Privacy Commissioner

Annual Report 1990-1991

Annual Report
Privacy Commissioner
1990-91

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

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

Cat. No. IP30-1/1991

ISBN 0-662-58483-X

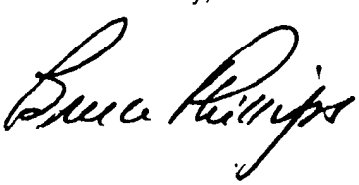
The Honourable Guy Charbonneau
The Speaker
The Senate
Ottawa

June 28, 1991

Dear Mr. Charbonneau:

I have the honour to submit to Parliament my annual report. This report covers the period from April 1, 1990 to March 31, 1991.

Yours sincerely,



Bruce Phillips
Privacy Commissioner

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

June 28, 1991

Dear Mr. Fraser:

I have the honour to submit to Parliament my annual report. This report covers the period from April 1, 1990 to March 31, 1991.

Yours sincerely,

Bruce Phillips
Privacy Commissioner

Table of Contents

Mandate 1

New conductor, familiar score 2

Privacy and the Charter 8

Cellular phones and privacy 13

Privacy in the private sector 15

Biomedical testing 18

Electoral reform—a permanent voters' list 22

Privacy and the public interest: a difficult balance 24

Complaints directorate 26
- Directorate report 26
- Tables and charts 30
- Cases 35
- Notifying the Commissioner 44
- Policy and research 47
  - Data matching 47
  - Technology marches on 52
  - Consulting the Commissioner 54
- Inquiries 55

Compliance directorate 57

Corporate management 61

Organization chart 63

Mandate

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

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

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

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 **Info Source** description of the contents of the information bank is deficient in some way;
- the department's listing in the Source does not describe all the uses it makes of personal information;
- an institution is collecting, keeping, using or disposing of personal information in a way which contravenes the *Privacy Act.*

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

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

New Conductor, Familiar Score

This is the first annual report to Parliament in eight years to be submitted by anyone other than John Grace who, until June, 1990, was the sole person to have served as Privacy Commissioner of Canada since the office was established as a function separate from the Canadian Human Rights Commission in 1983.

Mr. Grace completed his term of office in July of 1990 and assumed new duties as Canada's Information Commissioner. He departed this office with a high reputation in several respects: first, as an ombudsman with an outstanding gift for resolving privacy problems and complaints; second, as an energetic and eloquent spokesman for the cause of protection of personal privacy, and third, as the respected leader of a small but highly-motivated staff of skilled investigators and auditors who reflected his abiding concern for this vital but embattled area of human rights.

He also was ever alert to the new challenges to privacy protection which continue to arise with almost bewildering rapidity and number in a constantly-changing commercial and technological environment.

Thus Mr. Grace has bequeathed to his successor the advantage of a smoothly-functioning organization. Many of the issues touched upon in this report were initiated prior to Mr. Grace's departure.

During the interval between the departure of the former commissioner and the confirmation of a new one, a period of some ten months, the duties of acting commissioner were performed by the executive director, Alan Leadbeater. He served with distinction in the difficult dual role of both administrative head and ombudsman.

The new commissioner, coming into office almost on the eve of this report, is acting in some senses as a surrogate spokesperson for two predecessors, although he was, as assistant commissioner, the beneficiary of their experienced counsel and guidance. In fact, the ten months expended as assistant commissioner proved to be an invaluable introductory exposure to a field which is both complex and becoming more so. If the reader detects any diffidence in the tone of the observations, be assured it is attributable to the realization that the author still has much to learn.

It may be small comfort to this neophyte that he is not alone. In fact, the privacy guard also changed in Ontario and Quebec during the year. Paul-André Comeau was appointed Quebec's new Access and Privacy Commissioner and Thomas Wright was named Information and Privacy Commissioner of Ontario. One thing should not change—the cordial and mutually supportive relationship among these offices.

This report, in attempting to give a reading on the state of privacy protection in the nation, will share with its predecessors something of the quality of a "good news-bad news" story. It is the nature of the issue that there will be no final victories. Personal privacy is a problem intimately bound up with the relationship of the individual to society, and so long as society continues to evolve and change, so too will the problems affecting privacy.

There is no more fragile, yet important, right in today's complex society than the right to a reasonable expectation of privacy. It is not a right, which some cynics suggest, that only serves those with something to hide. Without a meaningful measure of privacy our fundamental freedoms of expression, belief and association risk becoming meaningless.

Justice Brandeis, in his famous 1898 definition of privacy as "the right to be let alone", could not have contemplated a world of ingenious machines with unlimited capacity for collecting, collating and transmitting information across global networks. Nor could he have foreseen a science capable of plumbing the deepest secrets of human heredity.

The right to be left entirely alone, if it ever existed, could now be exercised, if at all, only, in the farthest corner of the most remote reaches of our arctic. Even then, one suspects, the putative recluse would sooner or later see some indomitable servant of a government department looming over the frozen horizon bearing the all-important form which, when properly filled out, would confer that indisputable certification of human existence, a Social Insurance Number.

But if absolute privacy in modern society is neither attainable, practical nor even particularly desirable, the struggle must continue to preserve the individual's right to decide the degree to which personal privacy is to be sacrificed on behalf of other competing rights and claims.

So the notion of an annual fever-chart, while it provides a convenient method of keeping score, is to a certain extent misleading unless it is clearly understood that, where privacy is concerned, the patient will always be in danger since it is under assault from new afflictions as rapidly as remedies for older ones are found.

One is struck by this phenomenon in reading past annual reports. Many of the issues which dominate privacy discussions today were barely in the privacy vocabulary eight short years ago. For example there is drug testing, AIDS testing, and implications of genetic research, interception of cellular telephone communications, to name but a few, and some of which will be referred to later in this report. Doubtless this will continue to be the experience in future, since there is no reason to believe there will be any relaxation in the onward march of science and technology. The best one can do is to stand firmly on the privacy ramparts, trying to dam the breaches as they occur, and confident of nothing except that it will be a never-ending struggle.

So how did the struggle proceed in the year just past?

Certainly there is no reason on the available evidence to suppose there has been any abatement in the technological onslaught against personal privacy. Computers continue to proliferate (80,000 in the possession of the federal government alone, at last estimate), the tide of junk mail continues to mount, the commercial trafficking in personal information continues to increase (a $3 billion annual business in the U.S., and, presumably, on the usual proportion, at least $300 million in Canada).

But, on the proposition that an aroused and informed public is the best bulwark of privacy rights, there are very positive signs of real and lasting gains.

In the marketplace

Past reports have referred to the growing awareness of invasive marketing practices in the private sector. In 1990, the issue received the final accolade of media stardom—a TIME Magazine cover story. And although some of the participants might have wished otherwise, further proof of the rising profile of privacy issues emerged in the political arena in two provinces where ministers found themselves in difficulties over disclosures which, in two cases at least, led to a resignation. Whatever else one might think or say about them, these events underline that privacy rights cannot always be ignored with impunity. And, if the marketplace in recent years has generated some of the major threats to privacy, the marketplace acting in self-interest in the end may also prove to be at least partly a self-correcting mechanism.

Presumably in response to growing consumer concern, the private sector is showing (at long last, some might say) encouraging signs of action. During the past year, the Canadian Bankers Association, Bell Canada and the Canadian Direct Marketing Association have all produced codes offering significant improvements in the protection for privacy and confidentiality of information concerning their clients. These developments are discussed in more detail later in the report, but here it is worth noting that they offer some hope yet for the path of voluntary action.

The issue now is not whether the private sector can continue without privacy codes, but how long it will be before compulsion in one form or another enters the equation. Thanks to developments in Europe, North American business may soon lose its ability to engage in data transfers with European business unless it has privacy codes in place. This development lends added urgency to the Commissioner's recommendation to Parliament last year that the *Privacy Act* be amended to require all federally-regulated private sector firms to implement privacy codes based on internationally-accepted guidelines and principles.

Even assuming such voluntary codes become a feature of the Canadian marketplace, there remains a question about their effectiveness. Highly-respected authorities believe some form of oversight is necessary before business becomes truly accountable to the public for protecting privacy.

Dr. David Flaherty, the leading Canadian academic in the field of privacy research, argues that a federal audit power is required to ensure private sector compliance with its own voluntary codes. His is a view which must be respected, yet the Commissioner continues to hope (as did his predecessor) that such a degree of intervention (with the massive resources it implies) may be forestalled by the private sector demonstrating some good privacy citizenship.

Certainly there remains a long way to go. Citing one small example, some chartered banks in their credit card applications still include in the fine print virtual absolute waivers of the privacy rights of customers. These waivers confer upon the banks the right to re-use, in any way they see fit, any or all of the information provided, such as salary, employment history, personal assets and in one case, the Social Insurance Number. A few sharp-eyed consumers have noted these waivers and drawn them to the attention of this office but most, we suspect, did not notice. Such fine-print caveats do not meet any reasonable definition of "informed consent". Neither do they reflect the spirit of enhanced respect for privacy to which the chartered banks' own association now lays claim.

On the positive side, the Canadian Direct Marketing Association is commended for providing a process by which consumers may have their names removed from the mailing lists of their members. Since the association covers more than 80 per cent of the firms engaged in direct marketing, this is a forward step.

Still, such modest improvements are in no way keeping pace with the exploding volume of information exchange made possible by the computer. Thus a minimum step to imposing some standards on the trade in personal information should be the introduction of a legislated requirement that all business under federal jurisdiction implement approved privacy codes. The Commissioner considers this urgent.

Also needed is for Parliament to restore privacy to telephone communications in Canada, now eroding with the spread of cellular telephones. Cellular communications can and are being intercepted by easily available monitoring equipment. There seems no reason why the absence of conventional wires should deprive customers of the right and expectation of privacy. Sale or possession of monitoring equipment should be limited to authorized organizations for use only in conformity with laws governing surveillance activities.

Appraising the manager

Readers of last year's report may recall the Commissioner's cool reception of a proposed hotline for anonymous tips from public servants about government fraud, waste and mismanagement. Happily the idea was dropped.

But many of the same privacy problems are inherent in a new management tool departments are taking up with enthusiasm—"reverse" or "upward" appraisals. As the terms imply, the process allows employees to evaluate their managers' performance anonymously. Although it has been used by large private sector corporations, this is a novelty for government agencies which, as part of public service reform, now design their own appraisal systems.

The process requires employees to complete a questionnaire, rating managers on their management skills and personal traits. The completed forms then are analyzed, sometimes by a private consultant, and summarized. Managers receive a copy but do not see individual employees' ratings or comments.

There are several privacy problems in the process—first is promising employees confidentiality to prevent reprisals. The *Privacy Act* gives individuals the right to see what others say or write about them. And so promising confidentiality to employees who complete the appraisals is misleading and hollow.

In contrast, it is firmly established public service practice for employees to review, comment on and even (if they wish) appeal managers' appraisals of their performance.

Second, the notion that privacy rights can be sidestepped by contracting out the process is dangerous and unsupportable. To accept such a view would mean that all government privacy objectives could be foresworn by turning personal information over to private contractors. The implications go well beyond concern that managers would lose their right of access and that the Act would not protect this highly personal information from improper use or disclosure. However, once hired, contractors are agents of the government and it retains "control" of the information, wherever it happens to be stored.

Few would argue with government's aim to improve management and accountability. But establishing a process which subverts its own legislation is hardly the proper weapon.

A year at the office

As it has in almost every year since the office was established, the number of complaints, investigations, and audits has increased. Although the details are compiled in separate chapters elsewhere in this report, the office is now working at full stretch and, general restraint notwithstanding, Honorable Members and Senators must understand that the obligations they have laid on the office under the *Privacy Act* can not be discharged at their present level of efficiency by the existing modest staff of 34 persons. Investigations now number more than 1,200 a year, exceeding 100 per investigator. Any significant increase in this workload, which experience suggests is inevitable, simply cannot occur without sacrificing existing standards of service.

The compliance branch also had a busy year, but it is worth noting that after eight years of operation, it has managed audits in only about one-fifth of the 150 federal departments and agencies covered by the *Privacy Act*. Clearly, if the reach of the Act is ever extended to include audit responsibilities in the private sector, the existing compliance branch of nine persons will be unequal to the task.

On the research side, the major effort of the office during the previous year was a study of the privacy implications of drug testing. The study found that mandatory random drug-testing in the workplace was unjustified, and in some circumstances, probably illegal. The office notes with approval that the Department of Transport has modified to some extent its drug-testing plans, but disapproves of the Department of National Defence and at least one chartered bank going forward with drug-testing programs which constitute unwarranted breaches of personal privacy. This issue is discussed in greater detail in a separate chapter.

Now in the final stages of preparation is a study on the implications of progress in genetic research and testing, a subject which holds the promise of even greater privacy problems than drug-testing. The report is expected to be published in late summer of 1991.

