

“To avert disaster we have not only to teach men to make things, but also to produce people who have complete control over the things they make.”
—Prince Charles.

Unfortunately, an important component of any training—audio-visual material—is still missing. Both Treasury Board and the Commissioner's office make do with tapes of items aired on commercial TV. After seven years it is frustrating, and not a little embarrassing, to have to refer federal institutions to the Ontario and Quebec provincial commissioners for training audio-visuals. In fact, the office's 1990 request for a modest \$70,000 for public affairs was turned down because, with its heavy complaint load, the office “is well enough known”.

There is better excuse for other Canadians to be unacquainted with the *Privacy Act*. The Treasury Board and the Privacy Commissioner's office have had only modest resources to engage in a public information campaign. Posters and brochures in government offices are merely well-intentioned tokens. Full-fledged advertising campaigns are prohibitively expensive and, some might say inappropriate—at least for an ombudsman's office.

Yet rights which remain too much unknown and thus unused, are hardly worth having and could wither. One answer is found in the initiative of some departmental employees who have made it part of their jobs to inform citizens about the *Privacy Act*. One employee of a local EIC employment centre sent an article which she had written about the Act to the local paper where it was published. An admirable initiative.

Privacy disappointments have been discussed in earlier reports: slippage in the government's good intention to bring Crown corporations under the *Privacy Act* (Air Canada and Petro Canada appear to have escaped completely); delay in bringing forward amendments to the *Privacy Act*; slowness of the private sector to put in place voluntary privacy codes, despite Canada's commitment to the Organization for Economic Co-operation and Development's (OECD) privacy guidelines.

These are mainly grumblings about bureaucratic inertia and missed opportunities. The world does not share a privacy commissioner's sense of urgency. Nothing surprising nor anything inherently damaging about that. What is more likely to send a privacy protector into a blue funk on a bad day is the sheer magnitude of the threat from the new technologies.

Can any data protection regime do more than tinker at the fringes in a world of micro-computers, with their ever larger storage and transmission capabilities, local area networks, machine readable (smart) cards, laser discs, glass fibres, computer-matching, point of sale payments, enhanced databases, machine scanning—to keep the list short? “Is there some point”, as Professor James Rule of the State University of New York has asked “beyond which collection of personal data simply becomes excessive, whatever principles may govern the data systems?”

Consider the daunting challenge for data protectors in monitoring a centralized regime of fair information practices in an increasingly decentralized, if not fragmented, environment. A recent OECD paper summarized the functional effects of technological change as “the trivialization of data processing”. One could also speak of the “democratization” of access to data-processing through the proliferation, not only of micro computers, but by expert and microform systems, optical discs, two-way cable television.

Four years ago it was reported somewhat breathlessly in one of these reports, that the number of micro-computers in the federal government was about 6,700 units, some 1,700 having been acquired in the previous year alone. Today they are as common as once were manual typewriters. No one seems even to count any more though, for the record, as far as anyone knows, the total appears to be some 30,000.

It is not only that micros have access to larger computers; microcomputers are larger computers. Moreover, they possess such extraordinary flexibility that the old concept of what constitutes a file is becoming utterly outmoded. As another OECD report points out, “it is no longer necessary to work with clearly pre-defined file structures; existing file structures can be adapted to new ones”.

A file is now more slippery than that "damned, elusive Pimpernel". A file can be opened, blended, collapsed, and reincarnated at a push of a button. A study by the Council of Europe has concluded that some of the old assumptions in data protection no longer apply. The solution envisaged in the 1970s "were valid insofar as they were brought to bear on the then state of the art, characterized by main frame/stand alone computers with dedicated applications capable of storing and processing data on 'identified or identifiable individuals' on a 'file' under the authority of a 'file controller' identifiable at will by a 'supervisory authority'". Now how does a privacy commissioner, as the "supervisory authority", have any assurance that he is seeing a complete file on an "identifiable individual" when a file no longer possesses any definition?

Are dispersed computer files even records? The *Privacy Act*, with serendipitous prescience, was written broadly and speaks of personal information "about an identifiable individual that is recorded in any form". There is no mention of either records or files. The Act is also silent on how much computer programming, if any, must be carried out in a search for personal information.

To their great credit, there is no evidence that Canadian government institutions have circumvented the *Privacy Act* by refusing to give access to personal information if it is not neatly packaged and identified in a single file, either paper or electronic. Yet electronically stored and dispersed information can be instantaneously sorted, retrieved or even destroyed with a few computer keyboard strokes; the temptation to use new technology to thwart the Act grows stronger with each splendid new computer.

How can a privacy commissioner be sure that it is always resisted?

When the processing of data no longer needs to take place within a system of centralized data banks, the effectiveness of existing audit tests for compliance with the *Privacy Act's* rules must also be questioned. New decentralized, interactive and multi-functional computer terminals challenge the capacity of existing auditing methodology.

How can personal information be kept, as it should be, secure and segregated to its original purpose when it is now possible for every computer terminal to be connected, as an OECD paper has noted, through public or private transmission lines, to everybody else's terminal?

The general principles of data protection have stood up remarkably well, precisely because they are general. Every study comes to that conclusion. But the monitoring of technology must be clever enough to match the marvellous abilities of the new generations of computers. Otherwise, data protectors will find themselves merely wringing their hands and filling the air with lamentations. A compelling need in any privacy commissioner's office is to keep up with the technology in order to possess reasonable assurance that their technical experts can challenge the best in the computer business.

"Telecopiers without a technical system guaranteeing data protection must not be allowed to be sold, like a car without brakes."

—Professor Spiros Simitis, Hesse Data Protection Commissioner.

In an ideal world, the developers of new informatics technology are sensitive to the surveillance implications of their products and seek the advice of data protectors at an early planning stage. Alas, it is not an ideal world.

Privacy and the private sector

Pessimistic ruminations on a bleak day should not give way to despair. Those general privacy principles which have stood up so well can be adapted to new technology, to evolving situations. The OECD recently noted that regulatory approaches to privacy protection are moving more generally to "rules governing specific sectors of activity". A sector-oriented approach means tailoring rules to serve the specific needs of, say, banking, telecommunications, direct mailers, the airlines or government.

Rules for one sector can prove to be, unworkable—or ineffective—for another. Flexible codes for meeting challenges to privacy protection are now required for the successful selling of voluntary privacy codes to indifferent, hostile or merely dubious chief executive officers. In Canada, it is still possible to cling to qualified optimism that the Canadian private sector will yet come forward with public commitments to fair information practices. Slow progress continues to be made on a sector-by-sector basis.

In last year's annual report, the Privacy Commissioner stated:

"Without more evidence of effective self-regulation (in the private sector), however, the supporters of voluntary data protection codes will be increasingly hard put to defend their position".

During 1989-90, the Privacy Commissioner has had extensive consultations with associations representing the air transport, telecommunications and banking industries. While there has not yet been widespread adoption by these institutions of privacy codes of practice conforming to the OECD guidelines, meaningful expressions of intent have been made to move in this direction.

The Canadian Bankers Association's model privacy code, which had fallen into limbo for some years, is back under active consideration for adoption by most of the chartered banks. The Canadian Air Transport Association is working with the International Air Transport Association to adopt a data protection code of practice for customer records and will review the privacy practices in place for employee records. Member companies of Telecom Canada appear willing to organize their already heavily regulated customer records requirements into a privacy code. They are also reviewing their employee records management practices against the OECD privacy guidelines to verify or ensure compliance.

This missionary work showed signs of results at a meeting in Vancouver earlier this year between members of an organization bringing together most of the federally-regulated industries, (FEDCO) and the Privacy Commissioner. There was unanimous support in principle for voluntary codes.

"The global village is very restless."
—Geraldine Kenney-Wallace, President,
Science Council of Canada

Time for a nudge

But privacy commissioners have had assurances of action from the private sector in the past; assurances which never became realities. And so, while the actions of these three federally-regulated sectors are positive enough to keep alive the voluntary approach to privacy protection, the law should now give the process a firm nudge.

To that end, the government should consider bringing forth an amendment to the *Privacy Act* requiring federally-regulated firms to develop, implement and submit to the Privacy Commissioner for review, voluntary codes of privacy protection in conformity with the OECD guidelines. It is not necessary for the Privacy Commissioner to have the power to order changes to any such code or to have any role in its enforcement. He should, however, continue to monitor the effectiveness of these voluntary codes and, only if experiences prove unsatisfactory, develop recommendations to Parliament for stronger privacy regulation.

There are also clear trends elsewhere towards self-regulation. Even European countries, which began by compelling the private sector to register personal information holdings with privacy commissioners, are reducing licensing requirements and encouraging self-regulation.

Closer to home, that bastion of free enterprise and holder of vast amounts of personal information, American Express, has now announced to the world that "the issue of privacy will be so important in the years to come that we intend to be an advocate of consumer privacy". An American Express senior executive, speaking on behalf of his company, has said that he was "increasingly concerned by the companies that collect information for one purpose and sell it to another without the individual's consent".

American Express has seen the handwriting on the wall.

The company's own survey of consumer attitude revealed:

- 90 per cent of all Americans do not think companies disclose enough about their list usage practices;
- 80 per cent do not think companies should give out personal information to other companies;
- more than one-third of all Americans think the federal government should regulate the use of lists in their country.

Does anyone believe that Canadian figures would be substantially different? Of course not.

American Express has adopted a voluntary privacy code not out of a sudden intellectual commitment to privacy as an abstract virtue. It became convinced that in 1990 privacy protection has become good business. Good business, first, because, in American Express' words, "companies who respect their customer's patience and privacy will grow stronger in the years ahead; second, because the customer database can become... a tool of destruction that erodes consumer confidence and ultimately takes our future out of our hands and turns it over to the government". This is precisely the message the Privacy Commissioner has been preaching. It should carry more weight in coming now as an unsolicited testimonial from a company with impeccable credentials as a player in the private sector.

Dad: Have you been a good boy so Santa can send you what you asked for?

Son: Oh, I know Santa will send me what I want.

Dad: How do you know that?

Son: Because I'm in Santa's computer.

— Overheard by the New York Times.

During the Year

Public servants' hot line

The year brought the unusual, though surely not unedifying, spectacle of two officers of Parliament giving conflicting advice to their masters.

The issue arose when the Auditor General proposed a "hot line" which would receive anonymous allegations of fraud, waste or mismanagement. He believed that a guarantee of anonymity would encourage individuals to speak, protected as they would be against reprisals, and produce considerable savings to the taxpayer. This cause, of course, is entirely worthy.

The Privacy Commissioner intervened because of his *Privacy Act* responsibility to defend rights. One of those rights is to know what accusations against an individual — and who made them—are recorded in government files. Be they true and well-intentioned, as some may be, or false and malicious, as others may be, it is fundamental to our notion of justice that accusations not be secret nor faceless.

The dispute between the Auditor General and the Privacy Commissioner was a clash of two important values. For this reason, the Privacy Commissioner is grateful to the Public Accounts Committee for its invitation to both the Auditor General and himself to make their cases.

The case of the Privacy Commissioner was that the Auditor General could not, without changes to the *Privacy Act*, offer "whistle-blowers", no matter how public spirited, the guarantee that their identities could be protected. If the Auditor General's office was designated as an investigative body, as set forth under the *Privacy Act*, the names of his informers could be protected. But his office is not in the police business.

The Auditor General suggested in his 1988 report to Parliament that the *Privacy Act* should be amended to make possible precisely what he wanted to accomplish by his hot line.

While a guarantee of anonymity for whistle-blowers may produce savings to the public purse, one wonders what it would do to our public officials—union members and management alike. A Kafkaesque system of justice would be theirs—unknown accusers, unknown allegations, never knowing when or why the inquisition will befall them.

If stronger laws are required to protect whistle-blowers from retaliation, they should be enacted. But a lesson from history (and not so very distant history) is that governments which encourage their citizens to be faceless informers not only exact, but pay, a great price.

It is for Parliament, not the Privacy Commissioner nor the Auditor General, to decide when privacy rights should give way to other values. The Public Accounts Committee has not recommended that privacy rights be pushed aside in this matter. Nor has the Auditor General argued since for his project.

Reviewing the CSIS Act

In November, the Privacy Commissioner made a submission to the Special Committee on the Review of the *Canadian Security Intelligence Service Act*. What follows is largely an extract from that submission.

