Privacy Commissioner of Canada

Commissaire à la protection de la vie privée du Canada

Privacy

Annual Report

to Parliament 2002-2003

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

(613) 995-8210, 1-800-282-1376
Fax (613) 947-6850
TDD (613) 992-9190

Cat. No. IP30-1/2003
ISBN 0-662-67544-4

This publication is also available on our Web site at **www.privcom.gc.ca**

Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

Commissaire à la protection de la vie privée du Canada
112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél. : (613) 995-8210
Téléc. : (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

September 2003

The Honourable Daniel Hays, Senator
The Speaker
The Senate of Canada
Ottawa

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report for the Office of the Privacy Commissioner of Canada, for the period from April 1, 2002 to March 31, 2003 for the *Privacy Act* and from January 1 to December 31, 2002 for the *Personal Information Protection and Electronic Documents Act*.

Yours sincerely,

Robert Marleau
Interim Privacy Commissioner
of Canada

Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

Commissaire à la protection de la vie privée du Canada
112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél. : (613) 995-8210
Téléc. : (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

September 2003

The Honourable Peter Milliken, M.P.
The Speaker
The House of Commons
Ottawa

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report for the Office of the Privacy Commissioner of Canada, for the period from April 1, 2002 to March 31, 2003 for the *Privacy Act* and from January 1 to December 31, 2002 for the *Personal Information Protection and Electronic Documents Act*.

Yours sincerely,

Robert Marleau
Interim Privacy Commissioner
of Canada

Table of Contents

Foreword

My presenting this Annual Report for the fiscal year 2002-2003 may seem something of an oddity. I was appointed interim Privacy Commissioner in July of this year, well past the end of the reporting period, so I cannot take credit for any of the work that is reported here. But in fact this is less a real problem than it might seem. There is a lot more to the Office of the Privacy Commissioner than just the Commissioner, and even if I had been here for the entire time, it would be a fiction to call this "my" Annual Report. It reflects the work of very talented and dedicated individuals.

These are challenging times for the Office. For one thing, the task of protecting privacy has never been more arduous, what with new private sector legislation, a wide array of proposed anti-terrorist and security measures, and the increasing availability and sophistication of privacy-invasive technologies.

To complicate matters, the Office has undergone a period of intense public scrutiny and organizational disruption. The House of Commons Committee on Government Operations and Estimates conducted an inquiry into operational and administrative issues in the Office, and uncovered a number of

serious problems. As important and necessary as this exercise of Parliamentary oversight is, there is no denying that it, along with the accompanying media attention, has made it difficult for staff of the Office to conduct their work effectively.

I accepted the position of Privacy Commissioner on an interim basis in order to lead the Office through the process of rebuilding itself and repairing its relationship with Parliament and Canadians. Our task now is to regain the confidence of Parliament and our stakeholders, demonstrate to Canadians that they will receive top-level service in protection of their privacy rights, and ensure that organizations understand their obligations, and citizens their rights, when the *Personal Information Protection and Electronic Documents Act* comes fully into effect on January 1, 2004.

I have been impressed by the commitment of the Office's staff, and look forward to working with them in this exciting time. I am confident that from this period of renewal will emerge a new enthusiasm for the cause of privacy and a centre of excellence for its protection and promotion.

Overview

It is common to introduce an Annual Report with some remark about it providing an opportunity to reflect. In the case of this Report, that is not simply a throwaway introduction. The period under review has been an important one for privacy.

For one thing, privacy in our society has been in some danger. This of course is nothing new; privacy has never been something that we can take for granted, and particularly since the advent of computerization it has required active effort to preserve it. But if the danger to privacy is not new, it is intensified. The forces that have ground away at privacy for the last decade—technological advances in the collection, processing, matching, and analysis of personal information, growing pressure to identify and authenticate parties to electronic transactions, and the drive for security from crime and terrorism—have been particularly powerful in the last year.

Public security measures against crime and terrorism have certainly been the most acute and obvious challenge. They also present the most obvious challenge to privacy advocates and Privacy Commissioners, who must walk a fine line between protecting privacy and making life easier for criminals and terrorists.

But in fact the other forces threatening privacy are no less challenging, and arguing for privacy in the face of them often requires walking similar fine lines. Data matching catches people defrauding the system. Identity cards can make it harder for someone to fraudulently use your credit card. Electronic health records can facilitate diagnosis and treatment, and prevent costly or deadly medical mistakes. Giving researchers access to our personal health information can enable research that can prolong life and reduce suffering.

No one would argue with the goals of these measures. But privacy is not simply a frill or a selfish extravagance that can be tossed away the moment someone claims that it inhibits some other valuable social goal—regardless of whether the goal is security or public health or even individual life or death. Privacy is a cornerstone of individual freedom. It exists in a dynamic balance with our other social needs. The key to preserving privacy is careful analysis of any measure that purports to bring us some other social benefit, to ensure that the balance is maintained.

The results of our work in the past year have been mixed. We have continued to manage a large caseload of complaints and ensure that Canadians enjoy full protection of their rights under the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*. On more general questions of promoting and protecting privacy, we have made some important advances. We have also had some setbacks, and, on a couple of fronts, we have been forced to rethink our approach.

The Office achieved a successful outcome when it spoke up about the Canada Customs and Revenue Agency's proposed database about airline passengers.

This database, as initially proposed, was to contain extensive information on the foreign travel activities of Canadians—where

On more general questions of promoting and protecting privacy, we have made some important advances.

and with whom they travel, how they paid for their tickets, their contact addresses and telephone numbers, even their dietary and health-related requirements. The information would have been retained for seven years, and would have been available for a wide range of administrative and law enforcement purposes.

The impact of this would have been enormous, and unprecedented. The ordinary travel activities of law-abiding people, activities that previously would have passed unnoticed unless there were some reasonable grounds to suspect them, would have been recorded and retained, attached to their names. It would be one more loss of anonymity and privacy, one more way in which innocent people would be identified, tagged, and monitored by the state—in short, one more infringement of the right to privacy.

Our staff analyzed this proposal and concluded that the supposed security benefits to be gained did not justify the infringement of privacy that it represented. Our opposition, supported by public opinion, eventually led the Minister of National Revenue to revise the initiative, significantly reducing the impact on privacy.

One successful outcome does not make a great year. We continue to have concerns about other security initiatives, such as the provisions of the proposed *Public Safety Act* allowing the police to scan all airline passengers against outstanding arrest warrants, the "Lawful Access" proposals to enhance state powers to monitor electronic communications, the proposal for a national identification card, and the growth of police video surveillance of public streets.

One long-running dispute, about the confidentiality of census returns, appears headed for resolution in a manner that runs directly counter to the recommendations of our Office.

Canadians have been told at least since 1905 that the information they reveal in censuses will be held in confidence and only used for statistical purposes. The *Privacy Act* actually allows the National Archives to disclose personal

information collected in a census, 92 years after the information was collected. This remained largely academic until recently, because the only census records under the control of the Archives were those few that had been conducted up until 1901. Census officials took the view that, beginning with the 1906 census, regulations and legislation required them to keep the returns confidential rather than transfer them to the Archives.

Historians and other researchers have long sought access to these documents, and this year the government, following the recommendations of an expert panel but over our objections, released the 1906 census records and introduced legislation to allow the release of the rest.

Our Office had supported a compromise that would have limited access to the returns to scholars conducting peer-reviewed historical research and individuals wishing to conduct genealogical research on their own families. The government rejected this.

Our concern is with the repeated promises of confidentiality. Canadians were asked to reveal personal information to census-takers, and were led to believe that it would be kept confidential. Violating that promise could diminish the confidence Canadians have in government. We remain hopeful that this will be recognized when the House of Commons takes up this proposed legislation, which was passed by the Senate in May.

On another important privacy issue, video surveillance of public streets, we concluded that a new approach needs to be taken. The previous Commissioner had initiated a lawsuit in the British Columbia Supreme Court, alleging that the RCMP's video surveillance of a public street in Kelowna, B.C., violated the *Canadian Charter of Rights and Freedoms*. The Court, however, did not address the substance of the case at all. It ruled that the Privacy Commissioner simply does not have the capacity to launch such an action, and dismissed it on that basis.

This presented us with something of a quandary. On the one hand, video surveillance of public places has serious privacy implications, so the idea of simply

letting the issue drop because of a procedural problem seemed hardly satisfactory. On the other hand, regardless of what we wanted, the issue had become the one defined by the Court. If we had appealed the decision, the appeal would have been about that issue alone. To work our way through two more levels of appeal would have taken years, at the end of which we would have spent a great deal of the Office's energies and a considerable amount of public money, without any answer from a court on the substantive issue of video surveillance. The issue has to be addressed, but it must be done in a different way. Accordingly, we withdrew the case, but we will pursue this issue with determination.

It was striking this past year how many of our privacy concerns are tied up with anonymity and its opposite pole, identity.

It was striking this past year how many of our privacy concerns are tied up with anonymity and its opposite pole, identity. The ability to conduct the majority of our daily activities in an anonymous fashion is one of the keys to our keeping control of information about us. People can have a private life even if much of their lives is spent in public view, as long as their activities cannot be linked to each other and to themselves. It is the ability to connect activities to each other and to an identifiable person that is at the heart of profiling and surveillance.

This perspective ties together our concerns about such superficially different things as authentication of clients in electronic transactions, biometric facial recognition systems in airports, traveller databases, and a national identification card.

This was the view that we tried to impress upon the House of Commons Standing Committee on Citizenship and Immigration in its hearings on whether Canada needs a national identification card. We made the argument that such a card (whatever the details of the proposal are, and to date there is

no real proposal) would do little to address real problems, would present enormous financial and practical challenges to implement, and would do grave damage to privacy.

While the Office has wide-ranging interests and strives to serve as Parliament's window on all privacy issues, the heart and soul of its work is the system of enforceable privacy rights set up under the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*.