Privacy and the Charter

It is both fascinating and gratifying for a Privacy Commissioner to watch the Supreme Court of Canada fashion a prominent place for the right to privacy within the *Canadian Charter of Rights and Freedoms.* It is fascinating for the ups and downs of the saga — and gratifying for the overall growing strength of the right to privacy.

Two previous annual reports followed this unfolding study. There is more to tell this year.

On September 11, 1983, police seized 278 pounds of marijuana from a vehicle and charged a number of individuals with conspiracy to import an illegal substance. The Crown's case was based on 136 phone calls intercepted during an intensive investigation in widely separated areas of British Columbia.

The police believed that the alleged conspirators used public pay telephones to conduct their affairs and so they installed listening devices on 20 public pay phones. Tape recorders were attached to pay phones on some 20 occasions and left on automatic record overnight, intercepting and recording conversations of suspects and others. While the police obtained judicial authorizations for these wiretaps, none of the authorizations specifically allowed the bugging of pay phones. Rather, the authorizations employed a "basket clause" giving police the authority to intercept communications at certain addresses and "...elsewhere in the Province of British Columbia resorted to by (the suspects)...".

The trial judge ruled that, in these circumstances, the judicial authorizations were invalid. In his view, the automatic monitoring of public pay phones when such monitoring is not specifically authorized by a judge, permits a dragnet type of investigation not contemplated by the *Criminal Code* He ruled the intercepted communication inadmissible and directed the jury to acquit the accused.

The B.C. Court of Appeal saw it differently, reversed the trial judge's decision and ordered a new trial. The Court of Appeal concluded that it was not necessary for the authorization to make specific reference to pay phones as long as any monitoring of pay phones was not indiscriminate. The Court of Appeal found that an intercepted communication itself could (by containing a suspect's voice) provide evidence that the monitoring was not indiscriminate.

The Supreme Court of Canada resolved the matter in a 4-2 decision, *Thompson, et al* v. *The Queen,* issued October 18, 1990. The Supreme Court conclusion is most interesting, if puzzling.

Writing for the majority, Justice Sopinka concluded that the "basket clause" authorization was lawful even though no mention was made of public pay phones nor were any limiting conditions imposed to protect the public. However, he wondered whether the interceptions which took place in this case pursuant to the valid authorizations were "reasonable" under section 8 of the *Charter.*

He concluded that in at least four instances, taps were placed on public pay phones solely because they were near where a suspect was staying and that this was insufficient evidence to act upon, "...(it) amounts to little more than indiscriminate monitoring based on a hunch" (p. 26). Furthermore, since this jeopardized the right to privacy of innocent third parties (hundreds of private conversations may have been intercepted when not one target was involved), Justice Sopinka concluded that it infringed upon section 8 of the *Charter.*

Now the puzzling part. Justice Sopinka reasoned that it would not bring the administration of justice into disrepute to admit the evidence obtained from wiretapped public pay phones. Consequently, the appeal was dismissed and a new trial ordered.

What comfort does this give us? Strong admonitions are made against relying on the "basket clauses" in wiretap authorizations. Judges and the police are strongly encouraged by the Court to minimize the intrusions upon the privacy of innocent third parties when seeking or granting wiretap authorizations and when intercepting communications. Yet, the law enforcement community is essentially told that if it fails to live up to these standards, no matter — their cases will not be jeopardized.

The dissenting opinions of Justice La Forest and Justice Wilson point out the shortcomings in the thinking of the majority. Both said that since the tapping of public pay phones give rise, *per se*, to massive violations of privacy, judicial authorizations for such activity must be expressly made and not granted by implication under the "resort to" basket clause. By not taking this view, the Supreme Court has left it to Parliament to ensure that *Charter* infringements are not perpetrated by the police. How completely the respective roles of the *Charter* and Parliament have been turned. Justice La Forest puts it eloquently:

> "It will be obvious that the Act (*Criminal Code*) and the *Charter* place a heavy burden on the courts to ensure the privacy of Canadians. Electronic surveillance is indiscriminately acquisitive; its reach extends to the conversations of the innocent and the guilty alike. The indiscriminate acquisitiveness of electronic surveillance invites the courts to redouble their vigilance and to be especially sensitive of the potential of certain practices to undermine the expectation of Canadians that their private communications are inviolable. This legitimate and reasonable expectation of privacy will not long survive if the courts give their *imprimatur* to practices that allow the police to intercept private communications solely on the basis of their own reasonable belief that valuable evidence stands to be gained thereby. In my view, 'resorted to' clauses can easily result in the application of this low threshold and constitute the 'fishing expeditions of considerable latitude' decried by this

court in *Hunter* v. *Southam*, *supra,* at p. 167. It is sad to reflect that, even with the assistance of the *Charter*, the courts have failed to take the steps necessary to avoid this danger and that if Canadians are to receive adequate protection against the insidious threat to individual privacy posed by electronic surveillance, they must turn to Parliament to provide additional safeguards. There is biting irony in this. The *Charter* was designed to protect us from possible inroads on individual rights by Parliament". (pp. 13-14)

And so, a Privacy Commissioner, at best, has mixed emotions about the *Thompson* decision. We must applaud the Court's new insistence that, when police intercept private communications, the privacy rights of innocent third parties must be protected. There is a strong message to judges and the police to be especially vigilant when wiretaps are installed at places frequented by the public. Although the Court does not make it a mandatory requirement, it suggests that visual surveillance accompany the wiretap to ensure that only a suspect's conversations are intercepted. Canadians should be comforted by the Supreme Court's consciousness of privacy threats to innocent parties when police engage in wiretapping. Nevertheless, the Court also makes it clear that if Canadians are to be adequately protected against these abuses, Parliament must act to strengthen the wiretap provisions of the *Criminal Code.*

Therefore, the Privacy Commissioner urges the government to propose, and Parliament to enact, measures necessary to ensure adequate control of wiretapping practices.

This year's Supreme Court privacy story, however, does not end with a whimper. Its decision in the case of *Santiago Wong* v. *The Queen* (November 22, 1990) is a bang.

The *Wong* case resulted from a Toronto police gambling investigation conducted during the summer of 1984. The security staff of a major downtown hotel told police they suspected that hotel premises were being used for illegal gambling. There was evidence of gambling in a recently vacated hotel room and the police learned that the person who had reserved the room, Mr. Wong, had also reserved it for later the same month.

The police installed a video camera in the room with the permission of the hotel management but without judicial authorization or warrant. Activities in the room were monitored on five separate occasions and resulted in charges being laid against Mr. Wong and ten others for keeping a common gaming house.

The trial judge found that the video surveillance was an infringement of section 8 of the *Charter* and dismissed all charges. The Ontario Court of Appeal, however, noted that invitations had been widely circulated within the Chinese community and that strangers who came to the hotel room were welcomed. In these circumstances, the court found that the accused had no reasonable expectation of privacy and that, as a result, section 8 of the *Charter* did not apply. A new trial was ordered.

On appeal the Supreme Court, in a 6-1 decision, took a different view. It concluded that without judicial authorization, such video surveillance was an infringement of the section 8 protection against unreasonable search and seizure. This decision is especially remarkable because it extends the privacy right to a right to freedom from indiscriminate video surveillance by agents of the state. The Court concluded that this privacy right must be protected by an independent judiciary and that police cannot be left to decide when video surveillance may be employed.

In his majority judgment, Justice La Forest is clear that all forms of electronic surveillance by agencies of the state, not judicially authorized, violate section 8 of the *Charter*.

> "...the broad and general right to be secure from unreasonable search and seizure guaranteed by s. 8 is meant to keep pace with technological development, and, accordingly, to ensure that we are ever protected against unauthorized intrusions upon our privacy by agents of the state, whatever technical forms the means of invasion may take." (p. 6)

As a result of *Wong*, it is no longer appropriate for a court to inquire into whether a person who is the subject of unauthorized surveillance has "courted the risk".

In Justice La Forest's words:

> "...privacy would be inadequately protected if an assessment of the reasonableness of a given expectation of privacy were made to rest on a consideration whether the person concerned had courted the risk of electronic surveillance. In view of the advanced state of surveillance technology, this would be to adopt a meaningless standard, for, in the final analysis, the technical resources which agents of the state have at their disposal ensure that we now run the risk of having our words recorded virtually every time we speak to another human being." (p. 7)

Thus, despite the fact that the accused had widely issued invitations to his hotel room and opened the door to strangers, he did not lose his right to a reasonable expectation of privacy. The Court made it clear that while we might impose warrantless video surveillance on those who engage in illegal activities in their hotel rooms, society would object to imposing that risk on anyone who rents rooms. In order to avoid the latter, the Court considered that it must prohibit the former.

Unlike wiretapping, there is currently no available procedure for police to obtain a judicial authorization for video surveillance. The Court was fully aware of the handicap its decision imposed upon the police, but felt that only Parliament should decide the circumstances in which the police could invade privacy by means of video surveillance.

In Justice La Forest's words:

> "On my view of the matter the courts would be forgetting their role as guardians of our fundamental liberties if they were to usurp the role of Parliament and purport to give their sanction to video surveillance by adopting for that purpose a code of procedure dealing with an altogether different surveillance technology. It is for Parliament, and Parliament alone, to set out the conditions under which law enforcement agencies may employ video surveillance technology in their fight against crime. Moreover, the same holds true for any other technology which the progress of science places at the disposal of the state in the years to come." (p. 22)

No doubt the government will introduce legislation to provide for the judicial authorization of video surveillance by the police. That would be the responsible course since no one questions the need for video surveillance in law enforcement. However, as with wiretapping, the Privacy Commissioner urges Parliament to ensure that any process for obtaining judicial authorization for video surveillance protects the privacy of innocent parties.

Cellular Phones and Privacy

In the past year Canadians have become aware—some painfully so—that cellular telephone calls can be intercepted.

One British Columbia cabinet minister resigned after a newspaper printed extracts from calls he made on his car phone. Some provincial delegations at the Meech Lake Conference suspected that their cellular communications had been intercepted. And a provincial power corporation was embarrassed when someone intercepted and published an employee's comments about third parties during a cellular phone conversation.

Faced with this troubling new threat to privacy, the Commissioner has tackled two questions:

- Does the *Privacy Act* protect cellular phone calls?
- And do federal government institutions, including its law enforcement agencies, only intercept cellular communications in compliance with the law?

The Supreme Court decisions (discussed above) make it clear that, without proper judicial authorization, agencies of the state may not subject individuals to any form of electronic surveillance. To do so would be "improper search and seizure". It would sacrifice our right to a reasonable expectation of privacy, thus infringing section 8 of the *Charter of Rights and Freedoms.*

The state may no longer assume that individuals have waived their right to privacy just because they "court the risk" of surveillance by, for example, using a communications technology known to be vulnerable to interception. According to the Supreme Court, that assumption would incur a greater risk—that electronic surveillance without a proper warrant would so dilute our privacy as to be inconsistent with a free and open society.

That conclusion has direct implications for the *Privacy Act.* The Act controls the collection of personal information by federal institutions. Principal among these controls is one which prohibits collecting personal information "...unless it relates directly to an operating program or activity of the institution" (section 4).

This provision is open to interpretation in specific cases. But it cannot be read to sanction a collection of personal information which would otherwise be unlawful. Collecting personal information in a way which violates the Charter would also breach the *Privacy Act.*

Since the *Privacy Act* is implicated when federal investigative bodies intercept cellular calls, the Privacy Commissioner wants to satisfy himself that any federal interceptions comply with the Act. However, the emphasis is on fact-finding. There is no reason to believe that federal authorities are unlawfully invading the privacy of Canadians' cellular phone calls.

The commissioner is making inquiries and anticipates reporting the results in next year's annual report.

More troubling is the absence of any legal control over private citizens intercepting cellular phone calls. As one commentator puts it:

> "While the average cellular telephone user may be prepared to contend with occasionally finding another conversation sharing his line, he may be concerned to discover that conversations can be deliberately monitored using something as simple as an old TV set capable of receiving cellular UHF frequency".(**Network Newsletter,** Vol. 10, No. 24, July 30, 1990, p.1)

Using the *Charter*, the Supreme Court has cobbled together protections against cellular monitoring by agents of the state, but the *Charter* does not control individuals' behaviour. And it is doubtful whether current *Criminal Code* provisions prohibiting the surreptitious interception of private communications apply to cellular phone calls. After all, a cellular communication is carried on radio waves and so may not be considered "private".

Some other jurisdictions—California, for example—have passed laws prohibiting both interception of cellular calls and the sale or purchase of cellular eavesdropping devices. An even broader law is before the U.S. Congress covering computer communications and radio communications (H.R.3378 and S.1667). That proposal would make it unlawful to eavesdrop on a car phone conversation or any other private radio communication.

Of course, laws in themselves cannot ensure that cellular conversations remain private. In fact, some argue that such laws could lull cellular phone users into a false sense of security and, hence, be counterproductive. The Commissioner does not agree. It is vital for Parliament to act quickly to protect the privacy of cellular phone users. The mere disappearance of the wires which once carried our communications must not end in the disappearance of our privacy.