The major institutions comprising Canada's security-intelligence apparatus, including the Canadian Security Intelligence Service (CSIS), must comply with the *Privacy Act*. Yet Parliament took great care to ensure that the personal information access rights afforded to individuals by the *Privacy Act* would not undermine the ability of government institutions to safeguard national security.

Six years of the Privacy Commissioner's findings and Federal Court decisions, demonstrate the ability of the *CSIS Act* and the *Privacy Act* to co-exist, if somewhat warily.

By the nature of its work, CSIS makes difficult judgments about when it is appropriate to target individuals for surveillance. From the privacy perspective, the *CSIS Act* has provided the agency with important guidance which was unavailable to the former RCMP Security Service. Many of CSIS's problems with the *Privacy Act* have been inherited. Most concern information collected by the former security service—whether it was properly collected and whether it can be disclosed without injury to the CSIS mandate.

The solution to this problem is not, in the Privacy Commissioner's view, an amendment to the *CSIS Act*. Rather, it is timely destruction of that information inherited from the RCMP Security Service, the collection of which would now be improper under the *CSIS Act*. That review and destruction process is underway. The Privacy Commissioner is satisfied with the priority CSIS has attached to this task.

In its document, *Amending the CSIS Act*, the Security Intelligence Review Committee (SIRC) recommends:

“...that Parliament consider the advisability...of adding a paragraph to subsection 39(2) of the *CSIS Act* specifying that the Committee is entitled to have access to any information under the control of the Service, notwithstanding the existence of any investigations that may be undertaken by the Information Commissioner or Privacy Commissioner.”

While one may understand SIRC's unease in being denied access to anything it requests of CSIS, section 33 of the *Privacy Act* requires that the Privacy Commissioner's investigations be conducted in private. Moreover, subsection 33(2) provides that “no one is entitled as of right to be present during, to have access to or to comment on representations made to the Commissioner by any other person”.

If SIRC's proposed amendment were to be adopted, it would provide it with a right of access to CSIS's representations to the Commissioner and the Commissioner's correspondence to CSIS. This would infringe clearly upon the provisions of section 33.

The limits placed on SIRC's access to CSIS records set out in section 33 of the *Privacy Act* do not, in the Commissioner's view, impede SIRC in the exercise of its mandate. But from the Privacy Commissioner's point of view, those limits are necessary to the proper discharge of his mandate, especially to protect the identities of complainants and to foster candor in the investigation and resolution of complaints. Moreover, Parliament is already assured that one of its own officers has ample power to monitor CSIS's sensitivity to the privacy rights of Canadians.

In its 1988-89 annual report, SIRC said that it had asked CSIS to provide it with the files that had been the subject of a complaint to the Privacy Commissioner and a subsequent application under the *Privacy Act* to the Federal Court of Canada. The reason given by SIRC for this request is:

"We wanted to assure ourselves that the Service had not unreasonably withheld anything from the Privacy Commissioner's examination".

While the Privacy Commissioner appreciates SIRC's support, this statement reveals a lack of understanding of his role and powers vis-à-vis CSIS.

In conducting investigations of complaints against CSIS, the Privacy Commissioner has extensive powers to enter premises, compel the production of witnesses and documents and take evidence under oath.

Section 68 of the *Privacy Act* makes it a summary conviction offence to obstruct the Privacy Commissioner in the performance of his duties and functions. The Federal Court, too, has a role in ensuring that CSIS respects the *Privacy Act*. The Privacy Commissioner or a complainant may ask the Federal Court to review a decision by CSIS to deny access to requested information.

Surely it carries the notion of "oversight" to an extreme to suggest that SIRC has a role in ensuring that CSIS acts lawfully in its dealings with the Privacy Commissioner and with individuals exercising *Privacy Act* rights. That, in effect, would be reviewing the reviewer, Parliament's reviewer at that. Such a proposal calls into question the effectiveness of the Privacy Commissioner as well as the Federal Court. It even implies misbehaviour on the part of CSIS in its compliance with the *Privacy Act*. Such an implication is unfounded and unfortunate in the light of the commendable effort of CSIS to live by the letter and spirit of the *Privacy Act*.

A parallel monitoring by SIRC of CSIS's dealings with the Privacy Commissioner would send all the wrong signals to CSIS, the Privacy Commissioner, the Federal Court, Parliament and the public.

Consequently, the Privacy Commissioner recommends that any amendment to subsection 39(2) of the *CSIS Act* should not provide SIRC with a right of access to correspondence between CSIS and the Privacy Commissioner related to a *Privacy Act* investigation.

SINning...again

Lest the litany of SIN become a dirge, there were upbeat notes during the year.

Reports on the Commissioner's comments and suggestions about SIN have made the office a lightning rod for much of the public's frustration about trivial uses of the number. Consequently, many calls and letters concern uses well outside his mandate—most of them in the private sector.

Rather than pleading no mandate, the Commissioner has taken to passing on the comments, always emphasizing that their requests are not illegal but often offensive. He uses the opportunity to sell the concept of voluntary codes in the private sector and suggests that a little more sensitivity to SIN requests might reap public relations benefits.

The response has been surprisingly positive from, among others, General Motors, the Canadian Council of Professional Engineers, the University of Western Ontario and J.B. Marketing—a computer technology company.

Some details of these exchanges follow.

An MP had passed on to the Commissioner an advertisement in an engineering journal containing a Mastercard application which required the SIN. The executive director of the Canadian Council of Professional Engineers sympathized with the Commissioner's comments about the growing use of the SIN as "a de facto national identifier".

He replied, "while I concur that requiring the SIN is bad business practice and I will ensure that no further requests for it are made in the Mastercard advertisements...I have to wonder if by now any attempts to guard our privacy come too late." Citing the government's original (1964) commitment to use SIN only for social insurance benefits, he urged the government to "set a good example by not requesting the SIN when processing Canada Savings Bonds purchases."

The Commissioner conceded that the government's admirable new, more restrictive SIN policy had been "muddied" by recent changes to the *Income Tax Act*, but encouraged him not to despair and to continue resisting frivolous requests for the number.

A General Motors newspaper advertisement for a preferred customer card under GM's Smartlease program prompted a call from another MP. This ad also asked for the applicant's SIN. The MP considered the request "an example of excessive use of SIN".

The president of General Motors replied that the Commissioner's letter had given GM an opportunity to test one of its corporate values—to be "customer focused". He wrote: "... all future General Motors advertisements containing a form for customer information will no longer require the applicant's Social Insurance Number".

Two university requests for SIN were also eliminated. One problem was solved by the University of Western Ontario's ombudsman who succeeded in convincing university administrators to stop using the number when issuing locker keys to students.

Another student (at Simon Fraser University) objected to having to produce the SIN to prove that he qualified for a discount when buying computer software. Privacy staff inquired and found the request was contained on an outdated form the company, J.B. Marketing, had provided to the university.

The company told the Commissioner that in revising its American form, the request for SIN had been overlooked. Its education department "attempts to inform our clientele the SIN is not required to process the order". The company suggested the client get in touch with their representative to straighten the matter out.

SIN can be overcome when there is will and consumer resistance.

Thanks to Mr. Statsman

Worthy of special mention in an end-of-term report is the tangible commitment to privacy demonstrated by the Chief Statistician of Canada. It is especially noteworthy because many of the *Privacy Act* requirements do not apply to statistical records. Yet the Chief Statistician has voluntarily established the practice of consulting the Privacy Commissioner on privacy issues concerning statistical records.

Though Statistics Canada data bases are for statistical uses only and cannot lawfully be used in any decision-making process directly affecting individuals, detailed and sensitive profiles of individuals can be compiled from such statistical data. Thus decisions about establishing and linking such information holdings raise privacy concerns.

A project being considered by Statistics Canada will illustrate the point.

Statistics Canada proposes to cooperate on a health survey with the Manitoba Department of Health and the Canadian Institute for Advanced Research. The project would link limited information from the Manitoba health data bank with Statistics Canada data, including some taken from the 1986 census.

This proposal, known as the Manitoba Population Health Pilot Project, would create a statistical data base to help the Manitoba government assess its health care needs and to develop health policy options. Of course, other provinces have expressed an interest and Ontario has lent its strong support.

This proposal is unique because it would link census data with other administrative data bases. While postal codes, and not names or addresses, would provide the link, the resulting data (under the sole control of Statistics Canada) would be information about identifiable individuals. The original data subjects could not have foreseen that the information originally provided to Manitoba and Ottawa would be used to create detailed, sensitive profiles on individual Manitobans.

The Chief Statistician took the initiative, as he has on other privacy matters, and sought the Privacy Commissioner's view on whether the public interest justified conducting this record-linkage.

The Privacy Commissioner agreed that the proposed pilot project had potential for contributing significantly to the public interest; most important, he considered it possible to accomplish the goal without intruding on personal privacy. He suggested protecting the individuals' privacy by stripping away the personal identifiers—in this case the postal code.

Some may consider the *Privacy Act* remiss in not subjecting personal information used for statistical purposes to the same requirements imposed on personal information used for administrative purposes. No one should doubt, however, that the privacy concerns about statistical data are being addressed in practice.

The Chief Statistician of Canada is to be thanked for that.

Spreading the word

An organization's communications function is not usually the subject of an emotional debate. But the role of an ombudsman requires a delicate balance between telling the public he exists without appearing to be generating his own work or damaging his credibility.

Specialist ombudsmen such as the Privacy Commissioner have also to tread the fine line between being an advocate for the principles of their legislation while being seen as impartial enough to mediate disputes. The debate is not new.

The Privacy Commissioner does not have a mandate to tell the public what he can and cannot do as have the Chief Human Rights Commissioner or the Commissioner of Official Languages. However, since his office operates with taxpayers' money and provides a service to "anyone present in Canada", he must try to be visible, accessible and accountable to those who pay the bills.

Although the Commissioner has not allowed the absence of a specific mandate to prevent him from telling Canadians about their privacy rights, the lack of funds restricts this work. After seven years, many legislators and public servants—and, based on anecdotal evidence, most members of the public—know nothing about their privacy rights, a disappointing legacy.

However, strides have been made. During the past year alone, the Commissioner and staff spoke to more than 60 audiences which ran the gamut of government, the private sector, labour and universities. The Commissioner urged the private sector to adopt voluntary privacy codes at meetings of the Canadian Public Relations Society, the Canadian Information Processing Society, the Air Transportation Association of Canada, federally-regulated employers in the transportation and communications sectors and the Issues Management Association.

The Commissioner or his staff have spoken to (among others) a special Statistics Canada seminar considering a proposed match of federal social program data with provincial welfare files; the National Joint Council on employee privacy issues; records managers on the new data matching and Social Insurance Number policies; the Law Hours at Dalhousie University and the University of New Brunswick; and two classes of CSIS recruits.

The office has distributed its information material to members of the Canadian Library Association, L'association des bibliothécaires professionnelles du Québec, Employment and Immigration centres in eight provinces and MPs' constituency offices. Public affairs staff have also handled almost 1600 requests for material about the *Privacy Act*, the Commissioner's role and the impact of data protection.

Drug testing: everybody's doing it

Last year's report discussed the threats posed to privacy by new biotechnologies. There was a promise to monitor these developments.

Thus, the Privacy Commissioner's office completed a major study of the impact of drug testing technologies upon privacy and the *Privacy Act*. It is soon to be made public.

The study examines the scientific limitations of urinalysis, the most common drug-testing (other than alcohol) technology. Such testing cannot determine or measure the degree of impairment nor can it verify present use. It can verify only past use, and this with an error rate of from two to five per cent.

For this reason, urinalysis is a tool different from breathalyser or blood tests. The latter can provide confirmation of use and impairment at the time of the test—be that while operating a motor vehicle, or performing some other safety-sensitive function. Urinalysis, on the other hand, can only confirm past drug use—use which may have taken place in the privacy of one's home and have no impact upon the performance of safety-sensitive activities.

The *Charter of Rights and Freedoms* may stand in the way of infringing upon a person's "liberty" to consume intoxicants when it poses no reasonable threat to health or safety. This was the decision of the Quebec Superior Court in the case of *Dion v. the Queen* (1986).

Urinalysis testing intrudes into private lives. It is scientifically unsuited to answering the questions of whether an individual engaged in safety-sensitive activities is using, or is under the influence of, performance-altering substances. Yet governments and private sector firms appear eager to use urinalysis to protect the public, find the perfect employee or both.