On this account, 2003 was a noteworthy year. First of all, it marks the 20th anniversary of the *Privacy Act*. That calls for reflection not just on the past year, but on the past twenty, and in particular on the model of privacy protection that Parliament adopted with the *Privacy Act*. That model is based around an Officer of Parliament, the Privacy Commissioner, who advises Parliament on privacy issues, analyzes the implications of legislative and regulatory initiatives so that Parliamentarians and Canadians can make informed decisions, and acts as an ombudsman to protect privacy rights, through negotiation, persuasion and dialogue—and occasionally, as a last resort, through publicity. The system set up under the *Privacy Act* quickly showed itself to be a useful one, and it was no surprise that it was adopted and applied to the private sector when Parliament passed the *Personal Information Protection and Electronic Documents Act*.

We are confident that in the past year, this system has proved useful to Parliament, and indeed has been reaffirmed. Parliament has rethought and revised legislative initiatives such as the CCRA database so as to minimize impacts on privacy, and we think that the outlook for privacy in Canada, despite all the pressures, is encouraging.

The year 2003 is important for the other statute we administer, the *Personal Information Protection and Electronic Documents Act* or *PIPED Act* as we call it, since this is the last year before it reaches its full application. The Act has been coming into force in stages. At the outset, in 2001, it applied to certain commercial exchanges of information but excluded personal health information. As of January 2002, it extended to include personal health information. The

final stage will begin in January, 2004, when the Act will apply to all commercial activity in Canada except where provinces have passed substantially similar legislation. (To date, only Quebec has privacy legislation deemed substantially similar, but both British Columbia and Alberta introduced legislation this year, another promising sign for privacy protection in Canada.)

In general, the introduction and implementation of the Act have gone far more smoothly than some had predicted. The business community has responded well to the demands of complying with the legislation, and while there have been some bumps in the road, on the whole the new way of doing business has not been as difficult or traumatic as some had predicted. We are seeing a general recognition that respecting privacy is not as onerous as some people thought, and in fact is simply good business practice. One of the most encouraging signs is the obvious interest in compliance among the business community. In fact, a sort of compliance cottage-industry has sprung up, with a host of consulting firms offering expertise in compliance with the Act. Hardly a week goes by without our receiving a brochure for a seminar or workshop about the *PIPED Act*.

And the ombudsman model, which proved itself under the *Privacy Act*, has also worked well with respect to the *PIPED Act*. We have been encouraged by the willingness of private sector organizations subject to the Act to comply with the requirements in the legislation and to recognize the Office's specific expertise in getting to the bottom of privacy issues.

We are seeing a general recognition that respecting privacy is not as onerous as some people thought, and in fact is simply good business practice.

As far as day-to-day operations are concerned, the Office continued to face significant challenges, but it remains a resilient and healthy organization in the face of heavy public demand for its services. We

dealt with a heavy caseload of complaints under the *Privacy Act*, including a 35% increase in new complaints over last year. Under the *PIPED Act*, the number of new complaints almost tripled over last year, and we can expect a significant increase with the extension of the application of the Act in 2004.

An important development in the past year was the introduction of the Treasury Board's new policy on privacy impact assessments.

A privacy impact assessment, or PIA, is quite simply an assessment of how, and how much, a program or activity affects the privacy of individuals. Typically, it will entail a description of the program, an analysis of what will happen to the personal information collected, used, and disclosed, and an assessment of the program's compliance with privacy principles, legislation, and policies. The Treasury Board's new policy makes PIAs a condition of funding for all new, substantially redesigned, or electronically driven programs and services that collect, use, or disclose personal information. Canada is the first country in the world to make PIAs mandatory in this way.

The implementation of this policy means that government institutions will have to look at privacy right from the outset, from the moment they begin planning a new program. The significance of this is that questions of whether a program or project has a negative effect on privacy—whether it will entail new data matching or increased sharing of personal information, for example, or result in the development of new common personal identifiers, or extended use of existing ones—will be asked before any privacy violation occurs. This preventive approach, rather than a punitive or remedial one, is the most sensible approach to an issue like privacy. Once privacy is violated, once an individual's personal information has been taken out of his or her control, it cannot be undone. Lost privacy cannot be given back. That is why Treasury Board's policy is so

So it has been a year of some good news, some disappointments, and many continuing challenges.

welcome. When government initiatives add to sound governance, it should be recognized and applauded.

So it has been a year of some good news, some disappointments, and many continuing challenges. Fortunately, we have not had to face all our challenges alone. The protection of privacy involves us in a continuing dialogue, in Canada and abroad, with privacy advocates, civil libertarians, academics, and, of course, other privacy and data protection commissioners. They have helped us to bear the burden of the disappointments, and they deserve full credit for their part in bringing about the good news.

The Standing Committee on Government Operations has done its duty in holding this Office accountable to higher standards of prudence and probity in the use of public funds. As we move forward in another watershed year for privacy issues, the Office of the Privacy Commissioner will work for renewed support from the Senate and the House of Commons to blunt the impact of pervasive and invasive technologies and policies on the privacy rights of Canadians.

Substantially Similar Provincial Legislation

Under paragraph 26(2)(b) of the *Personal Information Protection and Electronic Documents Act*, the Governor in Council can exempt an organization, a class of organizations, an activity or a class of activities from the application of *PIPED Act* with respect to the collection, use or disclosure of personal information that occurs within a province that has passed legislation deemed to be substantially similar to the *PIPED Act*.

The intent of this provision is to allow provinces and territories to regulate the personal information management practices of organizations operating within their borders, provided that they have in place a law that is substantially similar.

If the Governor in Council issues an Order declaring a provincial act to be substantially similar, the collection, use or disclosure of personal information by organizations subject to the provincial act will not be covered by the *PIPED Act*. Personal information that flows across provincial or national borders will be subject to the *PIPED Act* and the *PIPED Act* will continue to apply within a province to the activities of federal works, undertakings and businesses that are under federal jurisdiction such as banking, broadcasting, telecommunications and transportation.

On September 22, 2001, Industry Canada published a notice in the *Canada Gazette* Part 1 setting out the process that the department will follow for determining whether provincial/territorial legislation will be deemed substantially similar.

The process will be triggered by a province, territory or organization advising the Minister of Industry of legislation that they believe is substantially similar to the *PIPED Act*. The Minister may also act on his or her own initiative and recommend to the Governor in Council that provincial or territorial legislation be designated as substantially similar.

The Minister has stated that he will seek the Privacy Commissioner's views on whether or not legislation is substantially similar and include the Commissioner's views in the submission to the Governor in Council.

The process also provides for an opportunity for the public and interested parties to comment on the legislation in question.

According to the *Canada Gazette* notice, the Minister will expect substantially similar provincial or territorial legislation to:

- incorporate the ten principles in Schedule 1 of the *PIPED Act*;
- provide for an independent and effective oversight and redress mechanism with powers to investigate; and
- restrict the collection, use and disclosure of personal information to purposes that are appropriate or legitimate.

The process also provides for an opportunity for the public and interested parties to comment on the legislation in question.

In addition to providing comments to the Minister of Industry with respect to specific provincial or territorial legislation, the

Privacy Commissioner is required by subsection 25(1) to report annually to the Parliament of Canada on the "extent to which the provinces have enacted legislation that is substantially similar to the *PIPED Act*."

The previous Commissioner issued two reports to Parliament on the matter of substantially similar provincial legislation. In May 2002, he issued a report in which he concluded that Quebec's *An Act Respecting the Protection of Personal Information in the Private Sector* is substantially similar to the *PIPED Act* in terms of the extent to which it protects personal information. In June 2003, the previous Commissioner issued a second report in which he raised concerns about Bills 44 and 38 that have been introduced, but not yet passed, by the provinces of Alberta and British Columbia, respectively.

As neither Bill has been passed, we will continue to monitor their progress and maintain a dialogue with our provincial counterparts.

Part One

Report on the *Privacy Act*

INTRODUCTION

The *Privacy Act*, which has been in force since 1983, protects individuals' privacy with respect to personal information held by federal Government institutions. The *Act* governs how federal institutions collect, use, disclose and dispose of personal information, and it gives individuals rights to request access to and correction of their personal information. It also sets out the Privacy Commissioner of Canada's duties, responsibilities and mandate.

The Privacy Commissioner receives and investigates complaints from individuals who believe their rights under the *Act* have been violated. The Commissioner can also initiate a complaint and investigation himself, in any situation where there are reasonable grounds to believe the *Act* has been violated.

As an ombudsman, the Commissioner's first priority is to resolve complaints to the extent possible, through mediation and negotiation if that becomes necessary. But the *Act* also gives the Commissioner broad investigative powers – he can subpoena witnesses and compel testimony, enter premises to obtain documents and conduct interviews. Obstructing an investigation is an offence under the *Act*. While the *Act* does not grant the Commissioner any order-making powers, the Commissioner can recommend changes to the way

Government institutions handle personal information, based on findings in a complaint.

The Commissioner also has a mandate to conduct periodic audits of federal institutions and to recommend changes to any practices that he considers not being in compliance with the *Privacy Act*.

The *Act* requires the Commissioner to submit an Annual Report to Parliament on the activities of his Office in the previous fiscal year. The current Report covers the period from April 1, 2002 to March 31, 2003 for the *Privacy Act*.

INVESTIGATIONS AND INQUIRIES

The Office's Investigations and Inquiries Branch is responsible for investigating complaints received from individuals under section 29 of the *Privacy Act* (and section 11 of the *Personal Information Protection and Electronic Documents (PIPED) Act*, which is discussed later in this Report).

Essentially, these investigations serve to establish whether individuals have had their privacy rights violated and whether they have been accorded their right of access to their personal information.

Where privacy or access rights have been violated, the investigation process seeks to provide redress for individuals and prevent violations from reoccurring.

The *Privacy Act* gives the Commissioner the authority to administer oaths, receive evidence and enter premises where appropriate, and examine or obtain copies of records found in any premises.