Privacy in the Private Sector

In a highly computerized society information knows no boundaries. Yet Canada contents itself with an information policy which distinguishes between the government and the private sector. There is some legal protection against information abuses in the federal (and some provincial) public sectors. But there are no controls over the private sector.

In Europe, the situation is markedly different. Most member countries of the European Community (EEC) have imposed data protection controls over both the public and private sectors. And Europeans are strengthening and harmonizing these controls as they plan for a unified Europe in 1992.

These developments have significant implications for Canadian firms doing business in Europe—or which hope to. Without comparable data protection laws in Canada's private sector, European countries may no longer allow companies to transfer their citizens' information to Canada. In effect, European data protection laws could become a non-tariff barrier, seriously hampering Canadian firms in their dealings with what promises to be one of the strongest trading blocks in the world.

This is no idle fear. In July 1990 the EEC issued a draft directive on protecting individuals' personal data. If adopted, it would bind all EEC member countries on January 1, 1993. The directive is designed to accomplish two broad goals.

- The first is to establish a uniform, high level of privacy protection in both the public and private sectors.
- The second is to remove all barriers to the free flow of personal data among member countries.

The directive has alarming implications for non-EEC member countries which do not measure up to the European standards. Article 24 of the draft requires members not to transfer personal data to any jurisdiction which does not ensure the data adequate protection. Given current Canadian law, it is unlikely that the private sector could prove that it adequately protects personal data.

All relevant European authorities—the OECD, the Council of Europe, the EEC and European data protectors—are fully aware of the directives's implications for countries which are not EEC members. They know that Canada (and the U.S., too) endorses data protection principles (Canada has signed the OECD Guidelines on the Protection of Personal Information). And they know that North America prefers to let the private sector police itself through voluntary compliance. But the Europeans also know that voluntary compliance has not proved particularly successful. In both Canada and the U.S. only a handful of private firms have established meaningful data protection codes of practice.

And so, while the Europeans have been willing to accept that there may be more than one way to ensure adequate data protection (voluntary codes among them), they are unwilling to compromise on the principle. There must be meaningful protection. European data protectors, the guardians of their citizens' privacy, will no longer agree to risk it by authorizing transfers of personal data to countries that pay only lip-service to data protection.

This is not a prediction hazarded on a whim. It is a summation of the comments of several European data protectors to the Privacy Commissioner.

In last year's annual report, the Privacy Commissioner recommended that Parliament amend the *Privacy Act* to require federally-regulated private sector firms to develop, file and implement privacy codes based on the internationally accepted principles established in the OECD Guidelines.

From his discussions with European data protectors the Commissioner believes voluntary codes would be acceptable—as long as they had this statutory underpinning.

Therefore, the Commissioner considers action on this recommendation is urgent. Not only do Canadians deserve this much privacy protection but, without it, Canadian firms risk labouring under a significant competitive disadvantage in their post-1992 dealings with Europe.

Hopeful beginnings

Private sector success stories should not be treated lightly simply because they are few in number. A case in point: in December 1990 the Canadian Bankers' Association (CBA) approved a model privacy code containing the minimum data protection standards member banks must apply to their customers' information.

The code provides customers with rights of access to and correction of their information. As well, it controls the banks' collection, retention, use, disclosure, disposal and security of customer records. Banks have an admirable success record in protecting customer confidentiality but now the code will give their customers greater control over their financial information.

Privacy advocates (the Commissioner among them) will find flaws. One that stands out is the code's failure to provide customers with access rights to recorded opinions or judgements about them. Only factual information will be available. Nor will the code protect employees. Nevertheless, CBA's adoption of a code must be applauded.

Another success story is Bell Canada, the largest telecommunications public utility. It too has adopted a privacy code. However, the Bell code grants privacy rights and protections to employees as well as customers. And access rights are not limited to factual data.

In an increasingly competitive telecommunications environment, Bell's tangible sensitivity to its customers' and employees' privacy is bound to have a ripple effect. The Commissioner urges other telecommunications companies to follow suit. He will monitor and report their progress.

Finally, important new privacy protections were recently announced by the Canadian Direct Marketing Association (CDMA). On February 13, 1991, CDMA launched its "Operation Integrity". CDMA has strengthened the privacy protections in its code of ethics, committing itself to giving consumers greater control over unwanted intrusions by direct mailers and telemarketers.

The program requires all CDMA members to allow consumers to opt out of their mail and phone lists. In addition, members must not include sensitive medical, financial, insurance or court information in the lists they rent. Finally, CDMA has established a task force of senior industry officials to study the privacy impications of direct marketing and to develop additional policies on transferring data.

Operation Integrity is an important step towards ensuring consumers' privacy is respected. The Privacy Commissioner appreciates CDMA's courtesy in keeping him informed and looks forward to continuing this dialogue.

Biomedical Testing

Drug testing

Regular readers of these reports will recall last year's strong cautions against resorting to widespread drug testing to wage the "war on drugs" in the federal government.

The Commissioner's in-depth study—**Drug Testing and Privacy**—examined several environments - transportation, prisons, the armed forces and athletics. Many testing programs being contemplated by the government risked violating the *Privacy Act*, the *Charter of Rights* or broader notions of the individual's integrity.

Clearly there has been some movement to protect privacy interests threatened by drug testing. The office has been consulted by Health and Welfare about drug testing protocols. It has responded to the federal government's report on drug testing in transportation. And it has discussed with the Correctional Service of Canada (CSC) its proposed regulations on drug testing in federal penitentiaries.

Transport Canada no longer proposes to conduct random mandatory drug testing for those in safety-sensitive positions. CSC's proposed regulations are an improvement over earlier ones struck down in 1989 by the trial division of Federal Court in the **Jackson** case. Health and Welfare testing protocols now contain less intrusive means of taking urine samples than did earlier proposals.

Unfortunately there are elements of the transportation drug testing policy that remain troubling. Transport Canada still intends to impose urinalysis at the time of employment, transfer and during regular medicals although its own research revealed no serious threat to safety in the industry caused by substance use. As well, urinalysis provides very limited information—that a substance has been consumed in the past—but not how often or whether the employee was impaired or, more important, is **now** impaired. Mandatory drug testing in these circumstances offends the *Privacy Act* and might not survive a challenge based on the *Charter of Rights and Freedoms.* Urinalysis should be confined to testing "for cause" or after an accident.

Regrettably, National Defence remains committed to its proposal to impose drug tests on its members.This, despite the Commissioner's recommendations and the transport committee's conclusions about random mandatory testing. DND intends to test for cause, as part of an accident or incident investigation, during a probation period following a positive test result and for data collection. It also plans random mandatory tests of members in operational or safety-sensitive positions. Unfortunately, although DND has not yet begun testing, it remains committed to the program or a modified version of it.

There is yet another concern. Fitness and Amateur Sport responded to the Dubin report on drug use among amateur athletes by setting up a new anti-doping organization funded primarily by—but not part of—the federal government. The organization will co-ordinate all sport anti-doping programs in Canada and conduct an expanded program of testing athletes for banned substances.

A major focus of the program would be "no-notice" testing of athletes outside of competition. Up to 3,000 tests could be conducted (presumably annually), the majority of which would be no-notice.

Because the anti-doping organization will not be a federal agency, it will not be subject to the *Privacy Act*. This may have been a deliberate attempt to circumvent the Act. Nevertheless, the organization's approach (as announced by the minister) prompts some general privacy objections. Athletes may find themselves with precious few privacy rights. The Commissioner intends to discuss this situation with officials from Fitness and Amateur Sport.

The Commissioner continues to be concerned about the lack of merit of most drug testing programs. Little this office has seen in the past year has altered its thinking about the fundamental futility of testing programs and their inherent intrusiveness. The government's example is a poor one for the private sector to follow. In most cases, the programs now contemplated or introduced by government appear not to comply with the *Privacy Act*. But public criticism of these programs is the strongest weapon this office has. It cannot enforce compliance.

HIV testing

The office's principal work on HIV/AIDS was the 1989 report, **AIDS and the Privacy Act.** The office also contributed to developing the "Guidelines on Ethical and Legal Considerations in Anonymous Unlinked HIV Seroprevalence Research". The guidelines were developed through meetings arranged by the Federal Centre for AIDS in late 1988 and published in the **Canadian Medical Journal** in 1990. In February 1991 the office participated in a review of the original guidelines.

In November 1990 the Commissioner's office was represented at the meeting of the Council of International Organizations of the Medical Sciences (CIOMS), a World Health Organization body. The meeting discussed draft ethical guidelines on epidemiological research, including HIV/AIDS research. Staff continue to handle requests and investigate complaints about privacy and HIV/AIDS. Since the requests often concern issues or bodies not covered by the *Privacy Act*, the office attempts to re-direct callers to the appropriate authorities.

The office's work on HIV/AIDS is complemented by work in Ontario. The Ontario Law Reform Commission is doing a broad study on the legal (and, to some extent, ethical) implications of HIV/AIDS testing. The Ontario Information/Privacy Commissioner has published two reports on HIV/AIDS, one dealing with HIV/AIDS and privacy, the other with HIV/AIDS and the workplace.

Genetic testing

Genetic testing is just one of many evolving biotechnologies that pose serious privacy dilemmas. Genetic testing encompasses three techniques. The first—genetic screening—examines a tissue or blood sample from an individual for genes or genetic "markers" indicating a present or potential genetic disorder or other physical trait.

The second technique is genetic monitoring. It looks for genetic or chromosomal changes that may be caused by exposure to workplace or environmental chemicals or phenomena (radiation or the fumes from plastics, for example).

The third technique is forensic DNA analysis, sometimes colloquially (and inaccurately) referred to as DNA fingerprinting. This technique matches samples of material genetically. Blood stains from the scene of a crime may be genetically matched with those of a suspect. Forensic DNA analysis may also prove blood relationships in immigration or paternity cases.

Genetic technology holds great promise for the identification of genetic disorders, a limited number of which may be treatable. However, there is a privacy concern in the potential of genetic testing to reveal highly sensitive information about the person tested and his or her genetic relatives.

Other forms of biotechnological testing, such as screening for HIV/AIDS antibodies or drugs, reveal only a single piece of information—infection with the HIV or the past use of drugs. But genetic testing can reveal hundreds of bits of information about an individual or relative. The data ranges from the certainty of developing crippling or deadly diseases (such as Huntington's chorea or cystic fibrosis), to the likelihood of developing psychiatric disorders (manic depression) to predispositions to elevated cholesterol levels, high blood pressure or certain cancers.

Genetic testing is on the brink of becoming an issue in human reproduction (pre-conception, prenatal and neonatal testing), employment (screening and monitoring), access to government and private sector services (schooling, insurance, credit), criminal investigations, during ordinary medical care and in performing research.

The current and potential uses of the information produced by genetic testing persuaded the Commissioner to study its privacy implications. While its uses are now confined primarily to reproduction, its potential is enormous. Better that society examine the technology's implications before it attacks privacy rights. The study should be completed by late Spring 1991.

The Commissioner has always been loathe to press for regulation of the private sector. However, the privacy implications of genetic testing demand that the government consider whether there should be direct regulation of any private sector uses of this highly intrusive technology.

The Commissioner is not alone. Privacy experts are examining similar measures in the United States. Most western European countries already regulate personal data collection by the private sector. In this sense, Canada is falling behind a growing movement to protect individual privacy not only from governments, but from the seemingly insatiable curiosity of the private sector.

Electoral Reform - A Permanent Voters' List

Privacy issues can rear their heads where least expected. A case in point was the government's appointment of a Royal Commission to determine whether Canada's electoral laws needed overhauling.

The commission was asked to examine the electoral process and party and campaign financing and to study the option of a permanent voters' list that would replace door-to-door enumeration.

Doing away with costly, time consuming door-to-door enumeration may be appealing. The process contributes to the length and expense of Canadian federal elections, but the alternative needs serious study.

The commission heard proposals which focussed on combining data from such federal data banks as income tax files, citizenship information, change-of-address notices to Canada Post, census forms and pension records. Others proposals suggested incorporating provincial health and drivers' records and there was significant support for a voter's identity card or a requirement that voters produce a Social Insurance Number.

As a result, the Privacy Commissioner wrote to the commission asking it to consider the privacy impact of its recommendations.

His concerns included the implication of new large-scale collections (or linkages) of personal information. This type of permanent voters' list would become the sort of population register that could pose a real threat to human rights and freedom. Wartime experience proves that such lists will be abused—even in Canada—to subject large groups of individuals to discriminatory treatment, arrest, detention and confiscation of their property.

Further, once in place, pressures would mount to make the list widely available to all arms of government for unrelated uses. Ensuring exclusive election use and absolute confidentiality of the data would be vital.

Growing dissatisfaction with abuses of SIN reflects public resistance to national identification and registration schemes—a resistance which would be compounded if SINs were used to link the databases and to establish a citizen's right to vote.