Transport Canada, for example, is proposing random and mandatory testing of Canadian transportation workers. Privacy concerns notwithstanding, the government is to be commended for initiating a process of public discussion of this proposal, including bringing the matter before Parliament by way of legislation.

There will be opportunities for all concerned parties, including the Privacy Commissioner, to address such hard questions as:

1. Is there reliable evidence of a significant drug abuse problem among transportation workers?
2. Are there available less intrusive means of dealing with such abuses?
3. Are adequate safeguards in place to satisfy a reasonable expectation of privacy? and
4. What role are U.S. testing requirements in the transportation industry playing in determining Canadian testing policy?

These matters are addressed in the Privacy Commissioner's study on drug testing and the *Privacy Act*.

Genetic analysis

Unprecedented research energy is being put into exploring the human gene for the wealth of information it contains about individuals. This area of bio-medical study is opening marvelous new diagnostic avenues, enhancing the possibilities of early detection of disease, improved treatment and ability to avoid the transfer of hereditary conditions. Genetic analysis is also becoming a major tool in the law enforcement field for identifying persons—either to confirm or eliminate suspects.

As with all technologies, however, there is a dark side. Genetic analysis is being explored to determine its reliability as a predictor of future behaviour—pre-disposition to antisocial behaviours or to mental or emotional disorders. The perennial search for the perfect employee is leading some to look to genetic analysis for information on the likelihood that an employee will remain healthy (genetic pre-disposition to cancer or heart disease), be honest and stable and have an aptitude for the job.

In the insurance industry, too, the possibilities of new gene technology have not gone unnoticed. In an industry where AIDS tests are becoming mandatory for life insurance policies over a certain amount—think of the attractiveness of a gene assessment.

Finally, this technology makes possible prenatal selection—with an especially frightening potential for discrimination against those who don't "measure up".

Canadian law has to do some running to catch up to the present state of genetic technology. We are lagging behind other countries and there is much at risk by our slowness.

Germany is on the leading edge. An official commission of inquiry of the German Parliament has already reported on the opportunities and risks of genetic technology. German federal and state privacy protectors have issued guidelines to control the threat gene analysis poses to privacy. Both reports conclude that stringent federal laws are required to control this technology. The recommendations include:

1. limit gene analysis in the criminal justice system to confirmation of identity only;
2. prohibit gene analysis in employment matters;
3. require insurance contracts to state that gene analysis is not a prerequisite and provide assurance that standard consents for disclosure by physicians will not cover genetic analysis information;
4. allow prenatal genetic probing only to reveal a curable condition which would otherwise lead to unacceptable damage to the future health of the child;
5. limit genetic screening of newborns to genetic illness which can be cured or at least substantially controlled by therapeutic means; and
6. require, except in law enforcement, gene analysis only be conducted on the basis of a truly voluntary and fully informed consent.

Such guidelines offer an important groundwork of protection against the dark side of genetic technology. Though some of these recommendations remain open to debate or may be beyond its legislative jurisdiction, Parliament should be aware of the fast-developing issues, do what it can as soon as it can, and prepare legislative proposals to control the uses of genetic analysis.

The Ontario Law Reform Commission and the recently-appointed federal Royal Commission on Reproductive Technology are both examining wider issues in this area and are aware of the possible need to respond to the new genetic technologies.

The Privacy Commissioner will continue to monitor the related privacy issues and keep Parliament informed.

Police databases-CPIC

Some of the most sensitive personal information held by government is in the automated data bases administered by the Canadian Police Information Centre (CPIC).

CPIC's computerized information system has four major data bases to which law enforcement agencies contribute—and from which they can obtain—a wide range of information. According to the RCMP, there were more than 72 million operational transactions on these data bases during the 1987/88 fiscal year; more than 21 million of these concerned individuals.

The centre, federally funded and administered by the RCMP, is governed by an advisory committee of the major municipal and provincial police forces (the RCMP in eight provinces) and the attorneys general of Ontario and Quebec. However, the sole authority for CPIC policy and procedure is the Commissioner of the RCMP.

Since some of the information is contributed by non-federal sources, jurisdiction over personal information in the centre's data bases remains in question. The need for some effective data protection oversight is not.

CPIC was established to provide more efficient handling and exchange of law enforcement information. The RCMP describes the system as "facilitating country-wide access to police information" and "improving the collection, storage and control of records by police forces".

Access to the data bases is controlled according to whether the requestor is a federal, provincial or municipal police force, foreign law enforcement agency or an agency with a limited law enforcement role (such as Canada Customs or Employment and Immigration).

The four data bases are:

1. Investigative Data Bank Files. These include files on missing and wanted individuals (including missing children), stolen vehicles and boats, major unsolved crimes and recovered but unidentified bodies.
2. Identification Data Bank Files. The files include criminal records and the criminal name index.

-
3. Intelligence Data Bank Files. These files include the Automated Criminal Intelligence Information System (ACIIS) with limited access from 27 terminals controlled by the Canadian criminal intelligence community. There are no foreign interfaces to ACIIS. The information concerns individuals, businesses, vehicles and other subjects. The "Focus" file contains information on organized motorcycle gangs.
 4. Ancillary Data Bank Files. These include registered vehicle owners, licensed drivers and information from federal and provincial correctional services.

The RCMP also operates a fifth automated system known as PIRS (Police Information Retrieval System) but not under the CPIC umbrella. PIRS contains information on events, subjects, vehicles and property. The service is operated on cost recovery and is available to other federal departments and to 12 municipal police forces.

After its in-depth review of the *Privacy Act*, the Justice and Solicitor General Committee recommended that CPIC be made subject to the Act and that the Privacy Commissioner audit the data bases to verify that the privacy interests of Canadians were being adequately protected.

The government rejected the recommendation, choosing instead to consult the participating law enforcement agencies on how best to address the privacy issues. After it appeared that no solution was forthcoming, the Privacy Commissioner suggested that the RCMP consult CPIC users to determine whether it could implement voluntary privacy controls over its data bases. These controls would take the form of a comprehensive data protection policy on the collection, use, disclosure and disposal of the information and the creation of access and correction procedures.

The Commissioner made four suggestions.

First, the most difficult aspect of a voluntary code would be to provide an acceptable access and correction procedure. The Commissioner urged the RCMP to go beyond simply referring applicants back to the source agency and to consider making access available to the entire system through a single access point.

Second, he asked that the policy restrict itself to limited, well-defined exemptions, cautioning the force against going beyond the exemptions contained in the Ontario, Quebec and federal privacy legislation.

Third, the Commissioner asked that the policy assure individuals that incorrect or incomplete information will be corrected or deleted in both the automated system and the original records. If there is an unresolved dispute about the accuracy or completeness of any information, it should be flagged as being disputed and a notation of the individual's version included on the file.

Finally, the Commissioner urged the force to provide a mechanism for handling disputes about exemptions, delays and correction requests.

The RCMP responded positively to the Commissioner's suggestions and has already begun applying these principles to its own systems, including the PIRS. The force also presented the Commissioner's views on privacy protection to the CPIC advisory committee which is actively considering voluntary privacy controls.

It is too soon to know whether there is any future for voluntary privacy controls over CPIC. But the police community's willingness to examine the options is reason enough for optimism that a balance can be struck between legitimate law enforcement needs and individual privacy rights.

Ring, ring... Orwell calling

Last year's annual report discussed the privacy implications of a proposal before the Canadian Radio-television and Telecommunications Commission (CRTC) which would require Bell Canada to sell its directory data base in machine-readable form. (At this writing no decision has been given.)

In 1989-90 another telephone privacy issue surfaced.

In this one Bell Canada sought CRTC approval for a number of services, including one which would display the originating phone number of all incoming calls on specially-equipped telephones. This proposal presented a feast of privacy issues. The service would protect subscribers from harassing or simply unwanted calls—a real “plus” for privacy. But it could also render it impossible to make an anonymous telephone call—a privacy “minus”.

After some initial hesitation—one is reluctant to prescribe which privacy value is more important—the Commissioner concluded that the privacy minus outweighs the plus. At base, it is unacceptable that we should surrender our anonymity as a necessary condition of using the telephone. The telephone is a basic public service which policymakers cannot treat as optional.

There is public interest, of course, in offering to subscribers a method for deterring abusive or intrusive incoming calls. To choose total loss of anonymity for all subscribers, however, is akin to invoking the *War Measures Act* to deal with a barroom brawl.

Perhaps the issue is not as black and white as it is painted. Is there not some middle ground—some way to give subscribers the proposed technological features while allowing others who can show a legitimate need to remain anonymous to opt out? Other jurisdictions have, for example, given number blocking capability to undercover police officers and to those who help victims of domestic violence. We searched for such a compromise.

In the end, however, the answer is clear: the issue is, indeed, black and white. Ours is not a society where the privacy rights of some are broadly paramount to or imposed upon those of others. The fundamental rights and freedoms contained in our Charter presuppose a carefully guarded underpinning of privacy.

Can one imagine that freedom of expression, of association or belief, or the right to liberty and security of the person, could be meaningful in the absence of strong protections of our privacy? Clearly the answer is "No", and it has already been unequivocally given by the Supreme Court of Canada in such cases as *R v. Dyment* (1989) and *Mario Duarte v. R* (1990).

It would too greatly diminish the state of our personal privacy if every call we made to merchants, government departments, social agencies or media outlets disclosed our identities. To prevent that loss of control surely we are willing to tolerate the fact that some may abuse their ability to call anonymously.

A new exempt bank

This year's news that the Canadian Security Intelligence Service (CSIS) would establish a new exempt bank—with the support of the Privacy Commissioner—demands some explanation.

This is particularly true since the Commissioner has always viewed the concept of exempt banks as contrary to the spirit of the *Privacy Act*, albeit necessary in very limited circumstances.

The tortured history of challenges to the original 20 exempt banks is traced in earlier annual reports. Of the three remaining, Revenue Canada/Taxation's is treated as open and its exempt status will soon be revoked. The RCMP's exempt bank order has recently been revoked and replaced. The new order was necessary because the individual files in the bank had not been reviewed, making the old order invalid. The Canadian Security Establishment's bank was validly constituted and remains closed.

CSIS's proposal to make an exempt bank simply recognizes that SIS/P-PU-010 is already effectively closed. This bank contains information about individuals who are approved CSIS surveillance targets or who have come into contact with targeted individuals or groups. CSIS responds to applications to this bank by neither confirming nor denying the existence of personal information. The *Privacy Act* does not require an agency to confirm that information exists if it "could reasonably be expected" to be exempt under other provisions of the Act.

The philosophy of this approach, simply put, is that it could injure CSIS's ongoing work for persons to know that they were or were not a CSIS target. Both the Privacy Commissioner and the Federal Court (in *Jamshid Zanganeh v. Canadian Security Intelligence Service*) have endorsed this position.

Less sensitive intelligence information (for example, about individuals who came to the attention of the former RCMP Security Service) may be released, with appropriate exemptions, from bank SIS/P-PU-015.

The current state of affairs—an officially open but effectively closed bank—misleads the public and may give the *Privacy Act* a bad name. Thus it is better to establish a properly constituted exempt bank.

Such action would put an extra burden of responsibility on the Privacy Commissioner to ensure that an exempt bank contains only information of this most sensitive nature. No exempt bank once established can be allowed to become an uncontrolled hiding place for personal information. Indeed, the *Privacy Act* recognizes this in section 36 by giving the Privacy Commissioner the mandate to examine exempt banks from time to time, recommend that files be moved to open banks, make application to the Federal Court to order the removal if the Service does not accept the recommendation and, of course, to report any non-compliance on the part of CSIS to Parliament.

When CSIS has a functionally exempt bank, as at present, as opposed to an official exempt bank, the Privacy Commissioner is deprived of those oversight powers and, most significantly, the power to apply to Federal Court, under section 43 of the *Privacy Act*, “for a review of any file contained in a personal information bank designated as an exempt bank under section 18”. The CSIS proposal to re-establish an exempt bank would correct this anomaly.

However, judging from a statement accompanying the proposal to close the bank, CSIS may be under the impression that closing the bank means it can deny access to the information without having to review the files. That is not how we read the Act. The provision for exempt banks makes it clear that refusing access to an exempt bank is discretionary, not mandatory. Perhaps CSIS will be able to explain to the Commissioner or the courts how it will exercise that discretion without reviewing the file. Responding properly to an application would seem to dictate reviewing the file, regardless of whether the bank is exempt or not.