We are pleased to note that we have had voluntary co-operation to date, and all complaints brought before the Commissioner and his predecessors have been resolved without having to use these formal investigative powers.

The Investigations and Inquiries Branch also responds to thousands of inquiries annually from individuals and organizations contacting the Office for advice and assistance on a wide range of privacy-related matters.

Complaint Investigations Closed
April 1, 2002 to March 31, 2003

2001-2002:	1,673
2002-2003:	3,483

COMPLAINTS UNDER THE *PRIVACY ACT*

During the current reporting year, this Office received 1,642 new complaints. Approximately 43% were filed by individuals alleging that their access rights under the *Privacy Act* had been violated; 24% concerned allegations that the confidentiality provisions of the *Act* with regard to collection, use, disclosure, retention and disposal of personal information had not been respected; and the remaining 33% were about the tardiness of Government institutions in responding to requests for access to personal information.

More than two-thirds of the total received were lodged against five federal Government institutions – Correctional Service of Canada, the Canada Customs and Revenue Agency, the Royal Canadian Mounted Police, the Department of National Defence, and Citizenship and Immigration Canada.

The former Commissioner issued findings on 3,483 complaints during the year. It is important to note that this figure includes 2,323 complaints related to the Canada Customs and Revenue Agency's (CCRA) disclosure of personal information on Customs' E-311 declaration cards to Human Resources Development Canada (HRDC).

At issue was whether there was sufficient authority to justify the use of personal information collected by the CCRA for one purpose – to declare goods

a traveller is bringing into Canada – for use by HRDC for a totally unrelated purpose – in an investigative data match program to identify returning travellers who were fraudulently receiving employment insurance benefits while outside the country.

The matter had been referred to the Court for an opinion on whether the disclosure was authorized by section 8(2)(b) of the *Privacy Act* and section 108 of the *Customs Act* and whether the use of that information by HRDC as evidence against the individuals contravened their rights under the *Canadian Charter of Rights and Freedoms*.

The Supreme Court of Canada ruled that the disclosure was permissible based on its interpretation of these provisions of the *Privacy Act* and the *Customs Act*. The Court also upheld the lower Court's decision that, based on the limited nature of the information disclosed, there was no reasonable expectation of privacy and as a consequence travellers had not been denied their right under the *Charter* to be secure from unreasonable search or seizure. On that basis, the former Commissioner was required to report to the complainants that their complaints were not well-founded.

Of the remaining 1,160 completed cases, 486 dealt with access matters, 293 dealt with collection, use, disclosure, retention and disposal of personal information, and 381 dealt with time limits. The 3,483 complaints were concluded as follows:

Not well-founded	2,711
Well-founded	371
Well-founded/resolved	77
Resolved	13
Settled	235
Discontinued	76

DEFINITIONS OF FINDINGS UNDER THE *PRIVACY ACT*

Not Well-founded: A finding that a complaint is *not well-founded* means that the investigation uncovered no evidence to lead the Commissioner to conclude that the Government institution violated the complainant's rights under the *Privacy Act*.

Well-founded: A finding that a complaint is *well-founded* means that the Government institution failed to respect the *Privacy Act* rights of an individual. This would also be the Commissioner's finding in a situation where the Government institution refuses to grant access to personal information, despite our recommendation that it be released. In such a case, the next step could be to seek a review by the Federal Court of Canada.

Well-founded/Resolved: The Commissioner will find a complaint to be *well-founded/resolved* when the allegations are substantiated by the investigation and the Government institution has agreed to take corrective measures to rectify the problem.

Resolved: *Resolved* is a formal finding that reflects the Commissioner's role as an ombudsman. It's for those complaints where *well-founded* would be too harsh to fit what essentially is a miscommunication or misunderstanding. It means that this Office, after a full and thorough investigation, has helped negotiate a solution that satisfies all the parties.

Settled during the Course of the Investigation: This is not a formal finding but an acceptable means to dispose of a complaint when the investigation is completed, and the complainant is satisfied with the efforts of this Office and doesn't wish to pursue the issue any further. The complainant retains the right to request a formal finding. When that happens, the investigator reopens the file, and submits a formal report, and the Commissioner reports the findings in a letter to the complainant.

Discontinued: This means that the investigation was terminated before all the allegations were fully investigated. A case may be *discontinued* for any

number of reasons – for instance, the complainant may no longer be interested in pursuing the matter or cannot be located to provide additional information critical to reaching a conclusion. The Commissioner does not issue a formal finding in discontinued complaints.

SUMMARY OF SELECT CASES UNDER THE *PRIVACY ACT*

CIC was collecting income tax information from Canadian employers

Three individuals who wished to employ live-in caregivers from the Philippines complained to this Office that the Canadian Embassy in Manila was asking them to provide sensitive income tax information before it would issue visas to their prospective caregivers. The individuals were worried about sending tax documents containing their social insurance numbers (SINs) and detailed information about their financial situation to a foreign country, especially with identity fraud having become such a major concern.

Citizenship and Immigration Canada (CIC) explained that the Live-In Caregiver Program (LCP) brings qualified caregivers to Canada in situations where there are no Canadians or permanent residents available to fill certain positions. Canadians wishing to hire a caregiver from abroad are required to have their job offer validated through Human Resources Development Canada (HRDC) and to sign a form declaring that they can financially support the person they will employ.

After the job offer was validated by HRDC, the Visa Section of the Canadian Embassy in Manila asked the prospective employers to send their Notice of Assessment for the last two years, their T-4 slips and a letter from their employer confirming employment.

CIC claimed that the information was necessary to determine the *bona fides* of an employment offer and to confirm that the employers were financially capable of supporting a caregiver.

When questioned about its authority to collect income tax information for the purpose of issuing visas to third parties, CIC referred to section 203 of the *Immigration and Refugee Protection Regulations*. A review of that document indicated that the visa officer must determine if the job offer is genuine and if the employment of the foreign national is likely to have a neutral or positive economic effect on the labour market in Canada.

In the previous Annual Report, the former Commissioner stated his position concerning the collection of income tax information without legislative authority. He explained that he found it untenable that an income tax return can be demanded from an individual for a purpose other than that required by law. Canadians should never be required to compromise a fundamental right in order to do business with the Government.

This Office presented those arguments to CIC and, as a result, the Embassy in Manila confirmed that it has ceased asking for income tax information for the purpose of issuing visas to live-in caregivers.

CCRA collected medical information for tax purposes

We received a complaint from a family who alleged that the Canada Customs and Revenue Agency (CCRA) had improperly collected their personal information from a provincial medical insurance plan. The family moved to Africa for three years and before leaving Canada the husband consulted with the CCRA and was told that, for tax purposes, he would be considered a non-resident during his absence from the country. Yet upon returning to Canada he was told that he did not meet the requirements for non-resident status and was taxed accordingly. He later obtained his personal information following a *Privacy Act* request to the CCRA and learned that it had asked the provincial insurance provider for all medical records about him, his wife and his children—including records originating some eight months prior to their departure for Africa and almost 2 1/2 years after their return to Canada.

We established that in order to qualify for non-resident status for tax purposes the CCRA must be satisfied that an individual has sufficiently severed ties

with Canada after moving to another country. The CCRA relies on provisions of the *Income Tax Act* as its authority to obtain sufficient information in order to assess non-residency status. It routinely conducts inquiries when assessing an individual's status, including verifying whether the individual continues to make claims under a provincial medical insurance plan during the time absent from Canada. The fact that an individual made such a claim could be an indication that all ties with Canada had not been severed.

The former Commissioner was satisfied that the CCRA had the necessary authority under the *Income Tax Act* to collect personal information about each family member from the province in order to make a determination on their residency status. Nevertheless, he was concerned about the *extent* of the medical information collected, particularly the information for the periods of time both before the family left the country, and after it returned. CCRA officials did not disagree with the concern that requesting medical information for the 2 1/2-year period after the family's return was excessive.

Under the circumstances, the former Commissioner determined that the CCRA collected more personal information than was necessary and, as a result, had exceeded its authority under section 4 of the *Privacy Act*. He found the complaints well-founded and recommended that the CCRA destroy the information that it obtained from the province.

Inadvertent disclosure of sensitive medical information by ATIP

Personal health information – information about the state of our bodies and minds – is arguably the most private information of all. When that information is not treated with the utmost care and confidentiality, the consequences can be disastrous. A case in point: an individual submitted an *Access to Information Act* (*ATIA*) request to a Government institution for all documents concerning the appointment of another Government employee to a specific position. The names of the two individuals were only vaguely similar. Yet because the departmental Access to Information and Privacy (ATIP) office's analyst had not taken care to properly read the individuals'

names when processing the *ATIA* request, an assumption was made that the requester and the appointee were one and the same individual. Thus, virtually all the information in the staffing file was disclosed to the *ATIA* requester – a small amount of third party information was removed. The file contained information about the appointee that was extremely private in nature – extensive medical and financial information, information about his family, his own employment and education history, and his home address and telephone number. It was also discovered that there was an uncomfortable history between the two individuals and that the requester had subsequently used some of the appointee's medical information to conduct his own personal inquiries about the appointee.

When that information is not treated with the utmost care and confidentiality, the consequences can be disastrous.

Following an investigation the institution readily admitted the error, apologized to the individual for what had occurred and gave him a copy of the same package the requester received so that he could see exactly what information about him had been improperly disclosed. The institution also asked the requester to return the information and to not keep any copies of it. While he returned the information, there were no assurances that copies had not been kept. Even had assurances been given, the damage had already been done and the appointee's personal information had already been further disclosed by the requester.

The former Commissioner accepted the fact that the situation occurred as a result of careless human error, but was appalled that the mistake was made at all – especially by the very people within the institution who are supposed to be the resident experts on the protection of personal information. Had the appointee's personal information been reviewed with the care it deserved this grievous violation of his privacy rights would never have occurred.