Finally, the *Privacy Act* prohibits access to other federal data bases to create such a list. Thus, Parliament would have to pass legislation to override the *Privacy Act,* a step the Commissioner could never support.

Citizens around the world are fed up with being counted, recorded and monitored by the state. A voters' list could evoke deep unease. It would be ironic if the electoral process—the heart of the democratic way of life—became the vehicle which tipped the scales further from the individual to the state.

While the Commissioner does not want to restrict progress, he does want to ask some pertinent questions before the project advances too far. The electoral commission has welcomed his input and plans to report to the public in the fall of 1991.

Privacy and the Public Interest: a Difficult Balance

Generally the *Privacy Act* prohibits government institutions from disclosing personal information without the subject's consent. However, the Act also recognizes 13 circumstances which dispense with this rule.

One of the 13 is very general and, hence, both difficult to apply and easy to abuse. Sub-paragraph 8(2)(m)(i) authorizes disclosure without consent:

> "for any purpose where, in the opinion of the head of the institution,
> (i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure..."

During the past year the most frequent user of this provision was Correctional Service of Canada (CSC). The situation develops when prison incidents such as escapes, unnatural deaths or hostage takings lead to internal investigations and subsequent reports. These reports contain personal information about both the inmates and prison officials who were involved. Consequently, CSC must consider the restrictions contained in the *Privacy Act* before disclosing the reports.

CSC may want to release the reports in order to preserve public confidence in the correctional system. It may also need to provide copies to journalists who have requested access under the *Access to Information Act* or to members of Parliament or Parliamentary committees wanting to review the reports to assess overall correctional administration. In these situations, CSC removes information which is exempt under the *Access to Information Act* as well as sensitive or extraneous personal details.

CSC seeks to disclose only sufficient personal information necessary to satisfy the public interest test set out in the *Privacy Act* and give the public a clear picture of what transpired.

Once this screening satisfies the commissioner of corrections and the solicitor general, they notify the Privacy Commissioner of the intended release, in advance if reasonably possible. When the Commissioner receives the notification, he assesses whether there is a public interest disclosure which clearly outweighs any resulting invasion of privacy. If he does not agree he tells the institution. However, the Commissioner has no power to prevent the release—only to tell the individuals affected that their information will be disclosed.

Evidence of just how difficult it is to apply the "public interest" test was demonstrated in two disclosures which the Commissioner reported last year ("Reports on two inmate escapes"). The Standing Committee on Justice and the Solicitor General wanted to inquire into the events surrounding the two widely-publicized prison incidents—the escape from Dorchester, New Brunswick, of Allan Légère (during which he allegedly murdered one person) and the day-pass release from the Edmonton institution of Daniel Gingras (during which he murdered two people).

CSC had previously disclosed censored versions of the investigation reports to the media and gave that version to the justice committee. The committee, however, wanted the uncensored versions and issued an order to the solicitor general for the complete reports.

The solicitor general refused to act on the order, maintaining that the *Privacy Act* prohibited the disclosure. His refusal became the subject of a question of privilege in the House of Commons and the matter was referred to the Standing Committee on Privileges and Elections.

In his testimony before the committee, the solicitor general held that he was responsible for respecting sub-paragraph 8(2)(m)(i) of the *Privacy Act*. Therefore he had to be satisfied that a public disclosure of the reports would be in the public interest and that this interest clearly outweighed any invasion of individual privacy. He did not believe that the *Privacy Act* gave him the authority to accede to the committee's demand for an in-camera review of the uncensored reports.

The then-acting Privacy Commissioner, appearing before the privileges committee, applauded the solicitor general's resolve to protect the privacy of persons mentioned in the reports. However, he felt that the minister was taking an unnecessarily narrow view. Sub-paragraph 8(2)(m)(i) of the *Privacy Act* clearly gives the solicitor general the authority to determine whether disclosure of the uncensored reports to an *in-camera* session of the Justice Committee is in the public interest. The acting Commissioner maintained that it was not at all inconsistent with the provision to decide that disclosure to the committee is in the public interest, providing it takes place under conditions which would ensure that the censored portions remain confidential.

At the time of this report, the final chapter of this story has yet to be written. The privileges committee has not concluded its deliberations and the Privacy Commissioner has not completed his investigation of a related complaint.

"The truth, the whole truth and nothing but the truth"

However, there is another facet to this story. It is unusual for the Privacy Commissioner to publicly remind government institutions that privacy is not an absolute value. But the Act does recognize that privacy may be invaded in order to serve certain important, collective goods.

Being doctrinaire in insisting on confidentiality in all cases risks giving the *Privacy Act* a bad name—one it does not deserve. These CSC incident reports are a case in point.

Although the public interest CSC wants to serve (by disclosing these reports) is public confidence in the corrections system, CSC has removed portions which are critical of correctional staff members. While CSC's action to shield these individuals may be understandable, it leads to a report which gives the public a less than complete picture of the incident.

Without giving the "bad" with the "good" can CSC really be serving the public "interest"? This question is the subject of ongoing discussion between CSC and the Privacy Commissioner. What is needed, it would seem, is for CSC to use the public interest clause as an extraordinary measure and, when it is invoked, to ensure that the disclosures give the complete picture.

Complaints Directorate

Complaints have increased by approximately 10 per cent per year since the office opened for business seven years ago. This year the pattern continued as the office received 1,239 complaints compared to 1,086 last year—a 14 per cent increase.

Time limit complaints

Occasionally the Commissioner felt like a stuck record during previous reports as comments about Correctional Service Canada and National Defence delays were a recurring theme.

Now, the music has changed. Time limit complaints were down substantially this year and full credit goes to Correctional Service Canada. CSC's response to the Commissioner's criticism of last year's performance was a complete overhaul of its request handling procedures.

The result was an astounding 200 per cent decrease in new CSC time limit complaints—from 214 last year to 50 this year. Last year's volume accounted for 50 per cent of the office's delay complaints. This year's total—only 15 per cent. A tip of the hat to Correctional Service for a job well done.

Another entrenched cause of delay complaints was the Department of National Defence handling of members' Personal Evaluation Reports (PERs). The problem occurred because military personnel had to make formal application to see their evaluations and the result was a huge caseload and an inevitable backlog. Last year the Commissioner applauded National Defence's decision to treat PERs requests informally. As predicted, the number of privacy requests to DND dropped 20 per cent — most of the decrease directly attributable to the policy change. The result is a 36 per cent decline in time limit complaints against National Defence—from 78 to 50.

Clearly, government institutions are trying hard to respect the statutory time limits, the trend is evidence of that. But shrinking resources threaten the "good news" story. An individual's right to timely access to personal information should not be sacrificed on the altar of fiscal restraint.

Fair Information code

Although complaints about denial of access were up, this past year's 14 per cent hike results from a substantial jump in complaints about collection, use and disclosure of personal data—the fair information code. This year's complaints against the code skyrocketed to an unprecedented 386 from last year's total of 173.

Again, labour-management disputes at Canada Post Corporation seem to be at the root of the problem. The corporation appears to be administering its new leave management policy aggressively. Employees are concerned that medical information about them has been improperly collected and used to manage attendance at work.

Top ten

This year's report includes a list of the office's top ten clients, a group which accounts for 80 per cent of its total caseload. Correctional Service Canada, the perennial leader in the new complaints category until this year, has happily ceded that honour to Canada Post Corporation.

New complaints against Canada Post went from 97 to 237, while CSC's 165 are less than half of last year's record 392.

Another significant increase occurred at Employment and Immigration Canada where the 128 complaints represented a three-fold jump. Transport Canada has returned to a more characteristic total of 67 after a low of six complaints in 1989-90. For no apparent reason National Archives, National Defence and the Canadian Security Intelligence Service have also seen significant increases while Health and Welfare and the RCMP have experienced decreases.

		GROUNDS		
DEPARTMENT	TOTAL	ACCESS	TIME LIMITS	OTHER
Canada Post Corporation	239	40	54	145
Correctional Services Canada	165	77	50	38
National Defence	163	51	56	56
Employment and Immigration Canada	128	61	44	23
Canadian Security Intelligence Service	77	67	9	1
Revenue Canada, Taxation	75	23	39	13
Transport Canada	67	43	17	7
National Archives of Canada	51	12	1	38
Royal Canadian Mounted Police	50	35	2	13
Health and Welfare Canada	32	14	15	3
Others	192	95	50	47
TOTAL	1,239	518	337	384

How institutions measured up

A number of factors—such as an unexpected volume of requests—can prompt complaints. Actually, many of the factors are beyond the control of the institutions. A more meaningful performance indicator is the proportion of complaints that are well-founded.

Using this measure, the Royal Canadian Mounted Police is the most successful institution by a long shot. Only five complaints were well-founded (or well-founded/resolved) while 16 were not well-founded and seven were discontinued. This is a decrease from 19 well-founded complaints two years ago and 10 last year. This reflects the RCMP's sincere respect for the letter and spirit of the Act. But special kudos are due the RCMP's access and privacy coordinator for his personal commitment to reducing the number of well-founded complaints.

And National Archives continues to maintain its high standards—only four of 23 complaints were well-founded, three of which were resolved.

At the risk of appearing inconsistent, there is praise for Canada Post. Despite having the questionable honour of first place as the office's most important client, only 50 of the 230 complaints were well-founded. Of these, 37 were resolved.

	RESULTS				
GROUNDS	WELL-FOUNDED	WELL-FOUNDED RESOLVED	NOT WELL-FOUNDED	DISCONTINUED	TOTAL
ACCESS	30	70	320	16	436
Access	27	69	305	16	417
Correction/Notation	3	1	14	0	18
Index	0	0	1	0	1
Language	0	0	0	0	0
PRIVACY	17	45	141	16	219
Collection	0	11	22	3	36
Retention & Disposal	3	4	7	2	16
Use & Disclosure	14	30	112	11	167
TIME LIMITS	245	0	101	23	369
TOTAL	292	115	562	55	1,024

Although CSC seems to have conquered its delay problems, it had the worst ratio of justified complaints among the large institutions as 64 per cent—103 of 162—of the complaints investigated were considered well-founded. Not far behind were Employment and Immigration and Revenue Canada Taxation with 60 per cent and National Defence with 58 per cent well-founded.

Overall, investigators completed 1,008 investigations comprising 551 not well-founded, 402 well-founded and 55 discontinued.

This year the complaints have been grouped under three major headings. They are: access complaints—dealing with individuals' problems with their applications to see personal records; privacy complaints—concerning the fair information code (proper collection, use and disclosure); and time limits—including both delay in the initial response to an application or time extensions.

More resources please!

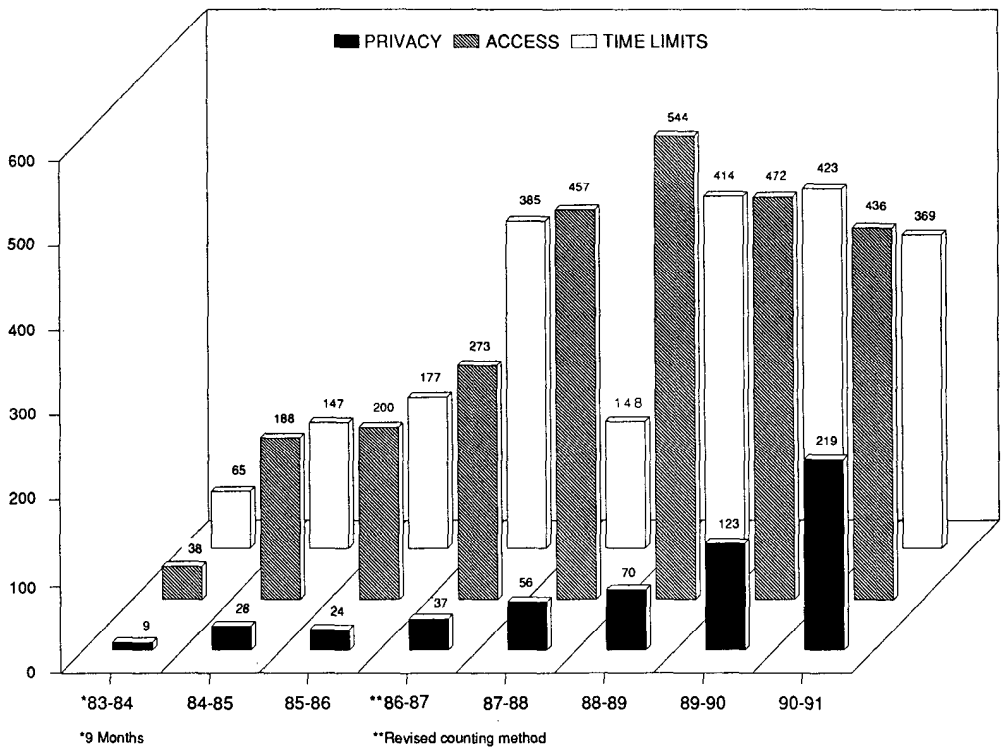
Despite having completed more than 1,000 cases, the norm for the past three years, 589 complaints were pending at the end of the year—a 38 per cent increase from the preceding year. Sadly, this means a return to the backlog the office worked so hard to eradicate two years ago. The problem will be compounded if the 10 per cent increase forecast for 1991-92 materializes—and it probably will if this year's 14 per cent increase is an indicator.