While CSIS may not have to justify denying access by applying one or more of the nine specific exemptions, anyone who is denied access to an exempt bank can complain to the Privacy Commissioner. Investigators would then review the relevant information and, if it does not qualify for inclusion, CSIS would be asked to remove it and process it as if it were in an open bank.

The Privacy Commissioner would not support granting exempt status to any bank if it would reduce the amount of personal information otherwise accessible to individuals under the Act. However, because of the nature of most of the information now contained in bank 010, and proposed to be included in the new exempt bank, he is satisfied that with or without exempt bank status it will be justifiably kept secret.

Making the bank exempt is the responsible course of action: no more confusion about whether the information is accessible, yet appropriate mechanisms to ensure that the exempt bank is sensitively used.

Complaints Directorate

After successive years of see-sawing complaint statistics—a new counting method in 1986/87, a decrease in 1987/88 and a substantial rebound last year—this report contains no surprises.

The office received 1086 complaints during the year, a modest increase over last year's 1039. Investigators completed 1018, of which 559 were well-founded; 410 were not well-founded and 49 were withdrawn or abandoned.

Fair information code

Another trend continues apace: the steady increase in complaints about breaches of the fair information code contained in sections 4 to 8 of the *Privacy Act*. This code controls the government's collection, use, handling, disposal and security of the personal information it uses to administer its various programs. Since 1984-85 this type of complaint has more than quadrupled.

Canada Post, for example, has experienced a remarkable increase in complaints, particularly those concerning the collection and use of personal information—from 12 in 1988-89 to 61 this year. Clearly, Canada Post employees have come to regard the *Privacy Act* as a mechanism to resolve labour-management disputes. This can be seen as employees challenge demands for more personal information under Canada Post's new leave management policy.

Denial of access

Denial of access remains marginally the largest single category of complaints. Health and Welfare, for example has experienced a large increase in complaints, a number of which concern the issue of ownership and patient access to medical records.

Prior to this year, Health and Welfare denied patients access to even the most routine medical information unless the treating doctor consented. The office succeeded in convincing Health and Welfare to consult only in special cases, a procedure that should reduce the time required to process requests and fewer denials of access.

Time limit complaints

Time limit complaints increased marginally this year. Correctional Service Canada (CSC) remains the number one laggard—responsible for 214 or 50 per cent of all time limit complaints. The Privacy Commissioner considered 78 per cent of these well-founded. National Defence was a distant second with 80, 85 per cent of which were well-founded.

These institutions' time limit problems were first described in the 1984-85 annual report.

While our statistics show a decline in delay complaints across government, CSC has not yet been able to address its problem. Indeed, there is some evidence of an endemic failure by CSC to respect the *Privacy Act's* timeframes.

For example, it became regular practice for CSC to claim extensions for consultation with other government institutions when, so far as the Privacy Commissioner's office could determine, no consultations were undertaken or necessary.

The Act imposes particular difficulties for CSC and at the highest level respect for the spirit and letter of the law has often been demonstrated. However, there has been ample time in seven years under the Act for CSC to allocate adequate resources and establish efficient administrative procedures. Federal inmates make significant use of the *Privacy Act* to obtain their records and CSC is aware that Parliament gave offenders the same rights under the Act as it gave other individuals.

It seems that the CSC bureaucracy simply feels that inmate privacy rights are at the bottom of its priorities.

CSC has eliminated the excessive delays of seven and eight months that once plagued applicants as requests now get responses in 70 to 80 days.

This improvement does not put CSC in compliance with the 30-day response time specified by the *Privacy Act*. That would require substantial procedural changes.

National Defence (DND) appears to be on the way to solving its problem. DND continues to receive almost half of all applications made under the *Privacy Act*, many as a result of its policy requiring members to apply formally under the Act to see their personal evaluation reports. To its great credit (abandoning a long-defended policy takes some doing), DND has decided to treat informally requests for the current evaluation. Not only will this lead to a decline in complaints to the Privacy Commissioner—it could also reduce significantly the number of formal applications to DND.

The lower numbers mean a loss only of a bureaucratic process. This informal approach keeps with the spirit of the *Privacy Act* and marks the end of years of nagging by the Privacy Commissioner and, even, Members of Parliament.

Grounds of Complaints and Investigation Results

| Grounds | Dis-continued | Well-founded | Well-found. Res. | Not Well-founded | Total |
|---------------------|---------------|--------------|------------------|------------------|-------------|
| Access | 11 | 36 | 137 | 259 | 443 |
| Use & Disclosure | 11 | 14 | 19 | 28 | 72 |
| Correction/Notation | — | — | 5 | 21 | 26 |
| Time Limits | 27 | 317 | 10 | 68 | 422 |
| Language | — | — | 1 | 2 | 3 |
| Index | — | — | — | 1 | 1 |
| Collection | — | 13 | 3 | 13 | 29 |
| Retention/Disposal | — | 4 | — | 18 | 22 |
| TOTAL | 49 | 384 | 175 | 410 | 1018 |

New Activities

The directorate embarked on two new activities during the year: assessing proposed new data matches and reviewing section 8(2)(m) notifications. For more detail on these notifications see **Notifying the Commissioner**.

Data Matching Review

The government's data matching policy took effect at the beginning of this reporting year. The policy requires government agencies to notify the Privacy Commissioner's office 60 days in advance of any proposed new data matches of personal information. This permits the Commissioner to act as an advocate for those who may be affected by the match.

The 60-day period allows the Commissioner's office to judge the proposed match against such criteria as:

- *assessing the advantages of the match against other approaches;
- *verifying that the proposed match relates directly to an operating program or activity of the institution;
- *considering whether the information could be collected directly from individuals and if not, why not;
- *determining whether individuals should be notified of the new use and if not, why not;
- *ensuring that the new data will be as accurate, up-to-date and complete as possible;
- *determining the time-frame of the proposal, and
- *determining whether individual consent is needed to match the data;
- *analyzing the costs and benefits of the matching operation.

Following the assessment, the Commissioner can make recommendations about the matching proposal to the head of the institution. The decision to match or not is, ultimately, made by the responsible minister, not the Privacy Commissioner. Of course, the Commissioner may report any serious concerns directly to Parliament.

The privacy staff examined one such match—a new Treasury Board system designed to coordinate departments' responses to access to information requests. The new system aroused fears among users of the *Access to Information Act* that it would reduce the amount of information available (because it would curb some departments tendency to respond more generously than others).

CAIR system

The new system is called CAIR and is not, technically speaking, a data match. It is a network of microcomputers which provides access to a central database of information about departmental access to information requests. Under the plan, departments are required to provide details of access requests to CAIR, which serves as a central reference and communication system for government access policy. Thirty-two departments are linked to the system.

The office examined CAIR to determine whether personal information about applicants could be retrieved from the database. The answer was an unqualified "no" as personal information is not entered into the database and, therefore, no breach of confidentiality is possible. As well, applications are described in a way which would make it unlikely that identities could even be inferred from the text. The investigator also found the system to contain comprehensive and effective security measures. The conclusion was that CAIR does not jeopardize access to information applicants' confidentiality.

The office is also examining three existing Employment and Immigration Canada (EIC) matches to follow up the office's assessment of EIC's internal privacy audit (1988-89 annual report). The matches include comparing Canada Job Strategy files with Unemployment Insurance (UI) Benefit files, immigration files with Secretary of State files and UI Benefit files with British Columbia Social Services files. The evaluation continues.

A third matching assessment is in its infancy and results from the new Good and Services Tax (GST) which will require some matching programs. For example, Revenue Canada anticipates matching GST and Income Tax data. The legislation also requires individuals and sole proprietors to register with their Social Insurance Number. Revenue Canada considers the SIN "the most effective means of cross referencing". The Privacy Commissioner's office is waiting for a detailed submission on the proposal.

The office has also been approached informally by External Affairs to examine a new single personnel data base to replace several stand-alone systems now in use. The Commissioner is waiting for more detail.

Debts deducted from subsidy cheques

A journalist wondered whether the federal government was breaching the *Privacy Act* by deducting outstanding debts from farmers' drought subsidy cheques.

According to the journalist, Agriculture Canada had withheld from the cheques any money owed on farm improvement loans guaranteed by the federal government, debts from cash advance or special grains programs, money owed to Revenue Canada or in default of support payments to spouses. The journalist asked whether Agriculture Canada had conducted a data match to determine what was owed and, if so, did it comply with the Act?

Agriculture Canada told the investigator that as farmers applied for drought assistance, they were to "understand and agree with the terms and conditions contained in the guidelines to the application form and further agree to any adjustment or refund to the Government of Canada that may be required". The conditions included a consent to release information about their farm operations to "any other government department, agency or corporation" and to various provincial agencies and marketing boards.

Clearly, farmers had been told of the conditions and had consented to them and to any releases. The investigator also found that there had been no data match with Revenue Canada files, although one individual's refund had been reduced at Revenue Canada's request. The application form did provide for offsetting refunds against defaulted family support payments, but this program is not yet operating.

The Commissioner concluded that there was no need for a formal investigation but reminded Agriculture Canada to advise his office of any considered data matches.

Notifying the Commissioner

In general, the *Privacy Act* prohibits federal government agencies from releasing personal information to anyone other than the person it concerns. As with most rules, there are exceptions. The act has 13—from releases to comply with a warrant or subpoena, to information to help validate aboriginal peoples' claims or grievances. Two such exceptions require the government agency to notify the Privacy Commissioner. The first covers releasing information "in the public interest" or to benefit the person concerned. Notification gives the Commissioner an opportunity to advise the person should he consider that necessary.

The second exception deals with releases for a use which is consistent with the purpose for which the information was collected but which has not been described publicly in the *Personal Information Index*. New consistent uses must then be included in the next edition of the Index.

There is some confusion about the Privacy Commissioner's role in examining proposed releases "in the public interest". Yet, the Act is clear.

The decision that personal details are of public interest rests with the head of the government institution, usually the minister, not with the Privacy Commissioner. The Commissioner is notified so that, if he believes it appropriate, he can inform the person whose information is being released. (The drafters of the law might also have anticipated that departments would be more circumspect in claiming "public interest" if they had to notify an independent ombudsman.)

The Commissioner cannot prevent the release or require that particular details be withheld—nor can the person concerned. This helplessness is an anomaly, particularly when compared with third parties' rights to block releases under the *Access to Information Act* all the way to the Supreme Court. The Privacy Commissioner has argued before that individuals too should be able to prevent unwarranted or damaging release of their information before it happens.

In practice, privacy office staff has always been ready to discuss a proposed release, which sometimes lead to a department rethinking its approach. The Commissioner remains apart from these conversations to preserve his independence to investigate any complaints that the release was improper.

The following examples are selected from the 32 notifications received during the year.

Doctor's evaluation reports

National Defence informed the Privacy Commissioner that it intended to disclose evaluation reports about a military doctor to a provincial college of physicians and surgeons.

The Forces had audited the doctor's medical unit and his personal competence and then released him from service. Because of the release and the doctor's standard of medical practice, the provincial college asked for the audit reports to help in its own evaluation of the doctor's competence as a physician. The college was concerned that the general public should be assured that licensed doctors meet a minimum acceptable level of medical competence.

The Commissioner notified the doctor of the release.

Japanese Canadians' records released

The Japanese Canadian Redress Secretariat asked National Archives for material in its files from the Vancouver office of the Custodian of Enemy Property.

The information concerns Japanese Canadians who were interned during World War II. It includes the minutes of advisory committees on disposal of property, correspondence, ledgers containing entries on money held in trust and real estate, and business records.

The secretariat considered (and Archives agreed) that the release would be in the public interest as it would allow the government to compensate an anticipated 12,000 Japanese Canadians eligible to benefit from the program.

The Commissioner saw no reason to object.

Reports on two inmate escapes

Twice during the year, Correctional Service Canada (CSC) told the Commissioner that it intended to make public detailed reports on escapes by federal inmates.

The independently-prepared reports described the circumstances surrounding the escapes of two convicted murderers, including names and some personal details about both federal employees and private citizens.

The first report concerned Allan Légère's escape while he was being treated at the Georges Dumont Hospital in Moncton, New Brunswick. Légère was considered dangerous and was suspected in a number of murders while at large. The local population was very concerned. He has since been recaptured.