Disclosure of criminal past to offender's family members

An individual complained to this Office that a Correctional Service Canada (CSC) employee disclosed information about his criminal past to members of his family (including his young children who were previously unaware of their father's past) and to the public. A number of years ago the individual had been incarcerated in the same federal institution where the officer worked and he alleged that the officer disclosed confidential information obtained in the course of his duties.

The individual had also filed a complaint with CSC, which in turn conducted its own investigation. From the outset, the complainant never wavered in his statements that the officer disclosed his personal information. The officer maintained that it was not he who made the remarks, but rather a friend who was present at the time the disclosure took place – an individual he refused to identify either to us or to CSC. All of our efforts to locate the friend met with negative results. Still, based on all of the information we gathered during our investigation, the former Commissioner was prepared to find that the rights afforded the complainant under the *Privacy Act* had been violated as a direct result of the officer's actions. Indeed, CSC concluded that the officer had contravened its Code of Discipline and that he failed to observe the provisions of the *Privacy Act*; he was subsequently suspended for 15 days without pay.

Before rendering his final decision in the matter, the former Commissioner questioned CSC's rationale for concluding that a three-week suspension was appropriate to the circumstances. It was only then that we learned that new developments in the case had caused CSC to reverse its decision and withdraw the officer's suspension. Given the disciplinary action meted out to the officer, his friend had come forward saying that it was he who had disclosed the complainant's personal information, not the officer. While not fully convinced of the friend's credibility – and despite apprehensions in that regard – CSC nevertheless withdrew the suspension.

In light of this new information we conducted further inquiries but found no reason to believe the friend's version of events. Based on the evidence we

obtained, the former Commissioner concluded that it was the officer who disclosed the individual's personal information and that his friend likely only came forward because the repercussions to the officer turned out to be greater than anticipated. The former Commissioner therefore found the complaint well-founded and asked that CSC reconsider the reversal of its decision.

The former Commissioner also advised CSC that it should have advised our officials that the officer's friend had finally come forward after all of the attempts of both CSC and this Office had failed to find him. The former Commissioner considered this to be an extremely important development, one which caused CSC to reverse its initial decision and one which could obviously have had a direct bearing on his decision. CSC was well aware that we had an active investigation into the allegations made by the complainant and, in the former Commissioner's view, CSC should have immediately alerted our officials to the change of events. The former Commissioner received assurances that this was an isolated incident which would not reoccur.

Even a public record should be protected

An individual received an envelope, by courier and addressed to him, containing the Canada Pension Plan (CPP) appeal documents of another individual. He believed that the other individual must have received his own appeal information in error.

Our investigation into this matter confirmed these fears. The other individual had indeed received the complainant's appeal information from HRDC. The mix-up was the result of a lack of attention when the documents were inserted in the envelopes to be sent out.

Section 8 of the *Privacy Act* limits how Government institutions may disclose personal information. In essence, institutions may not disclose personal information to third parties without the consent of the person to whom the information relates, unless one of the permitted disclosures set out in section 8(2) of the *Act* applies.

HRDC explained that the information about the complainant that was disclosed consisted of documents that had been filed at the Federal Court and thus were part of a public record. Since section 69(2) of the *Privacy Act* states that section 8 does not apply to personal information that is publicly available, HRDC contended that it had not contravened the *Act* by sending out the information to the wrong individuals by mistake.

The former Commissioner disagreed because the complainant's information was not disclosed from a public record. The fact that it could be found in a public record does not negate the fact that HRDC disclosed the complainant's information to someone who had no need to know. On that basis, the former Commissioner concluded that the complaint was well-founded.

As a result of the complaint, HRDC apologized to the individuals, re-sent to them the information that had been misdirected and revised its mailing procedures to minimize the chances of a reoccurrence.

Unauthorized disclosure of a SIN

We investigated an individual's complaint that Human Resources Development Canada (HRDC) improperly disclosed his social insurance number (SIN) to a private investigator.

The complainant had filed a lawsuit against an insurance company that he believed had mishandled his insurance claim. During the court process he discovered that the insurance company had hired a private investigator to delve into his financial affairs. He obtained a copy of the investigator's report, and noted references to inquiries conducted at HRDC, and the information obtained as a result of those inquiries. Dissatisfied because of HRDC's apparent lack of willingness to address his concerns about this breach of his privacy, the individual eventually turned to this Office for assistance.

We established during the investigation that an employee of HRDC had queried the complainant's file in the Social Insurance Register (SIR) system during the same time period that the private investigator had conducted his inquiries. Although the complainant reported his concerns to HRDC, it did

not pursue the matter further until he indicated that he intended to subpoena HRDC employees to testify in court in his suit against the insurance company. At that time he asked for a copy of HRDC's investigation file concerning the disclosure of his SIN and any information related to the action taken by HRDC in that regard. It was only at this point – almost ten months after he first reported his concerns – that HRDC decided to conduct an internal inquiry to determine whether, or how, his SIN may have been compromised.

Dissatisfied because of HRDC's apparent lack of willingness to address his concerns about this breach of his privacy, the individual eventually turned to this Office for assistance.

It was clear from the evidence obtained during our investigation that the HRDC employee had obtained access to the individual's SIN without justification and disclosed it to the private investigator. The evidence also pointed to the possibility that the employee had also gained access to approximately 40 other client files on the SIR system for which there were no related HRDC case files that would require the employee to query their SIN files.

The former Commissioner was concerned with HRDC's lack of conviction in handling the individual's complaint about the disclosure of his SIN when he first brought it to their attention. They failed to take any action other than to issue him a new SIN, despite the fact that several officials were aware of the incident long before he complained to this Office. The former Commissioner was equally concerned that despite the seemingly adequate systems capabilities, HRDC managers do not routinely monitor the SIR system to identify and deal with any activities of a suspicious nature or that cannot otherwise be justified as part of an employee's duties.

The former Commissioner concluded that HRDC was responsible for its employee's improper disclosure of the individual's SIN to the private investigator, and that it had as a result contravened the confidentiality provisions of the *Privacy Act*.

In response to this finding, HRDC undertook to mitigate the damage to the extent possible. The Deputy Minister sent a letter of apology to the complainant, and implemented measures that will significantly enhance the security of personal information in the SIR database, and enhance monitoring of employees' access to the SIR. We are confident that this will improve HRDC's abilities to protect the personal information under its control and prevent any further violations of client privacy.

HRDC also decided to refer the matter to the Royal Canadian Mounted Police for criminal investigation – the employee was eventually fired by HRDC for the breach of security.

Statistics Canada census taker not responsible for disclosing personal information to banks

An individual alleged that Statistics Canada sold her name and address to financial institutions that then sent her unsolicited mail. The individual travelled frequently for extended periods and maintained a post office box. She was staying at a recreation vehicle park at the time of the 2001 census and the census taker explained to the individual that she would have to use the park address for the purposes of the census, which she did. Within a couple of months, she began to receive unsolicited mail addressed to her at the park. As she had only used that address for the census, it seemed logical to her that Statistics Canada must have sold or otherwise provided the address to the financial institutions.

We examined one solicitation that the individual had received and contacted the bank that had sent it to her. Using the code displayed on the form letter, the bank was able to determine that it had obtained her name and park address from one of the largest list management companies in Canada, which

handles more than 500 mailing lists representing some 25 million names. Its officials confirmed that the complainant's information was contained on one of the mailing lists which had been created and updated from information obtained from provincial telephone companies across Canada.

This detail prompted the individual to recall that she had a telephone installed at the park. While her telephone bill was sent to her post office box address, she had to provide the telephone company with the address of the park in order to have the telephone installed and serviced. It became apparent that it was the telephone company and not Statistics Canada that had disclosed the individual's name and address to the list broker, which in turn provided her information to the banks.

During the investigation, the list broker was asked to remove the individual's name from the mailing list, which it did immediately. However, the individual was alerted to the possibility that while her name would not be on an updated list, old lists held by the list broker's customers might still contain her information, and thus she might continue to receive solicitations. The former Commissioner urged her to contact those companies directly in order to remove her name from those lists. He also reminded the complainant that her name could be included in other lists in the future if, for example, she applies for credit cards, completes contest forms or purchases magazine subscriptions.

Time Limit Complaints

Under the *Privacy Act*, Canadians have a right of access to their personal information held by Government institutions and, by law, institutions must respond within 30 days after the request is received. Institutions can, however, extend that time limit to a maximum of an additional 30 days, but only under two specific circumstances: if meeting the 30-day time limit would unreasonably interfere with the institution's operations, or if consultations are required which cannot reasonably completed within that time.

The number of complaints related to time limits being exceeded by federal institutions for providing personal information to citizens increased to 541

this year, compared to the 428 that were reported for the previous fiscal year. We closed 381 of these complaints, of which 302 were well-founded.

There were more complaints about the personal information-handling practices of Correctional Service Canada (CSC) than any other federal Government institution. Of the 177 complaints against CSC that we completed, 159 were well-founded. Although CSC increased its staff and streamlined its procedures, a delay problem in responding to requests for personal information continues.

The number of time limit complaints against two institutions dropped significantly in comparison to last year, whereas those against four others increased:

Canada Customs and Revenue Agency:	down from 85 to 31
Human Resources Development Canada:	down from 57 to 16
Correctional Service Canada:	up from 125 to 233
Royal Canadian Mounted Police:	up from 16 to 71
Department of National Defence:	up from 35 to 58
Citizenship and Immigration Canada:	up from 40 to 49

One factor that continues to hamper the ability of institutions to respond to requests within the prescribed time limits is the complexity of processing audio and videotapes.

Institutions sometimes record interviews conducted for administrative or criminal investigations. Since the *Privacy Act* applies to personal information that is "recorded in any form," individuals can ask for copies of their information on those tapes. It is a time-consuming process to listen or view tapes and then to identify and sever the information that requesters are not entitled to receive, often because it constitutes personal information about other individuals. The Department of National Defence is one of the organizations that records interviews, and it has recently acquired new equipment in an attempt to simplify the process of reviewing and severing information on tape.