Unless the office receives more staff and money, its open caseload will soar to more than 700 complaints by the end of the current year. This represents more than the total caseload investigated by the office in the 1987-88 year.

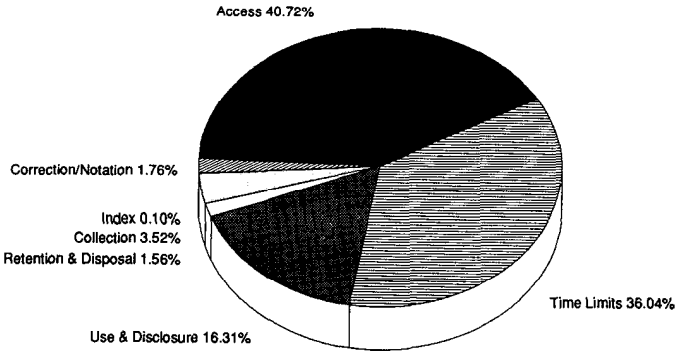
Despite increased productivity, the office has not closed more cases this year. Increased efficiency has been more than offset by the drop in time limit complaints (which consume fewer resources) and the rising tide of complaints against the fair information code (the most complex and time-consuming investigations).

Unfortunately the government turned down the office's request for more investigators and operating funds. This decision will exacerbate the ever-increasing backlog; increase investigator's caseloads and keep clients waiting longer for decisions on their complaints. In short, the office now risks becoming part of the problem.

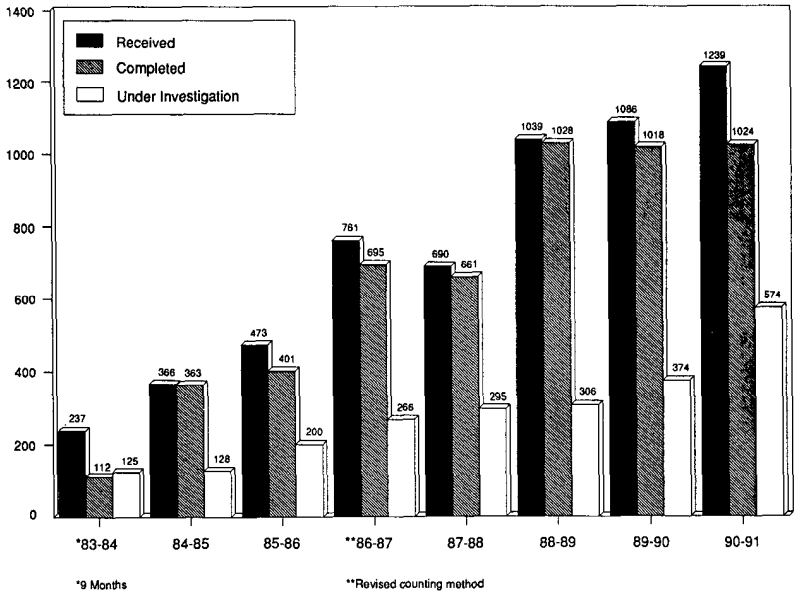
Completed Complaints and Grounds 1983-91



Complaints Completed by Grounds 1990-91



Completed Complaints 1983-91



*9 Months

**Revised counting method

Completed Complaints by Department and Result

Department	Results				
	Total	Well-founded	Well-founded; Resolved	Not Well-founded	Discontinu
Agriculture Canada	11	2	1	8	
Canada Post Corporation	233	13	39	171	
Canadian Human Rights Commission	5	1	3	1	
Canadian Security Intelligence Service	83	6	9	67	
Commissioner of Official Languages	1	0	0	1	
Consumer and Corporate Affairs Canada	5	3	0	1	
Correctional Service Canada	162	84	19	49	
Employment and Immigration Canada	78	33	10	27	
Environment Canada	1	0	0	1	
External Affairs Canada	7	3	0	3	
Farm Credit Corporation Canada	1	0	0	1	
Finance Canada	1	0	0	1	
Fisheries and Oceans	6	1	3	1	
Health and Welfare Canada	34	16	3	15	
Indian and Northern Affairs Canada	0	0	0	10	
Justice Canada	9	2	0	7	
Labour Canada	1	0	0	0	
National Archives of Canada	24	1	3	19	
National Defence	84	34	8	31	

Department	Results				
	Total	Well-founded	Well-founded; Resolved	Not Well-founded	Discontinued
National Museums of Canada	1	0	0	1	0
National Parole Board	20	2	5	13	0
Privy Council Office	3	2	0	1	0
Public Service Commission of Canada	2	0	0	2	0
Public Service Staff Relations Board	7	0	3	4	0
Revenue Canada, Customs and Excise	14	11	1	2	0
Revenue Canada, Taxation	71	43	0	28	0
Royal Canadian Mint	1	0	1	0	0
Royal Canadian Mounted Police	78	2	3	66	7
RCMP Public Complaints Commission	1	0	0	1	0
Secretary of State of Canada	3	2	0	1	0
Solicitor General Canada	14	1	0	12	1
St. Lawrence Seaway	1	0	0	1	0
Statistics Canada	1	0	0	1	0
Supply and Services Canada	3	0	2	1	0
Transport Canada	42	27	2	12	1
Treasury Board of Canada	1	0	0	0	1
Veterans Affairs Canada	5	3	0	2	0
TOTAL	1,024	292	115	562	55

Origin of Completed Complaints

Newfoundland	0
Prince Edward Island	8
Nova Scotia	41
New Brunswick	36
Quebec	148
National Capital Region Quebec	6
National Capital Region Ontario	53
Ontario	407
Manitoba	66
Saskatchewan	33
Alberta	55
British Columbia	166
Northwest Territories	0
Yukon	5
Outside Canada	0
TOTAL	1,024

Cases

Tax files not for fan mail

A journalist got a fan letter from a federal employee at her home address and called the Commissioner's office to inquire how the admirer could have found her private residence. The journalist did not want to lodge a complaint or get the employee into trouble, but she was concerned both for her safety and how the information had been obtained.

The office was torn between respecting her wishes and ensuring that federal employees not use government files for purposes well outside the most generous interpretation of a "consistent use". The investigator tracked the source to Revenue Canada-Taxation.

Confronted with his letter, the employee explained that he simply wanted the woman's autograph. He did not appear to pose any threat to the journalist, who was relieved and asked that the case be discontinued.

However, the revelation that the employee used information from Taxation data obliged the office to tell Revenue Canada which has a strict code of ethics and imposes stringent security measures on handling taxpayers' files. Taxation investigated, found this was not the only incident and disciplined the employee.

Revenue Canada delays

Even though the *Privacy Act* has been in effect for eight years, failure to meet time limits continues to be a problem.

To name just one, Revenue Canada-Taxation occasionally displays an indifference to applicants' rights to receive their information within the time the law allows. Curious since Taxation promptly penalizes taxpayers who are casual with tax filing deadlines!

For example, on May 7, 1990, a woman went to the Vancouver taxation office to inquire about an application she had filed in January to see her income tax file. Taxation had no record of the request so she made another. On June 26, she called the Commissioner's office to complain that she had neither heard nor seen anything.

The office called Taxation to inquire. Even so, the woman did not receive the file until August 13, 96 days later. Departments are allowed to ask for a 30-day extension under some circumstances. However, they must notify the applicant who then may complain if she considers the extension unreasonable.

Revenue Canada had no justification for not writing to the woman to acknowledge her request, to say when it would provide the file and—ultimately—for not responding in time.

The Commissioner considered the complaint well-founded.

Court orders CSIS to respond

The Canadian Security Intelligence Service (CSIS) told an applicant that it could not provide the personal information he wanted in the 30 days the Act allows.

The delay was partly the result of many new applications (apparently prompted by an article in the **Toronto Star**) and by the need to consult other parties before it could release the material.

The man complained to the Commissioner and told the investigator that he intended to go to Federal Court if CSIS did not give him the information within the maximum 60 days set out in the Act.

On the 61st day, when the Commissioner found CSIS had still not finished processing the man's records, he concluded the complaint was well-founded and advised the complainant of his right to go to Federal Court. (Applicants may not ask for a court review until the Commissioner has completed his investigation.)

The complainant asked the court to issue a *Writ of Mandamus* which would compel CSIS to produce the information. The motion was heard 20 days later and the judge ordered CSIS to reply to the man's request within one month of the date of the order. CSIS complied.

Although CSIS finally provided the information, the hearing (and the extra month the court allowed) added yet another 50 days to the process — hardly a satisfactory solution. After eight years of living with the *Privacy Act*, it is unacceptable for applicants to have to go to court to force departments to provide timely access.

More access during military grievances

A complaint against National Defence (DND) may have prompted it to change its grievance procedures for military members. The case raised important questions about a member's access to factual information collected by DND's legal services during the grievance process.

At DND, lawyers may investigate military grievances to prepare legal opinions and advise the chief of defence staff. Normally, government staff relations officers (who are not lawyers) investigate such grievances. The military procedure effectively extends legal privilege over more of the documents.

The problem this causes became apparent when an officer complained to the Commissioner that DND had denied him a good deal of information from his grievance file, claiming exemptions for solicitor-client privilege or personal information about other individuals.

The investigator confirmed DND used the solicitor-client exemption on all the documents either obtained or prepared by its legal services during the grievance investigation. The department argued that the material became privileged since its legal services developed the file specifically to prepare a legal opinion and recommendations for senior staff.

The Commissioner was concerned about such a broad use of the solicitor - client privilege, considering it both unfair and contrary to the spirit of the act to use the privilege to withhold factual material and witness statements obtained during the investigation. He suggested DND use its discretion to disclose more information to the complainant. DND agreed to reconsider and gave the officer ten more pages of information including the witnesses' statements.

The Commissioner also agreed that the other disputed material was personal information about other individuals and that it was correctly exempted.

DND has since revised its military grievance procedures and now discloses to members all documents (with some limited exceptions) which the adjudicative authority will review when considering their grievances.

Can't claim exemption if doctor to disclose

A man complained to the Commissioner when National Archives denied him portions of his old military medical records, considering it to be not in his "best interest" (section 28) to examine a 25-year-old mental health assessment. National Archives was prepared, with his written consent, to give the information to his family doctor who could then explain the assessment.

Privacy regulations allow a department to require an applicant to examine personal health records only in the presence of a qualified medical practitioner or psychologist who can explain the information.

In this case, however, the man argued that he knew the contents of the assessment and did not need an explanation.

The Commissioner held that if Archives thought it was not in the applicant's best interest to see the records it should exempt them entirely. But if it intended to disclose them—even through his doctor—then it was inconsistent to claim it was not in his best interest.

The Commissioner was also concerned that Archives refused access based on a review by a psychiatrist retained to assess the file when the man submitted similar privacy requests in 1985 and 1990. The Commissioner considered the assessment unreliable since it was based solely on a review of medical files dating back 25 years and did not consider the man's current emotional state.

The information was disclosed after the Commissioner concluded that the man was entitled to see the file. Further, National Archives agreed to change its procedures for processing sensitive medical information. In future, it will either claim the medical exemption or disclose the information directly to the applicant or to his or her doctor.

Witness statements available after investigation

A woman who had lodged a discrimination complaint with the Canadian Human Rights Commission (CHRC) asked to see the information in the CHRC complaint file. She complained to the Privacy Commissioner when CHRC withheld some of the data.

What CHRC had refused to disclose was addresses and telephone numbers of other individuals and witness statements. The Commissioner agreed that others' personal information was legitimately exempt. However, he disagreed with exempting the witness statements once the investigation was completed.

Generally, the Privacy Commissioner agrees that witness statements should not be disclosed during investigations because this might harm the investigation. However, in the case at issue, the investigation was complete. The Commissioner asked CHRC to demonstrate what injury could reasonably be expected if the complainant saw the witness statements.

CHRC was unable to demonstrate any reasonable possibility that disclosure would injure either this or future investigations. Nonetheless, it took considerable persuasion before CHRC finally agreed to disclose the statements to the complainant. Since the information was initially denied, the Commissioner considered the complaint well-founded but resolved.

Revenue Canada can see personal expenses

An Ontario woman's difficulties paying her federal income tax arrears generated a complaint against Revenue Canada - Taxation. The woman was upset when an officer insisted on examining her personal expenses to assess her ability to pay. He maintained that the *Income Tax Act* gave him that right but the woman felt the procedure was abusive and an invasion of her privacy.

The *Privacy Act* limits government institutions' collection of personal information to that which "relates directly to an operating program or activity of the institution". This effectively restricts government collection to personal information which clearly is required for that program.