The second report described the circumstances surrounding the escape of Daniel Gingras while on an escorted day pass from the Edmonton Institution. Gingras had overpowered his guard and stolen the car in which they were riding. He was later convicted of two murders committed while he was at large.

In both cases, CSC believed that there was a substantial interest in the public understanding what had led to the escapes and in being reassured that any mistakes in procedure had been corrected.

The Commissioner wrote to all the parties named in the reports, other than the escapees, to tell them of the circumstances of the release.

Woman seeks citizenship confirmation

Secretary of State told the Commissioner it intended to confirm the Canadian citizenship of a man for his sister-in-law. The man, whose wife had died, had left the country and apparently abandoned his two daughters. The provincial youth authority needed the information in order to rule on the aunt's application for custody of her two nieces.

The Commissioner agreed.

Immigrant's details released

Employment and Immigration (EIC) advised the Commissioner that it intended to brief an MP who was pressing the government to have a man removed from Canada.

The MP believed the man's membership in a particular organization precluded his being considered for permanent residence. EIC proposed to release a number of details to convince the MP that the man qualified for entry.

While the office was examining the proposal, a journalist asked the Commissioner whether he had approved the release. Apparently the MP had already been briefed.

The Commissioner told EIC that he doubted that the release was appropriate. He told the man the details which the MP had been given and advised him of his right to complain.

Ex-employees' privacy

Federal employees don't lose their privacy when they retire. This was illustrated when Supply and Services Canada (DSS) called the office about a request for a list of retired government communications officers.

Emergency Preparedness Canada wanted the list to reach former staff to determine whether they were prepared to be on standby during a major emergency. Emergency Preparedness asked DSS to provide the names and addresses.

DSS staff, uneasy about the request, called our office to discuss the proposal. DSS had rejected the request but wondered whether doing the direct mailing was a proper use of the lists which are assembled to mail pension cheques.

After the discussion, DSS denied the Emergency Preparedness request. It suggested getting in touch with communications people before they retire.

Some Cases

Supervisor's diary a departmental record

A Toronto-area man complained that Public Works Canada (DPW) had denied his request to see a notebook about him that his supervisor was keeping. Communications had broken down between the two men and the supervisor was keeping a diary to document the complainant's work behaviour.

The complainant alleged that the diary was kept in the supervisor's locked filing cabinet. When DPW reviewed the diary it exempted its entire contents, claiming that it concerned another individual (the supervisor) and that its release could endanger him.

When DPW learned about the complaint, it argued that the diary should not have been reviewed at all since it was the supervisor's own personal property and not "under the control of the government institution". DPW also challenged the Privacy Commissioner's jurisdiction to investigate a complaint about "private property".

When privacy staff asked to examine the diary it became apparent that the department could ask the supervisor to produce the diary at any time (for example, in response to the original privacy application) and, therefore, it was under DPW control.

The investigation also revealed that the supervisor had begun keeping the diary after a discussion with a more senior manager. All the entries dealt with the complainant's comings and goings and activities on the worksite. The supervisor had prepared the notes in his capacity as a public servant and the information could be used for such work-related purposes as preparing evaluations or responding to grievances. Therefore, it was subject to the *Privacy Act*.

The diary contained little information about anyone else and did not qualify as the personal information of the supervisor. This discovery called into question DPW's original exemption on the ground that the information concerned other staff members. DPW had also maintained that the supervisor had begun the diary because he believed his safety was being threatened and he might need a record in the event of legal action. However, the supervisor told the investigator he did not believe releasing the diary would threaten his safety. Despite a series of meetings, the department and Commissioner's office continued to disagree on control of the diary. Staff continued to try to resolve the impasse and, following several months' discussions, DPW agreed to give the complainant a photocopy of the diary pages after removing information about other individuals.

The Commissioner considered the complaint well-founded.

... But not board members' aides-memoire

A somewhat similar case reveals some fine distinctions between information intended to be used for an administrative purpose (as in the DPW case)—and notes taken as an “aide memoire” by a member of a quasi-judicial board.

In this case a former government employee was denied access to notes taken by an adjudicator during a hearing of the Public Service Staff Relations Board. The adjudicator was hearing the man's appeal of his discharge for unauthorized use of the government telephone system.

Adjudicators take copious notes during the hearings because the proceedings are not taped and no transcript is prepared. Their notes must reflect all the evidence presented and issues raised, not simply the conclusions reached. They then write their decisions using their notes as a reference. These notes are usually destroyed once the decision is released. In this case they were not.

When told of the complaint, the board argued that the notes were the personal property of the adjudicator and not controlled by the board, even though they were in his office. The board cited jurisprudence which supports that position. However, without prejudicing the argument, the adjudicator agreed to let the privacy investigator examine the 92 pages of notes.

There was no doubt that the information concerned the applicant but it was all essentially a recording of the evidence presented in an open hearing. The notes themselves were not evidence and were not used for an administrative purpose. The Commissioner concluded that the notes were not under the board's control and therefore not subject to the Act.

The Commissioner also observed that, even if the notes were under the board's control, they could be withheld under another section of the *Privacy Act* which allows exemptions of information which could harm the administration of a law. He considered that examining an adjudicator's notes could harm administration of this and similar acts by attempting to get behind the decision. The Commissioner concluded that the complaint was not well-founded.

Costs to be borne by department

One complaint prompted the Commissioner to remind Health and Welfare Canada (HWC) that costs to provide access must be borne by the department. The complaint concerned HWC's response to a Nova Scotia man's request to see the file which contained his application for a Canada Pension Plan disability which had been denied.

The man complained that he had waited two months for “useless” information—in excess of the 30 days allowed. The complainant told the investigator that one of two doctors' reports about him had been withheld because seeing it would not be in his “best interest”. Although the doctor had refused to release the report, he had agreed to discuss it with his patient. According to HWC, the man would have to pay any charges for the consultation.

A fairly straightforward complaint became a headache when HWC failed to respond to the complaint notification or to return phone calls. The problems were compounded when the investigator went to examine the material and discovered that the entire file had been lost—the disability application, the appeal of the HWC decision and the record of his privacy application.

Medical information can only be withheld from the patient when the department can demonstrate that the release would be contrary to the individual's best interests. HWC staff conceded this would be difficult to prove since the file was lost. HWC also agreed that it was improper to charge applicants for any procedures under the *Privacy Act*.

The complainant consulted the doctor as suggested and was not billed. He does believe that the doctor charged the provincial health care plan for the consultation.

The file remains lost. However, HWC has introduced new logging and handling procedures for all personal files and has begun a pilot project on a new tracking system.

The Commissioner concluded that the delay complaint was not well-founded since departments may take up to 30 days longer to consult other parties (in this case the two doctors). HWC claimed to have mailed the information 56 days after receiving the request and so met the 60-day deadline. However, the complaint that access was denied was well-founded since the Commissioner could not examine the information to determine that it had been properly exempted. The complaint that the applicant was to be responsible for any charges was also well-founded.

40-year old mistake corrected

An Ontario man wrote to the Commissioner in a last ditch effort to have National Defence pay what he alleged was a 40-year-old debt.

The man had served in the British forces during World War II and was entitled to an end-of-service gratuity. When the British notified the man in September 1946 that the gratuity would be paid in Canada, he wrote back to ask how it had been calculated. The British Admiralty responded in November, referring to "the payment made to you recently".

In the meantime, he had received his Canadian gratuity but not the British payment which should have been included. When he asked National Defence for the money, it refused, apparently relying on the British letter as proof that he had already been paid.

The man pursued the matter over many years, enlisting the help of a number of MPs and defence ministers. Each time his request was denied because DND relied on its latest correspondence to prove that he was wrong. Yet, no-one checked the original documents to see where the mistake had been made.

As a last resort, the complainant applied under the *Privacy Act* hoping to bypass all the subsequent letters and to examine the original documents in his pay account. He complained to the Commissioner when none of the material he received established that the payment had been made. He alleged that material he needed must have been withheld.

The investigation unearthed nothing new—he had received everything in the file. It appeared from an old pay document that the British payment was credited to the man's account. The disputed amount was then noted as being paid on the basis of the Admiralty letter. It was then deducted from the total owing.

The Commissioner concluded that DND had not denied access to any material. There was no documentary proof that the payment had been made. The Commissioner wrote to the complainant with his finding, suggesting that he show the Defence Minister the letter because it might help resolve the 40-year dispute.

When the office followed up, the man had moved and left no forwarding address.

Returned mail identifies inmate

An inmate complained to the Commissioner that Kingston penitentiary staff had returned two of his parcels, advising the senders that as a federal inmate he was not permitted to receive them. He considered that disclosing that he was an inmate was an unwarranted breach of his privacy.

The two packages, one from the U.S. Senate and the other from the Manitoba tourism department, contained road maps and travel material. Inmates are not permitted road maps and brochures describing the area around the penitentiary because they could be used to help an escape. The man had been allowed other travel material.

Correctional Service Canada (CSC) told the investigator that inmates may not receive "radios, books..etc.". All parcels are opened and searched for contraband then, if they are unauthorized, are re-sealed and returned to sender with a note quoting the relevant section of the penitentiary's standing orders. CSC maintained that the fact that someone is in a federal penitentiary is public information.

The Commissioner pointed out that CSC's own disclosure code does not permit releasing the inmate's location. Doing so is considered counterproductive to the inmate's eventual reintegration into society.

In the meantime, the inmate had lodged an internal grievance on a number of issues, including this one. When the grievance was upheld at the second level, Kingston penitentiary stopped identifying addressees of returned parcels as inmates.

The Commissioner recommended that CSC establish a policy to ensure that this disclosure not be repeated. Early this year, CSC issued a policy to all its regions requiring mail to be returned "with sensitivity".

According to the new policy, "simply marking the unauthorized package or mail as 'refused' and returning to the return address, with no further explanation, is sufficient...".

The Commissioner considered the complaint well-founded and resolved.

Complainant sees board documents

A man complained to the Commissioner when Canada Post denied him access to submissions to a review board and its final report.

He wanted to see all material examined by the board to determine whether Canada Post had had sufficient evidence of his distributing hate propaganda to warrant intercepting his mail.

Canada Post restored his mail service after the board's public hearing and report.

The complainant also alleged that Canada Post had given the report denied to him to a third party who quoted from it during a newspaper interview.

Initially, the privacy investigator found that Canada Post had not reviewed the material page-by-page, deciding that withholding the entire ten-volume file could be substantiated under a variety of exemptions. As a result of the investigator's request, staff reviewed the file and claimed the following specific exemptions.

*information provided in confidence by another government (section 19);

*information obtained or prepared by an investigative body (section 22(1)(a));

*information which could threaten the safety of individuals (section 25);

*information about other individuals (section 26);

*information subject to solicitor-client privilege (section 27).

Canada Post's Security and Investigations Services is an investigative body under the *Privacy Act*. Thus, most of the requested information could be withheld. However, the board report did not fit this exemption category, nor did documents submitted to the board hearings by the Canadian Civil Liberties Association (CCLA) and an expert witness.

Canada Post agreed to reconsider this material and withdrew its claim that releasing some of the material would endanger other individuals.

Following months of negotiations, Canada Post allowed the man to examine the board's report and the expert witness's submission. When the CCLA submissions continued to be withheld, the privacy investigator suggested Canada Post seek CCLA's permission to release. The CCLA agreed and Canada Post made the documents available.

The Commissioner concluded that the other exemptions were valid and considered the complaint well-founded and resolved.

The office could not investigate the man's allegation that the report had been improperly disclosed because it happened before the *Privacy Act* came into force.

Police told inmate to see reports

Information supplied by other governments "in confidence" must be withheld under the *Privacy Act*. The outcome of investigations into denied release is often a foregone conclusion: If a provincial or municipal government designates the information confidential, it may not be seen

In two cases, however, the privacy investigator found that both National Parole Board (NPB) and Correctional Service Canada (CSC) withheld the same information from an inmate even though the parole officer told the city police force that the inmate would see the information it provided and the force had agreed.

The investigator found other information received in confidence from the provincial government had been similarly exempted. The Commissioner concluded that the provincial government information had been properly exempted but not so the police force material. Both NPB and CSC agreed to release.

Income tax data in harassment file

The *Privacy Act* specifies that information gathered for one purpose may not be used for another unless the secondary use is consistent with the original purpose.