Requests for voluminous investigation files also account for some delays in responding in a timely manner.

Transmittal of information by fax

Although we discourage institutions from sending personal information by fax, we realize that they are used regularly by institutions for the purposes of expediency in getting information to its destination.

One of our investigations uncovered a problem with the manner in which a Government institution was keeping a record of the personal information it was sending by fax. Fax cover sheets indicated the number of pages sent, to whom, by whom and on what date, but the institution could not identify, after the fact, which specific documents or pages had been transmitted. In other cases, the institution was not able to identify what it had received by fax from other areas in the institution.

It is imperative that institutions keep a record of the use and disclosure of personal information under their control. Except in limited circumstances, individuals have the right to know which documents containing their personal information are sent to whom and why they are disclosed.

A solution to this problem is to list the documents sent or received on the transmittal cover sheet itself. This will ensure transparency, document the flow of information and assist us in our investigations.

Processing original files versus photocopies

Some Government institutions have denied individuals access to their personal information, thus contributing to the rising number of complaints to this Office, because the departmental Access to Information and Privacy (ATIP) offices are increasingly relying on photocopies provided by their program areas, rather than working with original documents, when processing requests. The problem with this arrangement is that ATIP analysts cannot be certain that what they are given represents all the information the individual is seeking.

When this Office receives a "denial of access" complaint, we ask to see the original file to compare it with the information processed by the ATIP office. Often we have discovered that the ATIP office did not have all the information contained on the original file-because someone did not think it was relevant or had removed internal notes, or simply because the backside of double-sided documents had been missed when the documents were photocopied.

The subtle nuances that can only be appreciated when viewing original files are also lost. Photocopies do not reveal the use or meaning of different coloured forms or highlighting of significant passages, and may not capture the exact placement of post-it notes with comments. Nor do they include the paperclips that explain why certain documents are grouped together or why they are out of chronological order. These elements are essential to understanding the context of the file and to decide whether the personal information can be released to the individual.

Having our investigators review original files eliminates any misgivings that the institution may not have located all the requested information, and also gives us the unequivocal certainty that we require to ensure access has not been denied.

Although some program areas would rather not surrender their original files, particularly those with ongoing administrative activities, we suggest that they retain a photocopy for their own use for the few days it takes the ATIP office to review the original file. We also urge ATIP co-ordinators to reclaim their responsibility for the quality of responses they send to individuals by working with original files only.

INCIDENTS UNDER THE *PRIVACY ACT*

Incidents of mismanagement of personal information that warrant further review by this Office are sometimes brought to our attention. We conducted 32 such reviews last year.

As an example, last summer, following an office relocation from one building to another in Ottawa, Human Resources Development Canada's (HRDC) Disability and Benefits Appeal Branch staff discovered that two computers were missing. Although HRDC, following an investigation by its Security Division, was unable to determine exactly what had happened, it is believed that the computers were stolen when they were left unattended while waiting to be loaded into the moving trucks. It has been suggested that since both computers were new, they were taken because of their monetary value and not for what they contained. The theft was also reported to local police, but they were unable to find the missing computers or the perpetrators.

Our investigators ascertained that the computers had not been packed in boxes, but simply placed on moving trolleys without being secured in any way. They also determined that one HRDC employee was responsible for ensuring that all items were removed from their original location to the loading area, but no one actually supervised the physical transfer of items from that location to the moving trucks parked outside the building.

Although the computers were never found, HRDC was able to determine, by means of back-up computer tapes, that they contained the full names, social insurance numbers (SINs) and medical information of dozens of Canada Pension Plan (CPP) disability benefits recipients. Therefore, HRDC decided to notify those recipients about the theft.

During our review of the incident, however, we noted that an additional 38 individuals whose surnames and SINs appeared on documents had not been notified. Since this would be sufficient personal information to possibly identify these individuals, we asked HRDC to notify them of the theft as well, which it did.

We also recommended that HRDC implement additional security measures to ensure that this does not reoccur, specifically that it ensure that all personal information is removed from hard drives of computers before they are moved from one location to another; and that additional staff be present during moves to ensure adequate security for any personal information that is affected by the move.

In another incident, an individual informed this Office that documents he received from a small claims court relating to his suit against a Port Authority included personal information relating to other individuals, specifically their credit card account numbers.

Our staff determined that when the Port Authority filed its Statement of Defence in small claims court, it included a copy of a daily cash and deposit report and a cash deposit receipt. These documents identified other individuals along with their account numbers, invoice numbers, credit card numbers, and amounts paid to the Port Authority.

In its defence, the Port Authority believed that it had no choice but to file complete, unvetted documents with its Statement of Defence to comply with court procedures. As part of its defence it needed to present the information relevant to its financial transactions with the plaintiff, and was under the impression that it could not remove any information relating to the other individuals named in those documents.

When this Office made inquiries with the small claims court, we learned that it would in fact accept partial or severed documents. The Port Authority therefore could have removed all information not relating to the plaintiff when it filed its documents in court, including the personal information about the other individuals. We brought this matter to the attention of the Port Authority and, as a result, it has undertaken to have the information relating to the other individuals removed from the court's file. The Port Authority also contacted the concerned individuals to advise them that their personal information was included in a public record.

PUBLIC INTEREST DISCLOSURES

Paragraph 8(2)(m) of the *Privacy Act* allows the head of a Government institution to disclose personal information without an individual's knowledge or consent if there is a clear overriding public interest in doing so – either because it outweighs the individual's right to privacy or because it would clearly benefit the individual. Under section 8(5) of the *Act*, the Privacy Commissioner is to be notified in advance of any proposed disclosures.

This past year, the former Commissioner reminded a couple of institutions, following a review of their notifications, that the discretion to disclose personal information in the public interest should occur on an exceptional basis, where the disclosure cannot be justified under any of the other permissible disclosure provisions found in the *Act*.

It had become increasingly evident that some institutions were using the provision on a systematic and routine basis, with little apparent thought as to whether there was indeed an overriding public interest at the time. This was troubling because the situation seemed to play little or no part in the decision-making process. Often there had been no evaluation to assess what was of public interest and whether that interest should override the individual's privacy rights. As an individual rarely, if ever, has a chance to challenge the decision, it is critical that the decision-makers act in a judicious manner and ensure they have all the relevant information before making a fair determination.

However, of the 70 public interest disclosure notifications we received during the year, one was clearly warranted: the decision of the Department of National Defence (DND) to share with Veterans Affairs information regarding approximately 2,500 individuals involved in chemical warfare experiments.

From World War II to 1992, Defence Research and Development Canada (DRDC), a branch of DND formerly known as the Defence Research Establishment, compiled a list of DND members it had exposed to various

chemicals as part of its chemical warfare research program. The members were volunteers, but some may not have been aware they were part of the experiments.

As a result of a recent investigation by the Office of the Military Ombudsman, DND felt that the DRDC's information would be useful to Veterans Affairs in identifying veterans who could be entitled to benefits. The information included the individual's last name and initials, the name of the chemical administered, the date administered and the location. It also included some service numbers but no dates of birth, which left it impossible for DND to positively match all of the individuals to its employee records.

The DRDC had not copied this information to the service or medical files of the affected employees, and DND hoped that Veterans Affairs would compare the information with its records to identify any matches in its inventory, and get in touch with the individuals. The intent was that Veterans Affairs could review the cases of those veterans who claimed to have been exposed to noxious substances, including anthrax, but were refused financial assistance because there was no evidence on their service or medical files to support their claims.

The former Commissioner readily agreed with DND's decision. The benefit to the individuals was evident-Veterans Affairs could help to resolve benefit entitlement issues as well as to assist in the diagnosis and treatment of disease resulting from exposure to toxic substances.

Top Ten Departments by Complaints Received

April 1, 2002 to March 31, 2003

Organization	Total	Access to Personal Information	Time	Privacy	Other
Correctional Service of Canada	456	106	233	117	0
Canada Customs and Revenue Agency	205	127	31	47	0
Royal Canadian Mounted Police	200	101	71	28	0
National Defence	130	51	58	21	0
Citizenship and Immigration Canada	107	52	49	6	0
Human Resources Development Canada	85	38	16	31	0
Canada Post Corporation	71	37	13	21	0
Justice Canada	65	47	13	5	0
Canadian Security Intelligence Service	57	48	8	1	0
Canadian Nuclear Safety Commission	36	1	0	35	0
Others	230	100	50	80	0
Total	**1,642**	**708**	**542**	**392**	**0**

Completed Investigations and Results by Department

April 1, 2002 to March 31, 2003

Organization	Well-Founded	Well-Founded/ Resolved	Not Well-Founded	Discon-tinued	Resolved	Settled	Total
Agriculture and Agri-Food Canada	2	1	1	2	0	5	**11**
Canada Customs and Revenue Agency	37	14	878	6	8	46	**989**
Canada Mortgage and Housing Corporation	0	0	0	0	0	2	**2**
Canada Post Corporation	17	4	11	6	0	8	**46**
Canadian Heritage	0	0	1	0	0	0	**1**
Canadian Human Rights Commission	0	0	1	0	0	0	**1**
Canadian International Development Agency	1	0	1	0	0	0	**2**
Canadian Nuclear Safety Commission	0	0	35	1	0	0	**36**
Canadian Security Intelligence Service	5	2	18	0	1	0	**26**
Canadian Space Agency	2	0	0	0	0	0	**2**
Citizenship and Immigration Canada	33	4	28	13	0	28	**106**
Commission for Public Complaints against the RCMP	0	0	5	0	0	0	**5**

Completed Investigations and Results by Department (continued)