Revenue Canada explained that as administrators of the *Income Tax Act*, it is responsible for collecting individuals' income tax. The department has a collection procedure that ensures that the law is applied equitably to all taxpayers, but yet allows it to consider each individual's financial circumstances. In fairness to the majority who pay promptly, the department's policy deals firmly with those who do not.

The Commissioner reviewed Taxation's collection policy and agreed with the collection officer's need to examine the taxpayer's personal expenses. Under the circumstances the *Income Tax Act* requires her to provide this type of information. Thus, the Commissioner considered Taxation had respected the collection provisions of the *Privacy Act* and he concluded that the complaint was not well-founded.

Hiring must balance fairness and privacy

A complaint against Employment and Immigration Canada (EIC) demonstrated the difficulty of making the hiring process transparent without stripping away candidates' privacy.

Two successful candidates in an internal EIC competition complained that a staffing officer gave their personal evaluations and personal references to another employee who was appealing the results. This person then circulated the information in the office.

The Public Service Commission's policy on appeals requires departments to disclose only directly relevant personal information about the successful candidates. In this case the evaluations had been used during the staffing process but were neither referred to during the appeal nor considered as part of the appeal decision. Clearly they were not relevant. The disclosure was a significant invasion of the employees' privacy although the result of a perhaps overzealous attempt to be fair.

EIC reminded all its personnel divisions about the disclosure policy and will issue more detailed guidelines for staffing officers caught between the competing demands of fairness in staffing and protection of candidates' privacy.

Immigration disclosure of refugee claim "consistent"

A man wrote to the Commissioner objecting to an immigration officer having told officials of a U.S. state (without his consent) that he was claiming refugee status in Canada.

During his refugee hearing, it became apparent that the man had been found guilty of a criminal offence in a state but he had failed to appear for sentencing.

The complainant argued that since the process was not complete, his situation was not equivalent to a criminal conviction in Canada which would prevent him being considered a refugee. A senior immigration officer wrote to the clerk of the state's first circuit court to determine whether the man was considered to have been convicted. The letter explained that Immigration needed the information because the complainant had applied for refugee status.

The state court confirmed that the judicial finding of guilt was a conviction.

The investigator found that one of the objectives of the *Immigration Act* is "to promote international order and justice by denying the use of Canadian territory to persons who are likely to engage in criminal activity". The Commissioner concluded that revealing the man's refugee claim was permissible because it was consistent with Immigration's purpose for having obtained the information. He considered the complaint not well-founded.

Direct pay request premature

A Transport Canada employee complained that the department was asking for his bank account number so it could deposit his pay directly, rather than issue a cheque.

Transport's request apparently followed the federal government's announcement that it would stop paying employees by cheque on April 1, 1991 and begin depositing pay directly into employees' bank accounts.

The complainant objected strongly to having to give his bank account number to his employer. In fact, he was just one of a number who called or wrote to the office wanting to know if they had to provide the information.

The investigator identified two privacy issues. First, could Treasury Board (the employer) require employees to provide the location and number of their bank accounts for direct pay deposit? Did it have legal authority for collecting the information?

The Commissioner concluded that the government had the legal authority to decide how it will pay its employees. Collecting the necessary details to administer its pay procedure would not breach the *Privacy Act*.

However, the second issue concerned how the employer would deal with employees who refused to provide the information. Could it give their names, addresses and social insurance numbers to a bank to open accounts without their consent?

Privacy staff had several meetings with Treasury Board and were told that the program was still voluntary—Transport Canada had simply been eager to begin. No information had been collected except from those who had opted into the program. However, the Board acknowledged the problem of handling recalcitrant employees' pay.

Still, with the Minister's announcement in December 1989, it appeared that the public service was moving toward mandatory direct deposit. The Commissioner decided to hold the complaints open until the policy became clearer.

Then, on December 15, 1990, the government announced that direct deposit would remain voluntary. The complainants would not have to provide the information and the government would not be opening any accounts on employees' behalf. Thus, the Commissioner considered the complaint not well-founded.

Staff relations board exhibits now kept two years

Although privacy regulations require government agencies to hold personal information for at least two years, a complaint revealed that the Public Service Staff Relations Board (PSSRB) kept its exhibits for just three months before having them destroyed or returned to the party who presented them.

The two-year period was written into the regulations to give individuals enough time to examine the material if they were interested.

A woman complained that her privacy rights were infringed because the PSSRB destroyed the exhibits well before the two-year period.

PSSRB explained to the privacy investigator that it lacked the facilities to keep all exhibits—items ranging from volumes of documents to a broken baseball bat, garbage cans and even a hangman's noose! PSSRB staff also pointed out that all parties to a hearing receive copies of the exhibits so nothing was being destroyed that they had not already received.

Nevertheless, the regulations are clear. The Commissioner concluded that PSSRB must keep exhibits containing personal information for at least two years after taking the last administrative action. The Board agreed and the Commissioner considered the complaint resolved.

Personal information should be accurate

A veteran Canada Post employee complained to the Commissioner that the post office had given false medical information about him to the Workers' Compensation Board (WCB), in order to deny him benefits.

Canada Post had told WCB that the employee was ineligible because his injury was caused by a chronic medical condition. According to the employee's supervisor, the employee had given her the information and she was merely reporting what she thought might be relevant to the claim.

The employee denied having the condition and a recent examination by a specialist confirmed this. He also denied ever having told anyone, let alone his supervisor, that he had the condition.

During his inquiries, the investigator noted a factor which may have contributed to the problem. Canada Post manages the WCB claims aggressively in order to minimize costs. It argues that it is obliged to give WCB any information which could question the validity of the claim.

The *Privacy Act* requires that personal information being used for administrative purposes be as accurate, up-to-date and complete as possible. In this case there was no evidence that the supervisor had made any effort to verify that the medical information was accurate.

After protracted discussions. Canada Post agreed reluctantly to tell the WCB that it had no information to substantiate its allegation that the claimant had the medical condition.

The Commissioner considered the complaint well-founded and resolved.

Licence holders list not for surveys

An airline operator's call to the office about a Transport Canada drug use survey prompted the Commissioner to initiate a complaint of his own.

The caller became concerned when a market research company asked for the names, addresses and telephone numbers of his employees. The company said it was conducting a survey for Transport Canada on substance use in the transportation industry. It needed the personal information to randomly select participants for the survey.

The surveys, it was established, were a major component of Transport Canada's study to determine what risks employee use of drugs and alcohol posed to transportation safety in Canada. Participants were asked to complete a questionnaire about their use of alcohol, prescription, non-prescription and street drugs and about workplace conditions which could influence their using these substances.

Two areas of privacy concern surfaced:

- Was there an improper collection of personal information during the survey? and

- Did Transport Canada respect the use and disclosure provisions of the *Privacy Act?*

Controls on use and disclosure require government agencies to collect only personal information that relates directly to their operating programs or activities. The information must be collected directly from the individual (whenever possible) unless that would lead to collecting inaccurate information or defeat the purpose or prejudice its intended use. And the individual must be told why the information is being collected.

The investigation established that the questionnaires contained no identifying personal information to link them to any specific individual. Since the respondents could not be identified, the information was not personal and so its collection did not violate the *Privacy Act.*

However, it was clear that Transport Canada compiled the list of some survey participants from personal information it collected for other purposes, none of which included disclosing to research organizations. In most sectors Transport gave the survey company only the names and work telephone numbers. But, in the case of airport employees, its source was a list of employees licensed to operate airside vehicles and disclosing the names was not consistent with the original collection purpose and was improper.

The investigator also found that the survey companies began collecting the information before written contracts were in place. The draft contracts contained no references to the collection principles in the Act. As a result, representatives of Privacy, Supply and Services (the contracting authority) and Transport Canada met to ensure that all future contracts requiring personal information collection contain standard clauses about collection, retention, use, disclosure and disposal of information to ensure that they comply with the Act.

The Commissioner also recommended that Transport Canada obtain the individuals' consent before considering any future use of personal information that is not consistent with the original collection purpose.

Notifying the Commissioner

During the reporting year the office examined 50 notices from government agencies advising of their intention to release personal information "in the public interest" or to benefit an individual. The disclosures ranged from confirming citizenship so that individuals could receive pensions or awards to detailed reports on escapes from federal penitentiaries. In fact, inmate incidents have become a recurring feature of the notification process (see page 24 for greater detail).

The following are examples of other public interest notifications.

DND releases security clearance details

National Defence (DND) advised the Commissioner that it intended to give an employee normally exempt information from his security clearance file.

In the midst of processing the man's application to see his file, DND staff learned that provincial police had laid criminal charges against him, including one of sexually assaulting a former employee. His security file contained a military police interview with the plaintiff during which she detailed their longstanding sexual relationship. She had made it clear to the military police that it was mutually desired.

Since the *Privacy Act* allows investigative bodies (including military police) to protect sources interviewed during security clearance investigations, DND would normally have exempted the woman's comments. They concerned her as well as him and it would have been virtually impossible to extricate only the man's information from the record and the source of the comments would have been obvious. The department's dilemma was that it had accepted in confidence information which appeared to contradict the woman's charges. The man may not have known about the information in his file and therefore be deprived of details vital to his defence. DND concluded it was in the public interest to provide him the information before the matter went to trial.

The Commissioner notified the woman.

Woman given details on son's death abroad

A woman asked the RCMP and External Affairs to tell her what they knew about the death of her son in Thailand. Although both the RCMP and External had been satisfied with the Thai investigation, and a Canadian pathologist had confirmed the overseas postmortem results, the woman still had questions.

The RCMP intended to give her 21 pages from its inquiry report, exempting some limited information about other individuals. External, meanwhile, agreed to provide material from files located in two overseas embassies and Ottawa headquarters.

Normally the *Privacy Act* would protect the information—even from the man's mother. But both agencies considered it was in the public interest to give her the report so that she could pursue her inquiries in Thailand—and perhaps put her mind at rest. The Commissioner agreed.

List of unclaimed dividends sought

An applicant used the *Access to Information Act* to ask Consumer and Corporate Affairs for lists of unclaimed dividends under three acts: the *Bankruptcy Act*, the *Canada Business Corporations Act* and the *Winding-Up Act*. The applicant intended to track down the creditors.

CCA advised the Commissioner that it would release the lists because it would benefit the individuals concerned (paragraph 8(2)(m)(ii)). The Commissioner agreed but admitted to "lingering unease about the need for this disclosure", observing that if government institutions are reasonably able to locate individuals to whom they owe money, they should do so. He concluded that it "seemed less than ideal" to disclose personal information without consent to permit third parties to locate creditors (presumably for a fee).

Poor catch for Revenue Canada

Fisheries and Oceans advised the Commissioner that it intended to provide Revenue Canada's GST Communications Office with a mailing list of commercial fishermen. The GST office wanted to send fishermen an information booklet explaining how they should "charge, record, calculate and send in the tax". Revenue Canada had no other way of reaching fishermen and Fisheries concluded that clearly it was in the fishermens' interest to receive the material.

The Commissioner was not so sure. The GST legislation had not then been passed and, while it might be helpful, he was not convinced disclosure of the list would "clearly benefit" fishermen. However, he told Fisheries he had no objection to their mailing the material for Revenue Canada.

The Fisheries department could not find sufficient "public interest" to warrant its mailing GST material. It did, however, provide Revenue Canada with a list of fishermen's associations.

Board members' names not "personal"

The International Development Research Centre (IDRC) told the Commissioner it would release the names of board members who had attended an IDRC meeting in Bangkok, Thailand. The centre had given a journalist (who applied under the *Access to Information Act*) the members' expense accounts, but not the names. The journalist complained to the Information Commissioner who recommended release.

After discussing the notification with IDRC staff, the Privacy Commissioner agreed with the Information Commissioner that the board members were officers of the centre and so their expense accounts would not normally be "personal information". However, in preparing the initial package, IDRC had provided more detail than was necessary—-menu selections, insurance policy numbers, the credit cards they held and—in one case—the member's American Express Card number.

This level of detail went beyond the requirements of public accountability. Having made the mistake, IDRC could not then withhold the names. The Privacy Commissioner accepted the notification and IDRC advised its board members of the release.

Policy and Research

Data matching

Electronic data processing poses its own threats to privacy. For example, the uncontrolled linkage of computer files could produce extensive dossiers on everyone, making a mockery of the collection restrictions set out in the Act.

To guard against this, the government introduced a data matching policy requiring that departments submit detailed proposals to the Privacy Commissioner 60 days in advance of linking databases.The policy, little more than a year old, applies a brake to untrammelled data linkage by ensuring that this independent agent (the Privacy Commissioner) weighs the proposals against a set of approved criteria. The Commissioner also acts as an advocate for those who may be affected by the match.

However, some departments seem to view the Commissioner's role as something of a rubber stamp to be applied after a last minute phone call. But Treasury Board's policy is clear — and the Commissioner's assessment is serious. Notifying the Commissioner when the system is on the launchpad will only frustrate everyone and cause delays.