Thus, a Revenue Canada, Taxation employee complained that the department had used his income tax information in a harassment investigation.

At the same time as the complainant was being investigated for the disciplinary matter, he grieved that he had been wrongfully selected for a tax audit. The privacy investigator examined the harassment investigation file and found several references to the complainant's tax situation. He also found evidence that the harassment investigator had access to the complainant's income tax return.

The Privacy Commissioner considered that the tax information should not have been in the harassment file nor should the harassment investigator have had access to the income tax return.

When the Commissioner told Revenue Canada that the complaint was well-founded, the department asked him to consider new facts. The Commissioner agreed, but further interviews uncovered nothing new. Though there was income tax information in the man's personnel documents, Taxation management insisted that it had disciplined him because of the outcome of the harassment investigation and not because of tax information.

The Commissioner could not say conclusively that the tax information had been used for discipline purposes, but the "mere presence of such information in unrelated files constituted a misuse...under the *Privacy Act*". He reiterated that the complaint was well-founded.

No details from other employer

A Nova Scotia man challenged Canada Post's collection and disclosure of his personal information to process his claim for worker's compensation. He had gone to work for Canada Post during a postal strike while on leave from another job. He was injured on his first shift and claimed compensation.

Employers documenting a worker's compensation claim must describe the tasks the employee would be expected to perform on return to work and provide a medical assessment of the employee's fitness to perform those tasks. Since the man was not a full-time Canada Post employee, the corporation obtained the information from his other employer and a Canada Post-appointed doctor. It then sent the information to the Nova Scotia Worker's Compensation Board for adjudication of the claim.

The privacy investigation had to determine whether Canada Post's collection and disclosure of this information was required by the *Workers Compensation Act*. To do so, the Commissioner asked the board to describe what information employers are required to provide to support such a claim.

From the board's response the Commissioner concluded that Canada Post had authority to collect information about the circumstances of the injury at its worksite but it was neither authorized nor required to collect information from the other employer. Further, the board did not ask Canada Post for details of the complainant's medical fitness to return to work. Apparently, the complainant was never told who would receive the medical report.

The Commissioner concluded that the complaint was well-founded. Canada Post has since drafted new procedures to govern compensation claims for anyone injured on Canada Post premises but who is substantively employed elsewhere.

Can't use compensation claim to fire employee

A Correctional Service Canada (CSC) employee told the Commissioner that CSC had ordered her to undergo psychological testing to support her claim for workers compensation, then used the medical reports to fire her.

The woman, a case management officer in a federal penitentiary, was ordered to take the tests to support her claim for compensation for stress brought on by sexual harassment by inmates.

The investigation confirmed that the tests had been conducted to document her compensation claim and that she had not been told the results would be a basis for dismissal. In fact, CSC also used the results to reject her application for another job.

The Commissioner concluded that CSC had misused the test results and that her complaint was well-founded. He asked CSC to guarantee no such situation would recur. CSC has since distributed an employee privacy code to its staff.

Medical details need not be given

Several employees of Canada Post's (CPC) Huron region complained that the corporation was threatening to discipline anyone who refused to complete "voluntarily" a consent for their doctor to give medical information to Canada Post.

The investigation revealed that in each case the employee had taken sick leave and completed the required occupational assessment form on their return to work. Local CPC management was dissatisfied with the form (which does not include a diagnosis) and asked employees to consent to their doctors giving Canada Post medical details.

Employees who refused to sign the consent form were disciplined for "insubordination" and warned that continued refusal would lead to dismissal.

Canada Post headquarters, when told about the complaints, ordered the practice immediately stopped and the regional director of labour relations rescinded dismissals brought to his attention. However, despite the promised resolution, the complaints continued. There seemed to have been a breakdown in communication.

Finally, Canada Post HQ instructed all its divisional general managers that they had no right to detailed, medically-sensitive information and that signing a consent to release this type of information must be strictly voluntary. Canada Post agreed to rescind any disciplinary actions and to pay employees for any days suspension they had served.

Partners' information common to all

Several complaints against Revenue Canada, Taxation required the office to examine difficult legal issues concerning the access rights of limited partnership members to tax information common to all members.

Members of a partnership wanted to appeal their individual tax assessments after Revenue Canada disallowed losses and investment tax credits claimed by the partnership in 1985. Thus, they applied to see information that included details of negotiations between the general (or managing) partner and Taxation.

Taxation claimed that releasing the information would injure the administration of the *Income Tax Act*. The department also invoked the tough confidentiality clauses in section 241 of that act which prevents release of tax information to anyone other than the individual taxpayer it concerns. These provisions, which make Taxation officials criminally liable for breaches of confidentiality, were considered to supersede the access right in the *Privacy Act*.

The applicants in this case received more information after the *Income Tax Act* was amended in 1988 to clarify what material an individual could receive to appeal a tax decision. However, the new release did not deal with information denied under the *Privacy Act*.

The partnership in question was established under the *Manitoba Partnership Act* which specifies that members may "inspect the books of the firm and examine... the state and progress of the partnership business". As well, members of a limited partnership have an individual relationship with Taxation and partners are individually responsible for paying their taxes. The information the members sought was personal about each of them but it was also common to all.

Taxation claimed that since the information concerned each member, it could not release it to any other member without the consent of all the others. The Commissioner maintained that since the information was personal and concerned each complainant, Taxation could not exempt it just because it was identical to information about all the other partners. He held that doing so would effectively deny each individual's right of access under the *Privacy Act*. He also asked Taxation to demonstrate the injury caused the *Income Tax Act* by providing access.

The Commissioner did agree with a number of exemptions which denied personal information that concerned only particular individuals, information supplied in confidence by a province and information exchanged by Taxation and its lawyers which is protected by solicitor-client privilege.

Following weeks of discussions, the department agreed that it could not demonstrate any injury to the *Income Tax Act*. It also agreed that the personal information which was common to each partner should be available to all.

As a result more than 2,000 pages of material were released.

**Origin of Completed
Complaints by Province and
Territory**

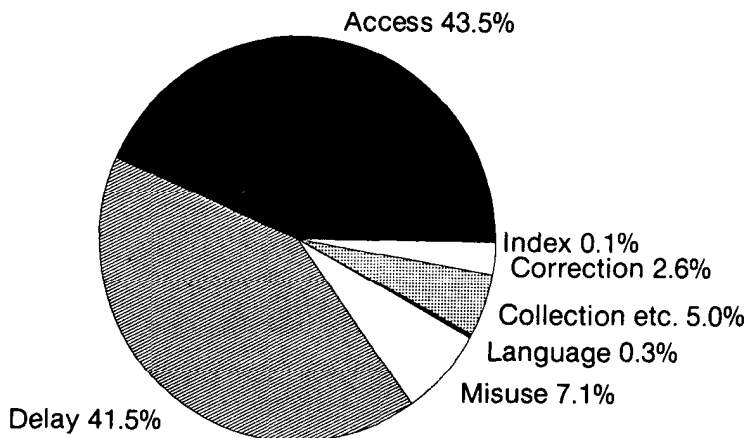
| | |
|------------------------------------|-------------|
| Newfoundland | 6 |
| Prince Edward Island | 7 |
| Nova Scotia | 57 |
| New Brunswick | 39 |
| Quebec | 147 |
| National Capital Region Quebec | 1 |
| National Capital Region Ontario | 102 |
| Ontario | 362 |
| Manitoba | 58 |
| Saskatchewan | 39 |
| Alberta | 80 |
| British Columbia | 113 |
| Northwest Territories | 2 |
| Yukon | 0 |
| Outside Canada | 2 |
| TOTAL | 1018 |

Completed complaints by department and result

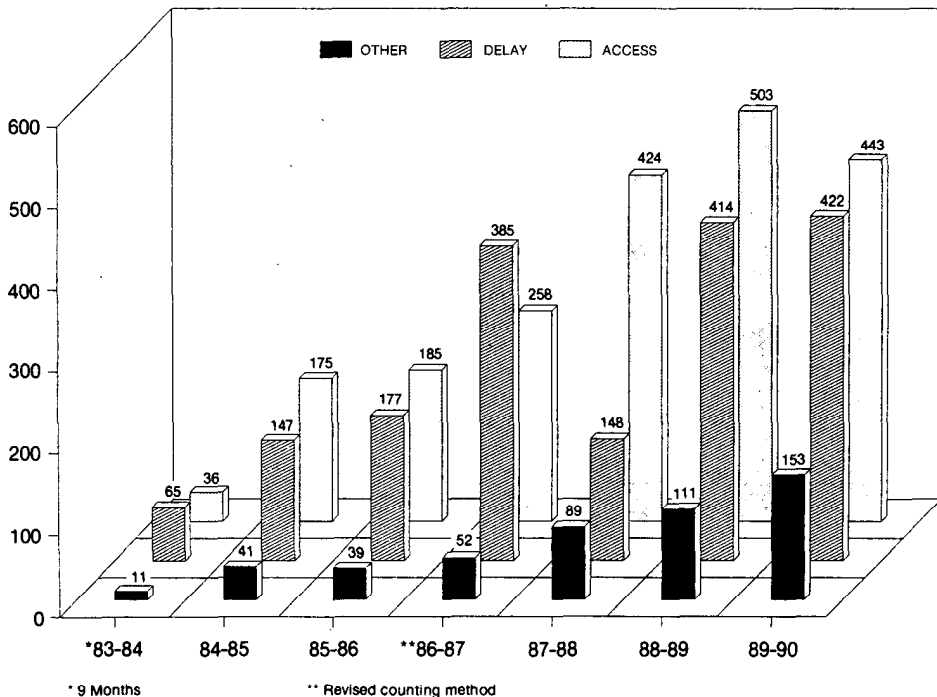
| Department | Total | Well- founded | Well- founded - Resolved | Not Well- founded | Dis- continued |
|---|-------|------------------|--------------------------------|-------------------------|-------------------|
| Agriculture Canada | 1 | 0 | 0 | 1 | 0 |
| Canada Mortgage and Housing Corporation | 1 | 0 | 1 | 0 | 0 |
| Canada Post Corporation | 61 | 21 | 9 | 30 | 1 |
| Canadian Aviation Safety Board | 1 | 0 | 1 | 0 | 0 |
| Canadian Human Rights Commission | 1 | 0 | 0 | 1 | 0 |
| Canadian Radio- television and Telecommunications Commission | 43 | 1 | 0 | 42 | 0 |
| Canadian Security Intelligence Service | 38 | 2 | 4 | 32 | 0 |
| Commissioner of Official Languages | 5 | 0 | 2 | 1 | 2 |
| Communications, Department of | 3 | 0 | 2 | 1 | 0 |
| Correctional Investigator | 1 | 1 | 0 | 0 | 0 |
| Correctional Service Canada | 395 | 188 | 59 | 122 | 26 |
| Employment and Immigration Canada | 53 | 13 | 18 | 17 | 5 |
| External Affairs Canada | 5 | 1 | 0 | 4 | 0 |
| Farm Credit Corporation | 1 | 0 | 1 | 0 | 0 |
| Health and Welfare Canada | 67 | 25 | 16 | 23 | 3 |
| Indian and Northern Affairs Canada | 10 | 0 | 0 | 10 | 0 |
| Justice | 7 | 1 | 3 | 3 | 0 |
| Labour Canada | 5 | 0 | 1 | 3 | 1 |
| Medical Research Council of Canada | 1 | 0 | 0 | 1 | 0 |

| Department | Total | Well-founded | Well-founded - Resolved | Not Well-founded | Discontinued |
|--------------------------------------|-------------|--------------|-------------------------|------------------|--------------|
| National Archives of Canada | 8 | 0 | 1 | 7 | 0 |
| National Capital Commission | 1 | 1 | 0 | 0 | 0 |
| National Defence | 117 | 74 | 14 | 25 | 4 |
| National Parole Board | 29 | 5 | 13 | 11 | 0 |
| Privy Council Office | 1 | 0 | 0 | 1 | 0 |
| Public Service Commission | 15 | 1 | 4 | 9 | 1 |
| Public Service Staff Relations Board | 1 | 0 | 0 | 1 | 0 |
| Public Works Canada | 3 | 1 | 2 | 0 | 0 |
| Revenue Canada - Customs and Excise | 7 | 2 | 3 | 2 | 0 |
| Revenue Canada - Taxation | 59 | 38 | 11 | 7 | 3 |
| Royal Canadian Mint | 1 | 1 | 0 | 0 | 0 |
| Royal Canadian Mounted Police | 47 | 4 | 6 | 35 | 2 |
| Secretary of State | 2 | 0 | 0 | 2 | 0 |
| Solicitor General Canada | 15 | 0 | 1 | 14 | 0 |
| Supply & Services Canada | 1 | 0 | 0 | 1 | 0 |
| Transport Canada | 7 | 4 | 2 | 0 | 1 |
| Veterans' Affairs Canada | 5 | 0 | 1 | 4 | 0 |
| TOTAL | 1018 | 384 | 175 | 410 | 49 |