April 1, 2002 to March 31, 2003

Organization	Well-Founded	Well-Founded/ Resolved	Not Well-Founded	Discon-tinued	Resolved	Settled	Total
Correctional Service of Canada	189	17	42	11	1	65	**325**
Environment Canada	0	1	2	3	0	0	**6**
Farm Credit Corporation Canada	1	0	0	0	0	1	**2**
Finance Canada	0	1	0	0	0	0	**1**
Fisheries and Oceans Canada	1	3	4	1	0	0	**9**
Foreign Affairs and International Trade Canada	0	0	5	0	0	0	**5**
Freshwater Fish Marketing Corporation	0	1	0	0	0	0	**1**
Health Canada	2	1	6	1	0	1	**11**
Human Resources Development Canada	19	7	1,568	6	2	6	**1,608**
Immigration and Refugee Board	4	4	13	0	0	1	**22**
Indian and Northern Affairs Canada	1	0	2	0	0	3	**6**
Industry Canada	0	0	1	0	0	1	**2**
Inspector General of the CSIS	0	0	2	0	0	0	**2**
Justice Canada	4	1	11	1	0	7	**24**
National Archives of Canada	1	0	1	1	0	3	**6**

Completed Investigations and Results by Department (continued)

April 1, 2002 to March 31, 2003

Organization	Well-Founded	Well-Founded/ Resolved	Not Well-Founded	Discon-tinued	Resolved	Settled	Total
National Defence	25	7	10	7	1	14	**64**
National Parole Board	0	0	1	1	0	3	**5**
Office of the Chief Electoral Officer	0	0	0	1	0	0	**1**
Office of the Commissioner of Official Languages	0	1	0	0	0	1	**2**
Privy Council Office	0	1	5	0	0	0	**6**
Public Service Commission of Canada	1	0	2	0	0	1	**4**
Public Works and Government Services Canada	3	0	0	0	0	3	**6**
Royal Canadian Mounted Police	20	5	41	12	0	28	**106**
Solicitor General Canada	0	0	6	0	0	0	**6**
Statistics Canada	0	0	6	0	0	6	**12**
Transport Canada	1	2	0	2	0	1	**6**
Treasury Board of Canada Secretariat	0	0	2	0	0	0	**2**
Vancouver Port Authority	0	0	0	1	0	0	**1**
Veterans Affairs Canada	2	0	2	0	0	1	**5**
Total	**371**	**77**	**2,711**	**76**	**13**	**235**	**3,483**

Completed Investigations by Grounds and Results

April 1, 2002 to March 31, 2003

	Well-Founded	Well-Founded/ Resolved	Not Well-Founded	Discon-tinued	Resolved	Settled	Total
Access to Personal Information	14	72	228	36	5	131	**486**
Access	14	71	221	33	5	129	**473**
Correction/ Notation	0	1	7	3	0	0	**11**
Language	0	0	0	0	0	2	**2**
Inappropriate Fees	0	0	0	0	0	0	**0**
Privacy	56	4	2,445	17	8	86	**2,616**
Collection	7	2	831	2	7	19	**868**
Retention and Disposal	4	0	4	0	0	13	**21**
Use and Disclosure	45	2	1,610	15	1	54	**1,727**
Time Limits	301	1	38	23	0	18	**381**
Correction/Time	2	0	0	0	0	0	**2**
Time Limits	287	1	29	23	0	18	**358**
Extension Notice	12	0	9	0	0	0	**21**
Other	0	0	0	0	0	0	**0**
Total	**371**	**77**	**2,711**	**76**	**13**	**235**	**3,483**

Origin of Completed Investigations

April 1, 2002 to March 31, 2003

Province/Territory	Number
Newfoundland	14
Prince Edward Island	3
Nova Scotia	59
New Brunswick	52
Quebec	2,247
National Capital Region–Quebec	22
National Capital Region–Ontario	96
Ontario	396
Manitoba	83
Saskatchewan	55
Alberta	167
British Columbia	273
Nunavut	0
Northwest Territories	0
Yukon	4
International	12
Total	**3,483**

Inquiries under the *Privacy Act*

April 1, 2002 to March 31, 2003: 5,183

We will attempt to provide a breakdown of these inquiries by subject in future Annual Reports.

PRIVACY PRACTICES AND REVIEWS

Section 37 of the *Privacy Act* empowers the Commissioner to initiate compliance reviews of the personal information management policies and practices of federal institutions. This means that, at the Commissioner's discretion, he can audit them to determine whether they adhere to the fair information practices set out in sections 4 to 8 of the *Act*. The Privacy Practices and Reviews (PP&R) Branch may evaluate the compliance of organizations with the requirements of the *Privacy Act*.

In the aftermath of September 11, 2001, a number of federal Government departments and agencies received significant funding increases to allow them to implement changes to combat terrorism and enhance national security. To assess the impact that these anti-terrorism measures are having on individual privacy, the Office initiated reviews of the personal information handling practices at the Royal Canadian Mounted Police, the Canadian Security Intelligence Service and the Communications Security Establishment. The reviews will be completed in the upcoming fiscal year.

A number of programs and activities established by federal Government institutions and agencies provide for the disclosure of personal information about Canadian citizens and residents to departments and agencies of the United States government. During this fiscal year, the Office initiated an examination of agreements, arrangements and memoranda of understanding between Canada and the United States that include provisions for the sharing of personal information. Eighteen departments and agencies were selected for this examination and a review will be completed in the upcoming fiscal year.

In addition to reviewing and auditing, our Office advises federal organizations on compliance issues and the privacy implications of new and existing programs and practices. The Office's PP&R Branch has been involved in numerous consultative efforts with Government departments, including the Treasury Board of Canada Secretariat, Elections Canada, Statistics Canada, Human Resources Development Canada, Indian and Northern Affairs Canada, and Health Canada, to name a few.

These consultations often involve reviewing new information management proposals, such as data-matching initiatives, the creation of databases and information-sharing arrangements with other organizations. It is important to note that the Commissioner's role in such issues is an advisory one. The Commissioner does not in any way provide formal approval for such initiatives, which would compromise his impartiality during subsequent investigations or reviews.

As described in our earlier reports, HRDC developed a review procedure to deal with policy analysis, research and evaluation activities involving the linking of separate databanks. Part of this procedure includes consultation with our Office. During the past year, the Office has analyzed and commented on close to a dozen HRDC submissions, including the Evaluation of HRDC Work Sharing Program, the Evaluation of Labour Market Information Services, and the Canada Student Loan Program Needs Assessment and Loans Disbursement Datasets Project.

One project that the department sent our Office, the Employer and Industry Activity System, was submitted as an undertaking involving databank connections. Upon review, our Office concluded that the project involved more than simply the linking of existing databanks. Rather, it would result in the creation of a new databank that would be used on an ongoing basis. It was never contemplated that this type of project would be dealt with through this process. As a result, we advised HRDC that the matter would be more appropriately dealt with by way of a Privacy Impact Assessment (PIA), which entails a more rigorous review. PIAs are discussed in more detail in the following section of this Report.

We have continued to notice an improvement in the detail and completeness with which HRDC's submissions address privacy issues. In our last Report, we expressed a concern that HRDC provided limited information regarding contracts with outside parties, and we said that HRDC should strengthen the contractual obligation of those parties to protect the privacy of personal information under their temporary stewardship. Although some of the submissions we received did not fully meet expectations, the department has improved in addressing this concern over the past year.

PRIVACY IMPACT ASSESSMENTS

On May 2, 2002, the Secretariat of the Treasury Board of Canada issued a new directive requiring federal Government departments and agencies to undertake a Privacy Impact Assessment (PIA) for all new programs or services that raise privacy issues. Canada is the first country in the world to make PIAs mandatory for all federal departments and agencies.

For more than a year prior to that date, the Office had been urging the Government to put a PIA Policy in place, in order to ensure that privacy considerations are built in at the outset of projects and not as an afterthought. In developing this Policy, we congratulate the Government for implementing the Policy and for recognizing that respect for citizens' privacy is critical to the success of all its programs and services, including the Government On-Line initiative.

New and existing programs and services with potential privacy risks must now undergo a PIA – in effect, a feasibility study from a privacy perspective. This includes significant redesigns of existing programs when the redesign involves a new or increased collection, use or disclosure of personal information, new data-matching, contracting-out or other changes that potentially raise new privacy concerns.

A PIA is designed to provide federal Government departments and agencies with a consistent framework to forecast a proposal's impacts on privacy, assess its compliance with privacy legislation and principles, and determine what mitigating measures are required to overcome the negative impacts. If done correctly, a PIA is a way to avoid extra costs, adverse publicity, and the loss of credibility and public confidence that could result from a proposal that is not privacy friendly. It is also a way to raise awareness and understanding of privacy principles, both internally and among citizens.

The conduct of a PIA is a shared responsibility. As the Treasury Board Policy states, PIAs are co-operative endeavours, requiring a variety of skill sets, including those of program managers, technical specialists, and privacy and

legal advisors. Although the deputy head of a federal institution, department, or agency is responsible for determining if a PIA is required, several Government departments have set up internal committees to review departmental projects to determine whether a PIA is required. Given the multi-disciplinary nature of the exercise, this strikes us as a sensible approach.

Of particular significance is the fact that the Policy requires departments to inform the Office of all proposals for new or modified programs and services that raise privacy issues. Departments must also consult the Office while preparing a PIA to ensure that privacy risks are identified and that mitigating actions to deal with those risks are appropriate. By reviewing the documentation in co-operation with institutional officials, our Office is then able to provide advice and guidance to institutions and identify solutions to potential privacy risks.

The Commissioner's role is not to approve or reject projects that are assessed in the PIAs, but rather to assess whether or not departments have done a good job of evaluating the privacy impact of a project or proposal.

To take on this new responsibility, we created a new division within the PP&R Branch devoted entirely to analyzing and providing comments on PIAs submitted for review.

During the period of this Report, our Office received 17 PIAs and 12 preliminary PIAs (PPIAs), and has been consulted on several projects that would require PIAs. Based on discussions with the Treasury Board Secretariat (TBS) and other federal Government departments and agencies, we expect to receive more than 50 PIAs over the next fiscal year.