This year the Commissioner's staff examined 11 proposals resulting from this policy. Following is a brief description of each match and the office's conclusions. Anyone wishing greater detail on these — or guidance on formulating their own proposals — should call the office.

Matching Employment and Immigration Canada Adjustment Assistance records with Toronto welfare files

Federal, Ontario and Toronto officials formed a committee to grapple with some of the problems caused by the increasing number of refugee claimants on Metro Toronto welfare rolls.

One of the problems was determining whether a refugee is receiving financial support from Employment and Immigration Canada's Adjustment Assistance Program. The program provides refugees with funds until they have sufficient income to support themselves or for one year, whichever comes first. Refugees benefitting from this program are ineligible for welfare.

The committee was concerned that, without some type of verification, both programs could be subject to fraudulent claims. Members agreed that EIC and Metro Toronto should share data to prevent such occurrences.

At first, EIC considered the match a "consistent use" and offered the Commissioner little substantiation. However, after a good deal of consultation, EIC provided a rationale and set out the legislative base for data sharing.

The Commissioner was satisfied but asked EIC to follow Metro Toronto's lead and tell applicants that the government agencies would verify their eligibility. He further asked EIC to add a notice and consent statement to the application forms as well as to assess whether the match reduced fraud cases enough to justify the action. EIC agreed.

External Affairs INFONNEL project

Last year's annual report said External Affairs had asked that the office examine its proposed new personnel management system which would incorporate smaller data bases into a single system with more sophisticated processing capabilities. The system would allow management to forecast, track and record all personnel actions.

Privacy staff became concerned that the proposed degree of integration might well exceed Treasury Board's approved uses of this type of database and that the proposal did not provide enough detail on system security. The staff concluded that the system design did not meet the requirements of either the *Privacy Act* or the government security policy.

Follow-up documents and discussions have failed to resolve the difficulties. Thus the office's audit branch will examine the system.

Agriculture Canada's Security Information System.

Agriculture Canada consulted the office on its plan to transfer some personal employee data from its human resource system to a security information system. Agriculture came to the office early in the process with a proposal for a "cleansing match"– one which simply verifies or updates a data base. The proposal set out the rationale for considering the transfer a "consistent use" and acted quickly to amend the bank descriptions to reflect the changes. In this example, Agriculture respected the policy and the result was a painless and speedy review.

The Personal Locator Beacon Registry

The office gave its seal of approval to a new Department of Communications system containing data on owners of "personal locator beacons". The devices are small, portable transmitters which campers, canoeists and hikers carry and activate in an emergency. The beacon transmits a radio signal to facilitate search and rescue.

Communications proposed to set up a voluntary registry containing such data as owners' names, addresses, type of vehicle and activity (land, marine or air) and next of kin. The registry, available to National Defence and the RCMP, will also be linked to DND and Transport Canada's joint search and rescue information system.

The registry is entirely voluntary and limited to this specific purpose. Participants sign a consent form and are told of the disclosures. Finally, all personal data will be stored in a newly-created personal data bank and listed in the **Info Source** guide.

Managers' new career counselling service

The office also had no difficulties with a Public Service Commission proposal to create a registry for its new confidential counselling service to help improve managers' skills.

The service is voluntary and within PSC's mandate. Participants provide the information directly and are told how it will be used. PSC will set up a bank to contain the data.

GST and SIN

A Revenue Canada notification on data linkages required by the GST has not been so clean.

Early in 1990, the Revenue minister advised the Commissioner that the GST program would involve some data matching and would use the social insurance number to register individuals and sole proprietorships. The minister assured the Commissioner that Revenue Canada took its clients privacy very seriously and promised a detailed submission "within the next few months".

Now, the legislation has been passed, detailed regulations have been adopted on sharing information and the use of SIN and still the Commissioner awaits the promised "detailed submission". In fact, only late in 1990 has the department begun to consider the data matching implications. This office has pressed for details but without success.

Fishing licence and vehicle match withdrawn

Fisheries and Oceans abandoned a project to step up fishing regulation enforcement by matching fishing licence holders with fishing vehicle permits. Fisheries withdrew the proposal when it became apparent that there was no legal justification for the match.

Immigrants' health records match

Health and Welfare Canada submitted a proposal to assess immigrants' overall health by linking its Immigration Health Services Records with provincial medical records.

The department proposed to extract statistical data only and promised not to use it for administrative purposes.

Technically this type of match does not require the Commissioner's review but the office appreciated being advised. Health care matches are a sensitive area which continue to worry the Commissioner.

Correctional Services' information gathering

CSC advised the Commissioner's office of a proposal to improve its gathering of "critical information" on persons about to be admitted to the penitentiary population. The need for better information became apparent after two recently-released federal inmates committed murders in Toronto.

When an inmate arrives at a federal facility, CSC requests information from the police, courts and various correctional and parole authorities. Agencies often do not give these requests high priority and CSC is left without critical information on which to determine the inmate's proper security level or the possibilities for parole. The problem is most acute in Metro Toronto.

As a result, CSC proposed contracting with former Toronto police officers to coordinate assembling the information.

The office examined these contracts to ensure that clauses covered contractors' collection and use of the personal information, that the collection procedure itself complied with the *Privacy Act* and that any information collected would be stored in a bank and made available to the individuals. CSC had taken all of these concerns into account.

The office noted that such release to provincial agencies might require review by the Commissioner's provincial counterparts. The staff also recommended that federal provincial agreements be drafted to cover the exchanges.

CIDA overseas student inventory

The Commissioner's office continues to struggle with a Canadian International Development Agency (CIDA) project to establish an inventory of CIDA-funded students from overseas.

CIDA's own files are organized by project or country, making it difficult to retrieve individuals' names and addresses. To solve this, CIDA proposed a tracking system that would link Employment and Immigration student authorization files which contain the information CIDA wanted. To accomplish this, it intended to send an employee to search the EIC files.

Despite privacy staff cautions that no legal authority could be found for the exchange, CIDA submitted a formal proposal. During discussions with Employment and Immigration it became apparent that their staff knew little about the proposal and — like privacy staff — could find no legal basis for this linkage. They also did not intend to comply.

As a result, CIDA asked for more consultation time and since then has submitted two different proposals. Examining the match did, however, reveal an oddity — CIDA lists no personal data banks for students and trainees in the **Info Source** guide. This was brought to the attention of Treasury Board which is responsible for ensuring government agencies comply with the *Privacy Act*.

Offsetting debts against income tax refunds

Probably one of the longest-standing data matching assessments concerns the government use of SINs to identify persons who owe money and to deduct the amounts owed from income tax refunds.

In June 1990, the Office of the Comptroller General proposed a research project to assess the usefulness of such a program to recoup some of the $800 million owed to the Crown for overdue student loans. The office agreed to a research match but held that deductions from tax refunds should not begin without legislative amendments.

The office also wanted to be assured that money would not be deducted solely on the basis of "a hit"— simply appearing on both lists. A principle of data matching schemes requires that there be some independent verification before taking any administrative action.

These differences of opinion remained unresolved by February 1991 when the government tabled its budget. It did mention changes to allow government to recover money owing from tax refunds.

Apparently individuals will be given fair warning and special care will be taken to ensure that the deductions from refunds will not cause undue financial hardship.

Nevertheless the office maintains that this type of debt collection will require legislative amendment and not simply the mandate of the *Financial Administration Act* or claims that such behavior represents either "consistent use" of the information, or disclosure "in the public interest".

Technology Marches On

Employment and Immigration (EIC) is at the forefront of applying new systems technology to its workplace. This fact is not surprising considering the department serves about 3,000,000 UI clients, receives some 40,000,000 claimants' reports and handles 31,000,000 inquiries each year.

Smart Cards

EIC has briefed our office on a pilot project to use "smart cards" for unemployment insurance clients. The cards resemble most bank or credit cards but are really mini computers containing 64K memory—as powerful as some of the early personal computers. Clients applying for benefits would use the card to report periods of unemployment through publicly available machines. EIC mainframe computers would then determine the claimant's eligibility, calculate the benefits and credit the payment onto the card. The claimant could then use the card to withdraw cash from an automatic teller machine or make purchases through retail direct debit machines.

The pilot project is expected to begin in two locations in the fall of 1991.

There are two clear privacy issues: ensuring that the correct person is accessing the system; and safeguarding against matching the data with other unrelated personal information.

Access appears to be controlled. Clients enter the system using a personal identification number (PIN) which they have selected. There are highly sophisticated internal security safeguards which EIC believes cannot be compromised. EIC will watch system security closely during the pilot project and brief the Commissioner.

The second concern, protecting against data linkage, has also been taken care of. Internal safeguards will prevent the card from being used for any other transactions and bank and retail machines will be limited to receiving the funds for the transaction.

However, EIC sees the single card eventually being used for as many as eight different applications. For example, cards could link the holder to an electronic job-search database describing available jobs which match their training and experience. Or they could be used to verify and pay training allowances and place the holder on training programs.

With so many possible functions, the cards could be useful for other government agencies or even private companies. EIC could sell them unused space for data or financial transactions. However, EIC recognizes that multiple uses would require segregation of the functions to prevent merging or cross-over of the data from one program to another.

Much of this project is still in the conceptual stage. EIC estimates it will take three to four years to start the UI program, another three to four years to implement and a total of 10 years for multiple applications.The scope of this project may require amendments to EIC legislation. Our office has suggested that any changes should focus on protecting the card and the transaction process, rather than simply authorizing its use.

EIC's new telephone inquiry system

The Commissioner's office remains concerned about Employment and Immigration's Automated Voice Response Enquiry System (AVRES). This pilot project allows touch telephone users to get general unemployment insurance information or details about their own claim over the phone. Callers use the phone keypad to select options and identify themselves by entering their social insurance number and date of birth. The technology permits computers to answer thousands of routine calls.

The office learned about the system when a Quebec City radio station asked us whether this was a proper use of SIN. There is no doubt that EIC can use the SIN—it was devised for the UI program. However, our office was concerned that individuals' SINs and dates of birth are so widely available that using them for identification does not restrict access to that individual.

Recognizing the weakness of SIN and date of birth, EIC looked at other solutions—client waivers, system recognition of the client's phone number or a client-chosen personal identification number (PIN), similar to bank card numbers. Although PINs appear to be the best solution, this would require a year for development and the pilot project was on the verge of launching into Ontario. With mounting internal pressure, Treasury Board approval and the system about to go to tender, EIC decided to proceed.

The Commissioner conceded that EIC was best suited to decide how to use technology to serve the public. However, he urged the department to hold off until more secure protections were in place, observing that EIC was courting the risk of embarrassment and, possible improper disclosure of a client's information.

Alas, it was too late—the project had already expanded to London and Peterborough. EIC believes the expanded pilots will enhance development and perfect a new security gate for the national system.

Consulting the Commissioner

The Commissioner's Office always welcomes opportunities to exchange information with those interested in the progress of privacy protection. Often such inquiries are outside the office's scope so it acts as a privacy clearing house, assembling material or referring inquiries to other sources. For example, research staff handled requests from Australia's new federal privacy commissioner for background on Canadian medical research guidelines, the application of federal data matching policy to law enforcement, security and intelligence data and Canada's experience with covert surveillance.

The Commissioner received other requests from down under as well. Privacy committees asked for the Commissioner's general assessment of the *Privacy Act* and his office's experience. The Australian electoral commissioner wanted information on Canadian legislative protection of whistleblowers (there is none) and Telecom Australia was interested in Canada's handling of caller ID and call management phone services, as well as codes of conduct for telecommunications companies.

The Hong Kong Secretary for Home Affairs, researching data protection legislation, needed information on registering computer systems and licensing data banks. Both these controls are features of some strict European data protection schemes—particularly the British Data Protection Act. They are not part of any Canadian legislation so his inquiry was referred elsewhere.

The Commissioner's staff also provided provincial counterparts with background information on

- federal data matching experience (Ontario);
- the privacy implications of linking health care and socio-economic records (Quebec).

The staff also assembled the latest federal material on informatics applications of government databases and a management framework for disseminating corporate affairs databases. This was in response to a request from the Ontario Ministry of Consumer and Commercial Relations for information on the privacy implications of public data bases.

The Royal Commission on New Reproductive Technologies asked the Privacy Commissioner for input on the privacy implications of the new reproductive techniques. The Commissioner intends to make a submission once the genetics study is complete, In the meantime, he welcomed the consultations.

Inquiries

Inquiries to the office continue to climb. Inquiries officers handled 4,032 calls and letters, compared with 3,447 the previous year—an increase of 17 per cent.

Fifty-five per cent of the inquiries concerned the use of or interpretation of the Act. Here are some examples: Canada Post employees asked whether they had to sign a consent to release their medical records to the employer; inmates questioned whether penitentiaries could open their mail; and Transport Canada's privacy office wanted to know whether a person's voice (on an audio tape) is considered personal information. In each case, the inquirers were referred to Treasury Board or the Department of Justice for interpretation.