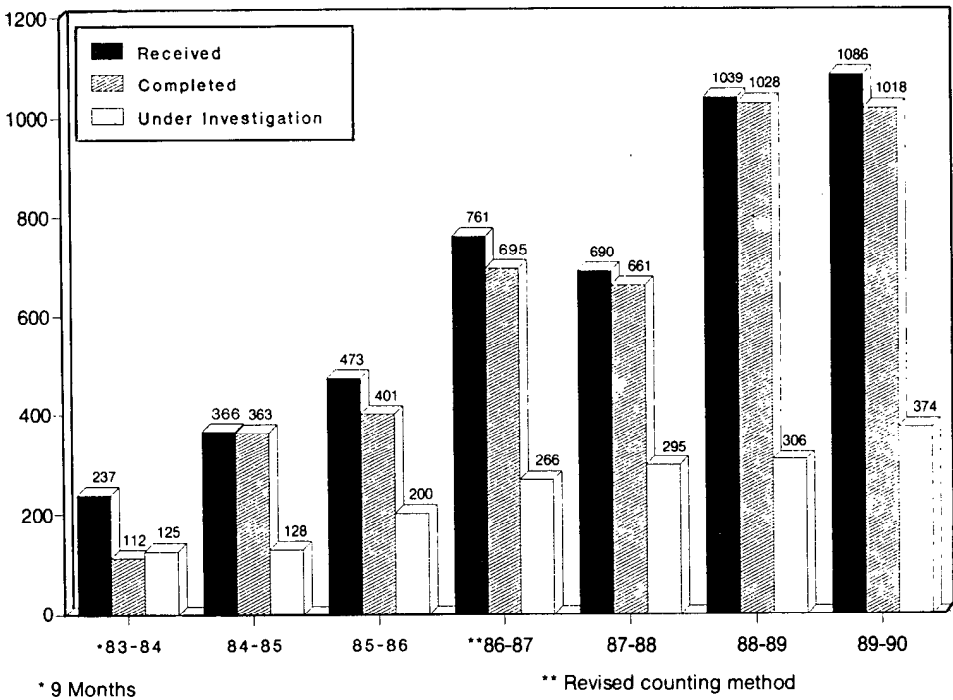
Complaints Completed By Grounds 1989-90



Completed Complaints and Grounds 1983-90



Completed Complaints 1983-90



Inquiries

Once again, the number of inquiries to the office took a substantial leap: 3447 compared to 2041 the previous year. The increase reflects real growth in workload (rather than just better recording which accounted for some of last year's increase). This growth will require the office to hire another staffer next year to help field the calls and letters.

A larger share of this year's inquiries dealt with understanding the *Privacy Act*—59 per cent compared with 46 per cent the previous year. Callers were concerned about employers' requests for medical information or identification documents such as marriage or birth certificates. In one instance, a caller had been asked for a complete list of his personal expenditures. Calls of this type sometimes evolve into complaints.

Public service union representatives were frequent callers on a variety of issues. One asked whether the union could demand a list of its members' actual salaries (rather than salary ranges which are public under the Act). The member wanted to confirm that the employer was remitting the correct dues. Staff suggested the union hire an independent auditor to confirm the accuracy of the information rather than seeking its release.

MP's called and wrote to refer their constituents' privacy concerns. One constituent was concerned about telephone surveys by Statistics Canada. The writer objected to answering personal questions over the telephone since he could not confirm the caller's identity. Statistics Canada is using the telephone increasingly to conduct surveys. However, it usually notifies in advance by letter or telephone those being surveyed and supplies a number for the person to call to confirm that the interviewer is genuine.

Calls about Social Insurance Numbers (SIN) dropped marginally to 19 per cent from 21 per cent a year earlier. Many callers continue to be concerned about the new reporting requirements in the amended *Income Tax Act*. One woman who had been exempted from using the number for religious reasons asked for the office's help because the amendments mean that she could be penalized by law for refusing to supply the number. Staff discovered that, contrary to American practice, no Canadian can be exempt from having a SIN, even on religious grounds.

Queries about organizations not covered by the *Privacy Act* increased to 16 from 15 per cent. Four per cent concerned federal agencies not subject to the Act and 12 per cent concerned organizations outside the federal government. For example, an Ontario government employee wanted to know if her agency could ask female staff whether they planned to become pregnant during the coming budgetary year. She was referred to the Ontario Privacy Commissioner. (A similar request by a federal agency would contravene the federal act.)

The number of misdirected applications remained fairly steady at seven per cent compared to eight per cent last year. The office forwarded these applications to the proper department. Six per cent of calls had nothing to do with the Commissioner's mandate and, whenever possible, were referred elsewhere.

The office's main switchboard (which is shared with the office of the Information Commissioner) redirected 8254 calls to Reference Canada offices across the country. The offices have revised their listings in the blue pages of telephone directories to better explain their mandates. But the combination of "information" in the title and a national toll-free line still prompts many totally unrelated (and expensive) calls.

Compliance Directorate

A seven-year retrospective

Since the *Privacy Act* came into effect on July 1, 1983, 27 government institutions have been audited for general compliance with the Act. In addition, the legitimacy of exempt personal information banks was audited in 11 institutions and more than 16 incidents of possible loss or theft of personal information have been investigated.

Ensuring compliance with the Act has meant breaking new ground with a unique new breed of professional—a hybrid of investigator, auditor, records manager and EDP specialist—the privacy auditor.

Compliance audit is an old and a new subject. What began as the essence of audit work, at the dawn of the 20th century evolved through operational audits, systems-based audits, value for money audits and the ubiquitous comprehensive audit.

However, the day-to-day tools of the traditional auditor cannot assess whether a department's information handling procedures comply with the law. This is so because traditional audit methodology and tools are oriented almost exclusively towards auditing volume and dollar value, not to determining compliance with a set of attributes.

Since the Act came into force, the tools and methodologies have been developed to assist in the audit of massive personal information banks to determine where to expend the scarce audit resources for the greatest good. Vehicles have been put in place to explore and assess the intricacies of the relationship of sections 7 and 8 of the Act as they relate to the security of information systems.

Where today's general auditor uses dollar-unit sampling techniques and utilities, the compliance auditor was left with locally developed questionnaires, a best-guess value for file sampling and a high level guide for the audit of compliance with the *Privacy Act*.

A first step in auditing for privacy meant determining that personal information is:

- *collected only when authorized by a specific program or activity;

- *kept as long as it serves its original purpose and long enough to allow the subject reasonable access;

- *used only for the purpose for which it was collected or for a consistent use;

- *disclosed to other parties only when permitted by the *Privacy Act*;

- *disposed of at the end of its useful life in accordance with National Archives standards;

- *protected according to the government security policy.

The object of the audit for compliance with the *Privacy Act* is to determine whether these six attributes have been accorded to the personal information held in the systems of those institutions subject to the Act. To make this determination requires the use of a tool to locate a statistically significant sample size from personal information banks which may hold as few as a couple of dozen records to as many as several million and then to identify the individual records for the auditor to review.

The first such automated program was developed, tried and field tested in the office of the Privacy Commissioner. It is used today in all audits conducted by the office and is a cornerstone in the methodology developed for use by Commission staff and those institutions which perform their own compliance audits. The program has been successfully employed to audit all types of holdings, from small manual information banks to massive automated relational data bases.

The second step was to develop an automated analytical matrix of criteria to determine the relative audit risk for all of the institutions subject to the Act. Using data derived from a profile questionnaire sent to all institutions in 1986, a computer based model was generated which permitted the Commissioner to assign audit projects based upon demonstrable criteria and not simply the best personal guess. Data for the model are now collected on an annual basis and upgrades allow it to change with the situations.

The third step was to develop and document the methodology so new staff could take advantage of the lessons learned and be consistent in working papers, reports and audit activities. Development of the methodology began early in the process and continues.

The latest step is to integrate the lessons learned and the tools developed with the task of auditing the latest generation of information handling systems and to review and evaluate the security implications of the new technology as it is applied to personal information.

The task is daunting but not without its success. The office has established new relationships with agencies responsible for policy and enforcement such as Treasury Board, the Communications Security Establishment and the RCMP—agencies with expertise in information policy and technology. As well, new colleagues are being found in provincial governments, private enterprise and associations of concerned professionals like the Canadian Information Processing Society, the Information Systems Security Association and the Institute of Internal Auditors.

Four major departments were examined in the first full year of application of new audit method and tools. The next year, six complete audits were done. The past year has witnessed the completion of 14 audits and five incident investigations. Future years will see a consolidation of effort in the largest of the institutions which possess the most sensitive personal information in the most advanced computer systems.

The major lesson to be learned from the Commissioner's auditing experience is that the name of the game is not "gotcha". It is a joint effort that will make privacy compliance a reality.

Without sharing experiences and knowledge and without participating in joint audits, the pursuit of compliance with the *Privacy Act* will remain a one-sided enforcement nightmare. True compliance will be achieved only when institutions, federal, provincial or private recognize the need for and benefits from a set of fair information practices.

During the year the unit audited the Canadian Cultural Properties Review Board, Canadian Patents and Development Limited, Export Development Corporation, Health and Welfare Canada (Medical Services Branch, Income Security Programs and Personnel Administration Branch), International Development Research Centre, Law Reform Commission of Canada, Public Service Staff Relations Board, Security Intelligence Review Committee, Social Sciences and Humanities Research Council and Supply and Services Canada.

What was found

Individual department audits reveal substantially the same weaknesses as those discussed in previous reports. Lack of awareness of the *Privacy Act* remains a major concern. Federal employees often do not know their privacy rights or those of their clients, nor are they aware of the impact the Act has on their day-to-day handling of personal information. The result could be inadequate protection and improper disclosure of clients' personal data. More resources for privacy training would reap dividends for individual departments and the government as a whole.

Personal information collections are often not accurately or completely described in the *Personal Information Index*, making it difficult—if not impossible—for applicants to know information exists or to find the appropriate bank to access. Occasionally personal information is not even recognized as a discrete collection and, therefore, it is not organized in a systematic enough way to attempt to describe.

Several of the institutions were not adhering to the retention and disposal schedules established for personal information after consultation with National Archives. This can lead to using inaccurate information (because it is out of date) or not having information available for access because it has been disposed of too early. It can also overcrowd the records room—but that is not a privacy problem.

Detailed personnel files are often available to supervisors or other employees who have no need to know details about the individual's charitable donations, family relationships, medical conditions, purchases of savings bonds and conflict-of-interest certification.

Inadequate security of personal information is another recurring refrain. Much of government's resources and attention have been put into providing proper security for information which is classified in the national interest (confidential, secret and top secret). Yet loss of, or unauthorized access to, personal information, while it may not damage the national interest, can have quite devastating effects on individuals. The use of FAX is a case in point. While encryption standards are in place and used for the transmission of information classified in the national interest, sensitive personal information is routinely transmitted without protection.

While recommendations to correct this problem may seem both picayune and costly to departments, the potential of this technology to compromise personal information is something this office takes seriously.

Other seemingly minor, yet potentially disastrous security lapses are also regularly uncovered—computer access codes which are never changed or taped to the display terminal, file cabinet keys left in open desk drawers, inadequate door locks, unsupervised access by cleaning staff, inadequate records kept of who has access to files, sensitive information disposed of in ordinary trash, and so forth. Some of the most common sense precautions most individuals take to protect their personal valuables at home seem to go unheeded in the handling of personal information in the federal workplace.

No institution which this office has audited (and among these must be counted the Commissioner's own office) has an unblemished record of privacy compliance. Neither can any department afford to wait for privacy auditors before carefully examining its information handling practices.