Most of these initiatives or projects involve the electronic delivery of services to individuals through the Internet, so the privacy risks come from a variety of sources, including systems characteristics, technical infrastructure and design of the on-line service or program.

Five of the 17 PIAs we received were prepared prior to the TBS Policy being introduced, and thus did not adhere to the policy requirements or the guide-

lines associated with the Policy. As a consequence, most were either returned to or withdrawn by the submitting departments to be revised in accordance with the Policy. So far, eight PIAs received have run the full course of the review process.

The Commissioner's role is not to approve or reject projects that are assessed in the PIAs, but rather to assess whether or not departments have done a good job of evaluating the privacy impact of a project or proposal.

While the majority of reports received to date from departments are PIAs, we have witnessed over the course of the year a growing number of Preliminary Privacy Impact Assessments (PPIAs). We believe this trend reflects an inclination on the part of departments to adopt a more cautious and phased approach to the development of their PIAs, given their unfamiliarity with the process and the probable lack of in-house expertise in this area. Where departments are facing a fixed and impending deadline for implementation, we have been advising those departments to directly draft their PIA to expedite the review process.

So far there has been no PIA, and certainly no PPIA, where our staff has not found it necessary to go back to the submitting department for additional information. Some commonly omitted elements include:

- a project implementation schedule;
- a complete inventory of data elements collected and used (information may be described, but not itemized);
- an adequate description of the business process;
- a data flow chart, or one that is complete; and
- an adequate description of the information security infrastructure associated with the project.

In addition to this, background documents commonly missing include:

- draft agreements, where third party service providers are involved;
- Threat and Risk Assessment (TRA) reports, where conducted;
- project feasibility studies, where conducted;
- project management plans, as they relate to project design; and
- technical specifications relating to system design.

There are also a number of common problems which we have observed in the privacy analysis. They include:

- confusing privacy with security and confidentiality;
- seeing the PIA process as essentially a privacy compliance audit exercise;
- failure to link identified risks with specific design elements of the project;
- proposed mitigating measures not addressing the risk identified; and
- proposed mitigating measures for risks that have not yet been identified.

Although these problems and omissions reflect the unfamiliarity of departments with the PIA Policy, it should be noted that we are now beginning to see a general improvement in the quality of the PIAs we are receiving.

If there are lessons to be drawn from our experience of the last eleven months, one is the need for greater education on how the PIA functions as a risk management tool. Another is the need for departments to notify and involve the Office at the earliest possible stage in the development of the PIA.

Given that there is a need for organizations to have a better understanding of the PIA Policy, we advise Government officials to contact the Treasury Board Secretariat or to visit its Web site at **www.tbs-sct.gc.ca** for more information.

IN THE COURTS

Section 41 of the *Privacy Act* allows an individual, following the results of an investigation of a complaint by the Privacy Commissioner, to apply to the Federal Court for review of the decision of a Government institution to refuse the individual access to her personal information. From the time the *Privacy Act* came into force in 1983 to March 31, 2003, approximately 130 applications for review have been filed in the Federal Court. Eight of these were filed in the year ending March 31, 2003.

Section 42 of the *Privacy Act* allows the Commissioner to appear in Federal Court. The Commissioner can apply to the Federal Court for review of the decision of a Government institution to refuse access to personal information if he has the consent of the individual who requested the information. The Commissioner can appear before the court on behalf of an individual who has applied for review under section 41. Or, with leave of the court, he can appear as a party to any review applied for under section 41.

There are currently no applications under the *Privacy Act* in which the Commissioner is actively involved. However, the Commissioner also participates in litigation that arises outside of the *Privacy Act*. Following is a summary of litigation involving significant privacy issues in which the Commissioner has been involved.

Mertie Anne Beatty et al. v. The Chief Statistician et al.

Federal Court File No. T-178-02

This issue was brought before the Federal Court of Canada by a group of Canadian citizens seeking access to the 1906 Census Returns for the Provinces of Manitoba, Saskatchewan and Alberta pursuant to section 6 of the Privacy Regulations.

The Offices's position has always been that disclosure of the 1906 census information is prohibited by the confidentiality provisions in the *Statistics Act*, and that legislative amendments should, therefore, be explored as a means of compromise.

Status

The Application was filed in February 2002. Following a review of the legislation, the federal Government decided that the information could, in fact, be released and did so. Bill S-13 was later introduced in order to retroactively modify census laws to allow access to records and address privacy concerns. Accordingly, the Application was discontinued.

Canada Post Corporation v. Privacy Commissioner of Canada

Federal Court File No. T-233-02

On January 14, 2002, the former Commissioner determined that Canada Post's use of its National Change of Address (NCOA) service contravened the *Privacy Act* in two ways. First, Canada Post contravened section 5(2) of the *Act* by failing to specify to NCOA applicants its intention to disclose new addresses to mass mailers and direct marketers for a commercial purpose. Then it contravened section 8 by failing to obtain the consent of individuals for the disclosure of their new addresses to mass mailers and direct marketers.

Status

On February 13, 2002 Canada Post filed an Application alleging that the former Commissioner had exceeded his jurisdiction in applying sections 5 and 8 of the *Privacy Act*. On April 4, 2002, however, Canada Post agreed to add a box on its form enabling individuals to provide consent for this activity. The issue thus became moot, and Canada Post discontinued its Application on April 14, 2002.

Privacy Commissioner of Canada v. Attorney General (Canada) et al.

British Columbia Supreme Court File No. S57566

In June 2001 the Office received a complaint regarding the installation of Royal Canadian Mounted Police (RCMP) surveillance cameras in the downtown core of the City of Kelowna, B.C. After an investigation, the former Commissioner determined that by recording continuously rather than recording only selective incidents related to law enforcement activities, the

RCMP is unnecessarily collecting information on thousands of innocent citizens engaged in activities irrelevant to the mandate of the RCMP. It was concluded, therefore, that the video surveillance in Kelowna was in contravention of the *Privacy Act*.

The RCMP informed this Office that the continuous video recording of the surveillance camera was terminated on August 28, 2001. Instead, the area under surveillance would only be videotaped if a violation of the law was detected. While this put the use of the surveillance camera into compliance with the letter of the *Privacy Act*, which technically only applies to information that is "recorded in any form", it was the former Commissioner's opinion that a continuation of the video camera surveillance even without continuous recording was insufficiently respectful of the spirit of the *Privacy Act* and of the privacy rights of Canadians.

On June 21, 2002, the former Commissioner filed a Statement of Claim in the Supreme Court of British Columbia, requesting declarations from the Court that this generalized video surveillance was unconstitutional, contravening the *Charter*, as well as Canada's international human rights obligations. From March 12 to 14, 2003 there was a hearing on the federal Government's motion to dismiss the case. The court held that the Commissioner lacked the legal capacity to bring the action.

Status

On July 4, 2003, the newly-appointed Commissioner announced that he had instructed counsel to withdraw its appeal into the case. Although the Commissioner and this Office continue to have a variety of concerns regarding video surveillance of public places by public authorities, continuing this particular action was not perceived as a useful way of spending public funds.

Information Commissioner of Canada v. Commissioner of the RCMP et al.

Supreme Court of Canada File No. 28601

A list of the career postings of four Royal Canada Mounted Police (RCMP) officers was requested under the *Access to Information Act*. The Commissioner of the RCMP refused to release the information on the grounds that it revealed employment history and thus was personal information as defined in section 3 of the *Privacy Act*. The Information Commissioner argued, however, that paragraph 3(j) of the definition of personal information in the *Privacy Act* states that information relating to the position or functions of Government officers or employees is not personal information for the purposes of section 19 of the *Access to Information Act*.

Status

The Supreme Court of Canada released their unanimous decision on March 6, 2003. The Court very clearly stated that information may be personal and yet still fall under the rubric of section 3(j) where it reveals general characteristics associated with the position or functions held by an officer or employee of a federal institution. The Supreme Court felt that none of the information requested pertained to the competence or characteristics of the employees. It therefore ordered that the following information be released for each of the named individuals: a list of historical postings, status and dates, a list of ranks and dates those ranks were achieved, and the years of service and anniversary date of service.

The decision of the Supreme Court limits the application of paragraph 3(j) of the definition. Even though this Office had argued for a narrower interpretation of the exception, the decision of the Supreme Court is not unreasonable.

Part Two

Report on the *Personal Information Protection and Electronic Documents Act*

INTRODUCTION

The *Personal Information Protection and Electronic Documents (PIPED) Act* sets out ground rules for how private sector organizations may collect, use or disclose personal information in the course of commercial activities.

Since the *Act* took effect on January 1, 2001 it has applied mainly to the commercial activities of what are known as federal works, undertakings or businesses, such as transportation and telecommunications companies, banks and broadcasters. It also applies to the personal information of employees in those companies, and it applies to personal information that is sold, leased, or bartered across provincial or national boundaries by provincially-regulated organizations. As of January 1, 2002, the personal health information collected, used or disclosed by these organizations is also covered. On January 1, 2004, the *PIPED Act* will cover the collection, use or disclosure of personal information in the course of all commercial activities in Canada, except in provinces which have enacted legislation that is deemed to be substantially similar to the federal law.

The second full year under the *PIPED Act* proved to be an interesting and challenging one for our Office on several fronts. We began to accept and investigate complaints that concern the personal health information of individuals. We also made further inroads into a myriad of issues, including consent and marketing, credit scoring, the recording of telephone calls and security clearances.

We also undertook a number of communications activities to raise awareness of privacy issues and federal privacy laws. From April 1, 2002 to March 31, 2003 the former Commissioner and senior staff delivered 49 speeches at conferences and special events; we issued more than 25 news releases and media advisories on key privacy issues; we responded to hundreds of media requests for information and interviews; we disseminated more than 23,000 of our publications to members of the public, businesses and other organizations across the country; and we received an ever-increasing number of hits to the Web site, averaging approximately 50,000 hits per month.