The second largest inquiry category—17 per cent—comprised calls about privacy problems outside the Commissioner's jurisdiction. Four per cent of these inquiries concerned federal agencies and Crown corporations not covered by the Act. In one instance, a correctional officer was upset because he was shown on a CBC telecast. Apparently the cameraman had assured him he was not filming but simply adjusting the lens. The man worried that appearing on camera could endanger his life and that of other guards who are sometimes threatened by inmates. Since CBC is not covered by the Act, the office could offer no help.

The other 13 per cent of these inquiries were about other levels of government or—frequently—the private sector. For example: A woman called to enquire about a job application given her by the Canadian Imperial Bank of Commerce (CIBC). The form asked for consent to disclose personal information from credit agencies and former employers and included a statement that "permission includes my consent to the release of personal information concerning me within the meaning of subsection 8(2) of the *Privacy Act*".

This puzzled the Commissioner's staff on two counts:

- the banks are not subject to the Act; and
- section 8 says that government may not disclose personal information without the individual's consent.

The subsection cited describes the exceptions to the rule, none of which could be remotely interpreted as including release to prospective employers!

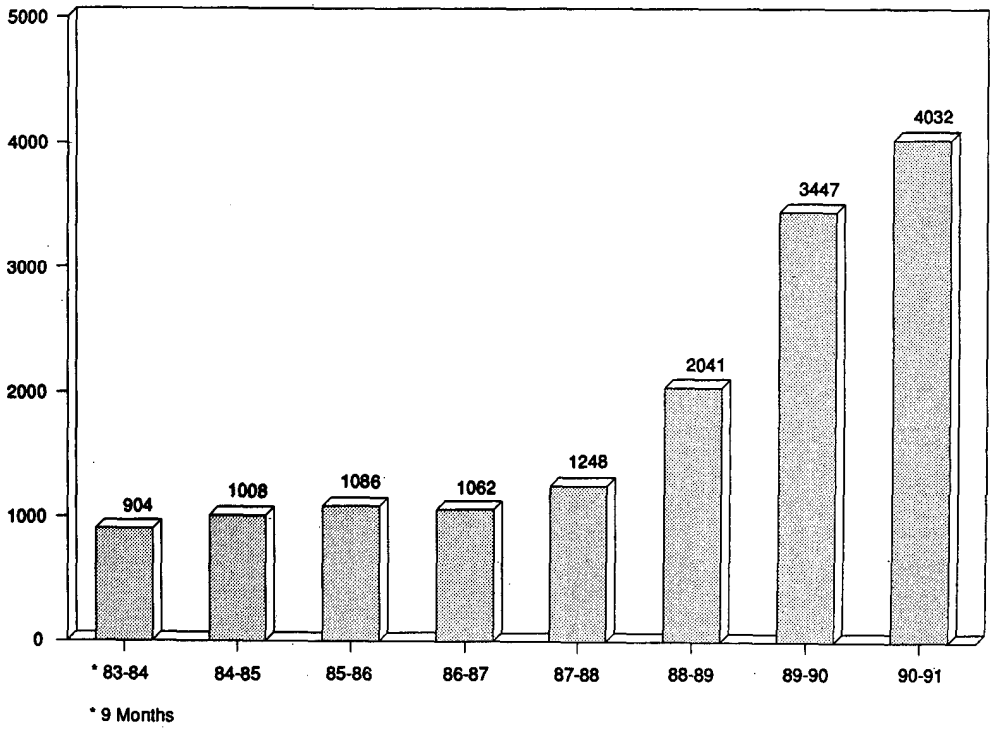
Staff concluded that the statement had no legal effect and did not dilute the protection of information held by the federal government. Legal counsels for both the office and CIBC discussed the consent, but, without jurisdiction, the Commissioner could not have the reference removed. And the bank has not apparently done so voluntarily since the office has received another complaint.

The most frequent Social Insurance Number (SIN) complaints (13 per cent of inquiries) cite insurance companies, video rental outlets, banks, grocery and department stores. Callers are amazed and unhappy that restrictions on uses of the SIN apply only to the federal government.

Several callers focused their anger on the Royal Bank's Gold Card application. The agreement requires applicants to consent to a blanket collection and disclosure of the SIN if they supplied it "in any application" to the bank. The office is inquiring whether opening a bank account (for which customers must supply a SIN under the Income Tax Act) is "an application".

Finally, eight per cent of inquiries were unrelated. A number of these deal with applying for a pardon and they are referred elsewhere. But many are from frustrated taxpayers who find in the office's toll-free line an opportunity to talk to a real person who works for "The Government".

Inquiries 1983-91



Compliance Directorate

The directorate's objectives for 1990-91 included auditing three major institutions, evaluating and improving the audit process and product, developing a privacy awareness component to audits and establishing an effective audit process for personal information held in electronic data processing (EDP) systems.

The office selected National Defence, the Royal Canadian Mounted Police and External Affairs, three institutions which hold the most sensitive and wide-ranging banks of personal information and operate some of the most sophisticated information handling systems in the country. While the war in the Persian Gulf and the Oka crisis at home had a serious impact on the success of the planned audit program, staff completed auditing the RCMP and DND and issued an interim report for External Affairs.

Due to the logistical problems and expense associated with international travel, the office has deferred its audit of External's overseas operation and the detailed review of its international information processing systems.

These agenda changes meant that the office could begin three smaller audits late in 1990; the National Capital Commission, the Office of the Comptroller General and the Commissioner of Official Languages. One of these, the Commissioner of Official Languages, was completed by year end.

The directorate now offers a "privacy awareness component" as part of its audits. Audit teams provide on-site presentations on the *Privacy Act* and have available two video cassettes which graphically illustrate the concerns pursued in the compliance audit. The videos are used only when the client institution chooses to become more informed.

All this year's investigations included an improved audit of information in computer systems. These new procedures and processes were used at DND, the RCMP and the Office of Comptroller General (OCG). In fact the OCG audit focussed entirely on EDP. Experience gained in these investigations will result in production of specific manuals and guides for this audit component.

The office was also involved in the following special investigations or projects:

- Cellular phone spectrum searching by the RCMP;
- CSIS establishment of an exempt bank;
- Indian Affairs and Northern Development (DIAND) internal audit;

- concerns about upward evaluation in Industry, Science & Technology and DIAND;

- the request for the release of Bell Canada technical information to the Criminal Intelligence Service of Ontario.

AUDIT FINDINGS

Royal Canadian Mounted Police

The audits to date have shown that the RCMP in particular has made a concerted effort to ensure that it complies with the *Privacy Act*. It has made privacy considerations a high priority, undertaking periodic information sessions at all levels and introducing training on the *Privacy Act* as part of the curriculum both for new recruits and officer trainees.

Although auditors found instances where personal information holdings were not adequately described in the Personal Information Index (now **Info Source**), these were due either to oversights or to descriptions not keeping pace with changes in operating procedures.

Some records containing personal information were not being disposed of in accordance with approved schedules and Privacy Regulations. This was particularly true with the disposal of performance logs (a type of manager's diary to record employees' daily performance). The logs were the subject of numerous meetings between privacy staff and RCMP privacy personnel, all seeking a solution that would satisfy both the privacy requirements and the force's administrative needs.

The audits found some instances of personal information not being adequately protected against unauthorized disclosure. The most serious involved the Victims Assistance Program where auditors found that volunteer counsellors have been given access to complete investigation files.

Two areas of particular interest examined during the RCMP audit were facsimile (FAX) transmission and using micro-computers to handle personal information. It is a pleasure to report that the RCMP has specific policies and procedures on transmitting personal information by FAX and handling it by micro-computer. These controls ensure that sensitive personal information is transmitted only through the RCMP's own secure communications facilities. Auditors inspected a number of computer systems and found evidence that the personal information they contained was properly protected.

National Defence (DND)

The office has reported its detailed findings to National Defence and is awaiting management's response. The practice is not to describe audit findings publicly until staff have had an opportunity to examine the department's comments and discuss any areas that may be in dispute.

Other audits

Other audits disclosed that retention and disposal standards are not always upheld or are inadequate. There was evidence that personnel files are not generally disposed of on time and some personal information banks have indefinite retention periods. Some third party information, which could be inadvertently disclosed, is found on personnel files. Sensitive and inappropriate information is often found on some personnel files and the need-to- know principle is not in place in most institutions. The security for personal information held by many institutions is inadequate, while descriptions for many information banks are inaccurate.

In fairness, however, most personnel expressed interest not only in the audit objectives but also in the proper application of the *Privacy Act* throughout their institutions. In a number of cases staff corrected problems before the privacy investigators left.

Among smaller institutions with fewer resources to spend on applying the Act, there tend to be greater opportunities for inappropriate handling of personal information. Policies and procedures tend to be out of date or absent and general knowledge of the Act is consistently lower than in the major departments. The security of personal information collected by these institutions is usually at risk.

So it is refreshing to report on a smaller institution which generally handles personal information in accordance with the *Privacy Act.*

Office of the Commissioner of Official Languages

Throughout the audit of the Office of the Commissioner of Official Languages it was evident that although most employees had only a cursory knowledge of the *Privacy Act*, all had a high degree of concern for the proper management of personal information. Auditors agreed that this concern reflected the provisions in the *Official Languages Act* dealing with the confidentiality of complaint investigations.

Yet, there were instances of personal information not being adequately protected against unauthorized disclosure and in one case, the computer system's security features had been rendered inadequate due to improper administration and protection of passwords.

Common findings

Overall, some of the most common observations in all audits were:

Inadequate protection of personal information

- Managers, supervisors and other employees are allowed to see personnel files for routine administrative purposes. Records staff have access to their own and each others' personnel file, allowing them to see sensitive personal information for which they have no "need-to-know". (e.g. - Personal History Forms, results of credit and reference checks, medical diagnosis, details of family members, designation of beneficiary, Canada Savings Bonds purchases, United Way contributions, etc.)

- Some files contained a limited amount of third-party personal information, usually when the subject's name is on a list with other employees, often including everyone's Social Insurance Numbers.

- Usually personal information handled by microcomputers is not adequately protected either by external security provisions (keyboard locks, hard disc protection, etc.) or internal protection (accounts, IDs, passwords, partitions, backup, etc.).

- File jackets tend to bear the particulars of an individual along with the caption of the file. This is especially pertinent where the file relates to investigations, complaints or special requests. For example, one personal file jacket included notations about a sexual harassment allegation, including the victim's name. The information was clearly visible to mail clerks or anyone who saw the file on a desk.

Improper disclosure of personal information

- Personnel records often contain documents that should have been purged from the file or retained on other files. Individuals' medical information and security-related material are found in up to 10 per cent of the records sampled.

Misuse of personal information

- Information properly collected for specific purposes is sometimes used for follow-on purposes (e.g. personal harassment files used for grievance and discrimination cases).

Improper retention and disposal

- Many banks have improper retention and disposal schedules and proper schedules are not being maintained.

Corporate Management

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

Finance

The Offices' total resources for the 1990-91 fiscal year were $6,372,000 and 78 person-years, an increase of $567,905 and three person-years over 1989-90. Personnel costs of $4,897,442 and professional and special services expenditures of $577,300 accounted for more than 87 per cent of the total. The remaining $852,060 covered all other expenses.

The following are the Offices' expenditures for the period April 1, 1990 to March 31, 1991*

	Information	Privacy	Corporate Management	Total
Salaries	1,685,327	1,856,590	652,525	4,194,442
Employee Benefit Plan Contributions	288,230	323,380	91,390	703,000
Transportation and Communication	38,141	114,167	123,309	275,617
Information	84,446	58,546	5,549	148,541
Professional and Special Services	411,801	130,150	35,349	577,300
Rentals	3,952	2,214	11,413	17,579
Purchased Repair and Maintenance	14,628	3,919	9,676	28,223
Utilities, Materials and Supplies	9,847	14,978	30,655	55,480
Acquisition of Machinery and Equipment	176,236	51,508	85,672	313,416
Other Payments	6,145	3,475	3,584	13,204
TOTAL	2,718,753	2,558,927	1,049,122	6,326,802

* Expenditure figures do not incorporate final year-end adjustments reflected in the Office's 1990-91 Public Accounts.

Personnel

An increase of three person-years and a change of both the Privacy and the Information Commissioners contributed to an active personnel program. There were 45 staffing actions, including outside recruitment, promotions, the hiring of term employees and some reclassifications.

Administration

New space was fitted-up for occupancy in the fall of 1990 and some progress was achieved in the records management area, particularly in the scheduling of administrative records.

Informatics

A new information technology was introduced to the organization. Three studies were undertaken concerning case management systems, additional office automation and networking in a secure environment. These studies will be completed in 1991-92 and will provide the necessary information to form a long-term information technology plan.

Library

The library provides services to the Information and the Privacy Commissioners. It is a resource centre for both the Information and Privacy staffs which is also open to the public.

A total of 436 books, periodicals, and annual reports were acquired through the Government Depository Services program. There were 835 items loaned and 847 reference questions answered. The automation of library functions was completed this year.

Organization Chart