Yet there is an important positive side to the story. Departments have demonstrated a high level of sensitivity to and respect for the *Privacy Act*. No systemic or wilful breaches of the law have been uncovered. Shortcomings are quickly and willingly rectified. More and more departments are including privacy compliance as a regular part of regularly scheduled internal audits. While 27 audits from an audit population of some 150 institutions may not be an adequate basis for generalization, significant achievements should be acknowledged. The caveat is this—no one should rest on deserved laurels, privacy audits will continue!

Some incident investigations

Accident investigation reports restricted

The Commissioner's office pursued a newspaper report which claimed the Manitoba Public Insurance Corporation (MPIC) had used a Transport Canada accident report to deny compensation to a man injured in a traffic accident.

The *Winnipeg Free Press* described how compensation was denied because a Transport Canada research report which assigned him part of the blame had found its way into MPIC files. Police investigating the accident had found the other vehicle at fault.

Compliance staff determined that the report was part of an ongoing study on fatal traffic accidents done for Transport Canada by local universities. The study analyzes accidents to determine the contributing factors and to measure the effectiveness of a number of new safety devices now required on cars. The reports were never designed to replace, or supplement, local police investigations.

Prior to 1978, the lengthy reports contained substantial personal information which a knowledgeable person could link to a specific event. These reports were available in government libraries. In the case in question, it appeared that a local police officer, alleged to have been related to the victims, had given the report to the insurance corporation.

Though the incident happened before the *Privacy Act* came into force, it focused the office's attention on the

availability and use of the reports. The privacy investigation found that the new reports are shorter, contain few personal details and are transferred electronically to national accident files.

Privacy staff reviewed the storage methods of both old and new reports and made a number of recommendations to ensure the privacy of those involved in the accidents. Transport Canada readily agreed to new controls which will limit access to the data and ensure that it is used only for research purposes.

Trade Marks Act prevails

A caller told a privacy investigator that approximately 20,000 "protected" files (the security designation for personal information) were kept in an open office in the commercial lobby of a Hull government office.

When investigators visited the area, occupied by the Trade Mark Registry Office of Consumer and Corporate Affairs (CCA), they found names and addresses of those applying for a registered trade mark. The Act requires that this information be protected.

CCA staff pointed to the *Trade Marks Act* which states clearly that the information "shall be open to public inspection". Since the *Privacy Act* protects personal information against disclosure "subject to any other Act of Parliament", the open storage of the files did not breach the Act. Nevertheless, the investigators identified other physical security problems which were noted by CCA privacy staff. These problems are being corrected.

Corporate Management

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

Finance

A new computerized budget control system was introduced to improve the control and reporting of financial commitments and expenditures.

The Offices' total resources for the 1989-90 fiscal year were \$5,856,000 and 75 person-years, an increase of \$765,000 and six person-years over 1988-89. Personnel costs of \$4,481,351 and professional and special services expenditures of \$715,783 accounted for more than 90 per cent of expenditures. The remaining \$560,135 covered all other expenses.

The following are the Offices' expenditures for the period April 1, 1989 to March 31, 1990*

| | Information | Privacy | Corporate Management | Total |
|--|--------------------|------------------|----------------------|------------------|
| Salaries | 1,585,156 | 1,794,669 | 505,526 | 3,885,351 |
| Employee Benefit Plan Contributions | 243,000 | 274,000 | 79,000 | 596,000 |
| Transportation and Communication | 36,925 | 86,040 | 130,663 | 253,628 |
| Information | 25,133 | 36,699 | 2,394 | 64,226 |
| Professional and Special Services | 595,374 | 68,916 | 51,493 | 715,783 |
| Rentals | — | 2,381 | 10,588 | 12,969 |
| Purchased Repair and Maintenance | 2,185 | 14,271 | 4,256 | 20,712 |
| Utilities, Materials and Supplies | 16,064 | 14,330 | 37,974 | 68,368 |
| Acquisition of Machinery and Equipment | 31,562 | 38,933 | 62,031 | 132,526 |
| Other Payments | 1,474 | 3,521 | 2,711 | 7,706 |
| TOTAL | \$2,536,873 | 2,333,760 | 886,636 | 5,757,269 |

*Expenditure figures do not incorporate final year-end adjustments reflected in the Office's 1989-90 Public Accounts.

Personnel

With a net increase of six person-years in 1989-90, the first time appointment of an Assistant Privacy Commissioner and the end of term for an Assistant Information Commissioner, the personnel program was active this year again. Thirty-eight staffing actions, including the appointment of one senior management position, were processed and a review of all Program Management positions was conducted to apply the new classification standards. The offices also underwent a staffing audit by the Public Service Commission.

Administration

Additional office space was obtained to accommodate the growth of the organization as well as anticipated needs.

Informatics

A local area network was implemented in the Privacy Commissioner's office to facilitate expansion of report and text production. Preliminary work has also been undertaken to address major changes to the dated case management system. A requirement study of the Information Commissioner's case management system was undertaken.

The office has also started a new informatics management infrastructure to meet the growing needs of the organization.

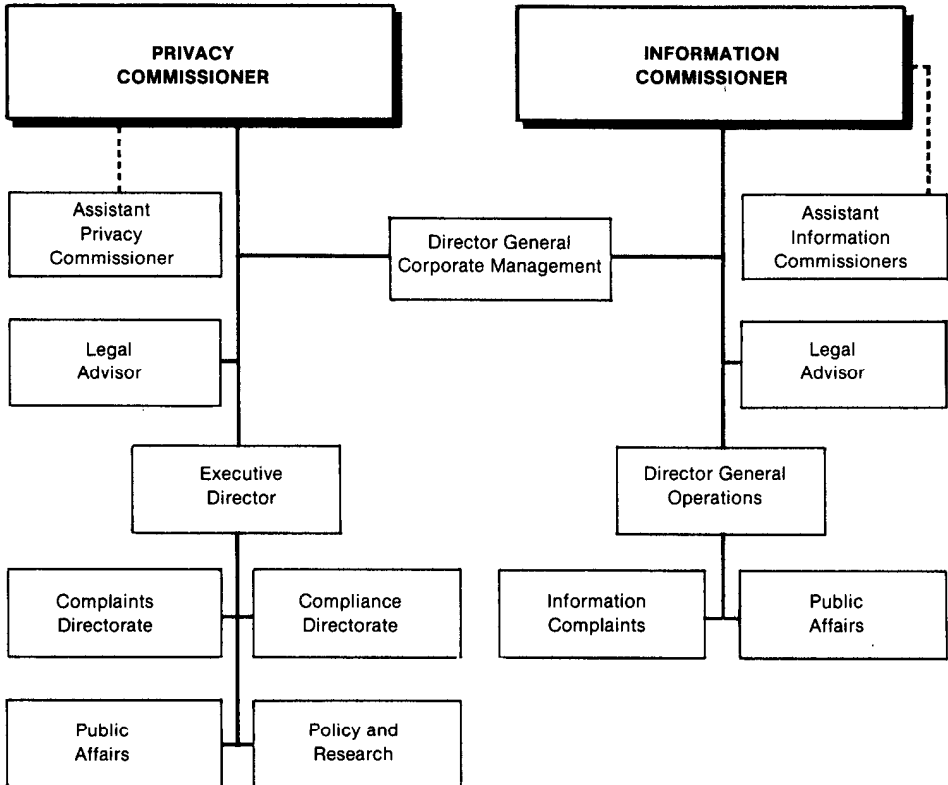
Library

The library supports the programs of both the Information and Privacy Commissioners. It is open to the public.

Among the services offered are the provision of interlibrary loans, manual and automated reference and research, and the maintenance of newspaper clipping files. The library acquires and retains national and international material on all aspects of freedom of information, the right to privacy, data protection and the ombudsman function. Comprehensive collections of annual reports on the administration of the Acts and ombudsman annual reports are also kept.

Automation of library functions is ongoing. Cataloguing of our library collection enables us to provide efficient, quick production of subject bibliographies, lists of periodicals received, and circulation statistics.

Appendix I



Appendix II

Government Institutions Covered by the Act

| | |
|--|--|
| Advisory Council on the Status of Women | Canada Ports Corporation |
| Agricultural Products Board | Canada Post Corporation |
| Agricultural Stabilization Board | Canadian Aviation Safety Board |
| Agriculture Canada | Canadian Centre for Occupational Health and Safety |
| Atlantic Canada Opportunities Agency | Canadian Commercial Corporation |
| Atlantic Pilotage Authority | Canadian Cultural Property Export Review Board |
| Atomic Energy Control Board | Canadian Dairy Commission |
| Bank of Canada | Canadian Film Development Corporation (includes Telefilm Canada) |
| Board of Trustees of the Queen Elizabeth II Canadian Fund to Aid in Research on the Diseases of Children | Canadian General Standards Board |
| Bureau of Pension Advocates | Canadian Grain Commission |
| Canada Council | Canadian Human Rights Commission |
| Canada Deposit Insurance Corporation | Canadian Institute for International Peace and Security |
| Canada Employment and Immigration Commission | Canadian International Development Agency |
| Canada Labour Relations Board | Canadian International Trade Tribunal |
| Canada Lands Company Limited | Canadian Livestock Feed Board |
| Canada Mortgage and Housing Corporation | Canadian Museum of Civilization |
| Canada-Newfoundland Offshore Petroleum Board | Canadian Patents and Development Limited |
| Canada Nova Scotia Offshore Petroleum Board | Canadian Pension Commission |
| | Canadian Radio-television and Telecommunications Commission |
| | Canadian Saltfish Corporation |

| | |
|--|--|
| Canadian Security Intelligence Service | Fisheries Prices Support Board |
| Canadian War Museum | Freshwater Fish Marketing Corporation |
| The Canadian Wheat Board | Grain Transportation Agency Administrator, Office of |
| Communications, Department of | Great Lakes Pilotage Authority, Ltd. |
| Consumer and Corporate Affairs Canada | Hazardous Materials Information Review Commission |
| Correctional Service Canada | Health and Welfare Canada |
| Defence Construction (1951) Limited | Historic Sites and Monuments Board of Canada |
| The Director of Soldier Settlement | Immigration and Refugee Board |
| The Director, The Veterans' Land Act | Indian and Northern Affairs Canada |
| Economic Council of Canada | Industry, Science and Technology Canada |
| Employment and Immigration Canada | International Development Research Centre |
| Energy, Mines and Resources Canada | Investment Canada |
| Energy Supplies Allocation Board | Jacques Cartier and Champlain Bridges Incorporated |
| Environment Canada | Justice Canada |
| Export Development Corporation | Labour Canada |
| External Affairs Canada | Laurentian Pilotage Authority |
| Farm Credit Corporation | Law Reform Commission of Canada |
| Federal Business Development Bank | Medical Research Council |
| Federal Mortgage Exchange Corporation | Merchant Seamen Compensation Board |
| Federal-Provincial Relations Office | National Archives of Canada |
| Finance, Department of | National Arts Centre Corporation |
| Fisheries and Oceans Canada | |
| Fisheries and Oceans Research Advisory Council | |

| | |
|---|---|
| National Aviation Museum | Office of the Auditor General |
| The National Battlefields Commission | Office of the Chief Electoral Officer |
| National Capital Commission | Office of the Commissioner of Official Languages |
| National Defence | Office of the Comptroller General |
| National Design Council | Office of the Coordinator, Status of Women |
| National Energy Board | Office of the Correctional Investigator |
| National Farm Products Marketing Council | Office of the Custodian of Enemy Property |
| National Film Board | Office of the Director of Investigation and Research |
| National Gallery of Canada | Office of the Inspector General of the Canadian Security Intelligence Service |
| National Library | Office of the Superintendent of Financial Institutions Canada |
| National Museum of Natural Sciences | Pacific Pilotage Authority |
| National Museum of Science and Technology | Pension Appeals Board |
| National Parole Board | Petroleum Compensation Board |
| National Parole Service | Petroleum Monitoring Agency |
| National Postal Museum | Prairie Farm Rehabilitation Administration |
| National Research Council of Canada | Privatization and Regulatory Affairs |
| National Transportation Agency (formerly Canadian Transport Commission) | Privy Council Office |
| Natural Sciences and Engineering Research Council | Public Service Commission |
| Northern Canada Power Commission | Public Service Staff Relations Board |
| Northern Pipeline Agency | Public Works Canada |
| Northwest Territories Water Board | Regional Development Incentives Board |

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