The *PIPED Act* requires the Commissioner to submit an Annual Report to Parliament on the activities of the Office in the previous year. The current Report covers the period from January 1, 2002 to December 31, 2002 for the *PIPED Act*.

INVESTIGATIONS AND INQUIRIES

During the 2002 calendar year, the Office received 300 complaints under the *PIPED Act* from individuals alleging that their privacy rights had been violated by a wide range of different organizations. Approximately 37% of the cases dealt with practices in the banking sector, followed by 19% with the telecommunications and broadcasting sector, 15% with transportation companies, and 13% with the nuclear sector. The remaining complaints, 16%, were filed against a variety of other types of organizations, including Internet service providers, credit bureaus and aboriginal band councils.

The former Commissioner issued findings for 162 complaints under the *PIPED Act* in 2002 and they were concluded as follows:

Not well-founded	61
Well-founded	45
Resolved	41
Discontinued	15

In addition to this, the Office also conducted five incident investigations. Incidents are matters that the Commissioner becomes aware of from various sources, including the media. Usually a victim is not identified and a complaint has not been filed with the Office.

What follows in this Report is a sampling of some of the year's more notable cases. More detailed summaries of all findings under the *PIPED Act* are available on our Web site, at **www.privcom.gc.ca**. These findings are posted in order to provide guidance to organizations and the legal community on the application of the *Act*.

DEFINITIONS OF FINDINGS UNDER THE *PIPED ACT*

Not well-founded: This means that there is no evidence to lead the Privacy Commissioner to conclude that the organization violated the *Personal Information Protection and Electronic Documents (PIPED) Act*.

Well-founded: This means that the investigation revealed that the organization failed to respect a provision of the *Personal Information Protection and Electronic Documents (PIPED) Act*.

Resolved: This means that the organization has taken corrective action to remedy the situation, or that the complainant is satisfied with the results of the inquiries made by the Office of the Privacy Commissioner of Canada.

Discontinued: This category applies to investigations that are terminated before all the allegations have been fully investigated. A case may be discontinued for any number of reasons, such as the complainant no longer being interested in pursuing the matter.

SUMMARY OF SELECT CASES UNDER THE *PIPED ACT*

A case of mistaken identity

A complainant who wrote to the Office said she was notified by a friend that a notice in the newspaper indicated that the police were looking for her. To her horror, the complainant found herself looking at her own image in a photograph accompanying the Crime Stoppers "Crime of the Week" article. The article described a recent theft of two cheques from an elderly woman and identified the depicted person as a suspect in the crime. The image had been captured from a video surveillance camera at a bank. The camera had been pointed at the teller's wicket where the thief had cashed the stolen cheques.

As it turned out, the complainant had indeed visited the same bank and the same teller's wicket on the day in question, but not to cash a cheque. She had gone there simply to pay a bill. It was clear that she was not the actual perpetrator of the crime.

It was the same bank, the same wicket, the same day, but not, as our investigator learned, the same time.

On the day in question, the clock on the bank's journal roll (its computerized record of transactions) had been 12 minutes slower than the clock on the video camera. When the bank's security staff later forwarded the videotape to the time of the cheque-cashing as indicated by the journal roll, the image that appeared was not that of the actual cheque-casher. Rather, it was the image of the woman who had preceded the cheque-casher at the teller's wicket by some 12 minutes – the complainant.

Thus, the photographs that the bank subsequently gave to the local police, and the police in turn to the Crime Stoppers organization, depicted the wrong person.

To her horror, the complainant found herself looking at her own image in a photograph accompanying the Crime Stoppers "Crime of the Week" article.

A week after the original "Crime of the Week" article, Crime Stoppers ran a retraction in the same local newspaper. On the same day, the newspaper itself ran a front-page story, clarifying that the complainant had been a victim of mistaken identity. The complainant also received formal apologies from the bank, the police, and Crime Stoppers. The two latter organizations further admitted that they had both failed to follow normal verification procedures, and both have since collaborated in instituting measures to prevent similar occurrences. The bank also instituted procedural changes to verify the time on surveillance tapes and journal rolls.

However, the complainant was not entirely satisfied. After her initial shock and distress, she became even more concerned about the effect the incident was having on her reputation when she learned that many people had indeed recognized her image from the article. This was of particular concern because her work depended upon her ability to visit clients' homes and offices. She was also concerned that her image may have appeared in other Crime Stoppers notices. Our Office was able to reassure the complainant that her photograph had been used in only the one newspaper article.

As to the disposition of her formal complaint to the former Commissioner, we considered the matter in relation to the bank's obligations under the *PIPED Act* to ensure the accuracy of personal information.

We determined that the personal information at issue – the photograph of the complainant – had been wholly inaccurate in a situation where accuracy had been crucial to the purpose of solving a crime. On that account alone, the bank should have made sure that the information it disclosed was as accurate as possible. It had not done so, and therefore was in clear contravention of Principle 4.6 of the *Act*. In the letter of findings to the complainant, the former Commissioner wrote:

> *" … an organization must take due account of the potential adverse consequences of inaccurate information for the individual. I have determined that your personal information inaccurately disclosed by [the bank] was used to make a decision about you – specifically, an erroneous decision to the effect you were to be sought as a prime suspect in a crime. This was a decision, moreover, that caused you substantial notoriety, embarrassment, and worry about your reputation and your livelihood. Being well aware that the police would likely use your personal information to make a decision about your status as a suspect, the [bank] should have taken due care to ensure that the information was accurate so as to minimize the possibility of a wrong decision with adverse consequences for you."*

The former Commissioner determined that this complaint was well-founded.

U.S. security measures affect Canadian pilots

The aftermath of September 11, 2001 continues to be felt by average Canadians. One individual directly affected by new security measures, a commercial airline pilot, was confronted with a difficult choice: forfeit his privacy rights or risk losing his job. In the past, when he needed to take aircraft training required to keep his licence, his employer simply sent him to a flight school in Florida. This changed after the September 11 terrorist attacks. American flight schools were now obliged to have their foreign students – including Canadian commercial airline pilots – sign an authorization form. The form would allow the U.S. government to collect and disclose personal information about the students. However, it did not adequately explain the purposes for, nor did it appear to set any limits on, this collection and disclosure.

When his employer asked him to sign the form, the pilot was incensed. After all, he had already undergone an extensive background check by the Government of Canada. He disliked the prospect of a foreign government sifting through his background – especially when it was not clear what information would be collected and to whom it would be disclosed.

He disliked the prospect of a foreign government sifting through his background – especially when it was not clear what information would be collected and to whom it would be disclosed.

No one seemed comfortable with the form – the Canadian Government, the airline, the union – but there was no immediate solution on the horizon. The federal Government had asked the United States to accept Canadian background checks on commercial pilots. But at the time of the complaint, the United States had not yet made a decision.

The airline was troubled by the wording of the form, but was in a difficult situation. By law, its pilots require the training. The nearest alternative was a flight school in Europe – a more costly prospect than sending its pilots to Florida. Furthermore, since the pilot and co-pilot must train together, the airline would be in an awkward position if one pilot was willing to sign the form and the other was not.

The pilot's union protested the requirement to sign the form. It negotiated an agreement with the airline which stated, among other things, that the decision to sign the form was voluntary, and that the company would provide alternative training for dissenting pilots.

The pilot decided not to sign the form. Although his employer obtained a temporary extension of his licence until a resolution could be found, it did

not make alternative training arrangements for him. Unless the U.S. government agreed to Canada's request, or the former Privacy Commissioner made his findings, the airline was not going to change its decision. The pilot's extension eventually ran out.

We were highly critical of the authorization form. It was entirely objectionable on many fronts and we concluded that the practices it authorized completely failed to meet the fair information principles that are the cornerstone of Canada's privacy legislation.

In making these determinations, we relied on the "reasonable person test" outlined in section 5(3) of the *PIPED Act* to assess the airline's purposes. We acknowledged that, on the surface, the airline's reasons for making its pilots sign this form appeared reasonable. Below the surface, however, the purposes ceased to be acceptable. We thought very little of the airline putting cost and convenience ahead of the pilot's right to refuse consent to collection and disclosure practices that were clearly in contravention of Canadian law. It was noted that the airline had options but that it had chosen not to exercise them.

In finding that the airline's purposes did not meet the expectations of section 5(3), in the letter of findings, the former Commissioner commented on this timely example of the difficulty of balancing national security requirements with the fundamental right of privacy:

> *"I agree that the circumstances that many countries, most particularly the United States, currently find themselves in warrant some security measures. Of course it is reasonable to demand that pilots receive security clearance in order to fly, and that is why Canada has in place security measures that Canadian commercial pilots must undergo… But would a reasonable person consider it appropriate to require these same pilots to then consent to unacceptable collection and disclosure practices at the request of a foreign government? I think not. Indeed, I suspect most reasonable Canadians would find this encroachment on Canadian rights to be highly objectionable. Furthermore, most*

> *Canadians would likely expect employers to provide reasonable options for employees and would demand that their government raise an alarm bell with the United States."*

After receiving the letter of findings, the airline agreed with the former Commissioner's recommendation and arranged to provide training at an alternative location for the pilot and others who refuse to sign the form.

Bank's disclosure to individual's employer inappropriate

An individual went to his bank on personal business – to dispute a charge for cheques. He was not satisfied with the bank's response he was given and a scene ensued.

The branch manager came onto the scene and decided his staff should not have to deal any further with the customer. The firm that employed the customer happened to do a lot of important business with the bank. Before terminating the bank's relationship with the customer, the branch manager thought he should discuss the matter with the customer's employer.

The complainant was astounded when his employer confronted him about what had occurred at the bank earlier that morning.

One of our first tasks was to determine what exactly had been disclosed in the telephone conversation between the bank manager and the employer. In the absence of any evidence that they had discussed the complainant's financial affairs, it appeared that the actual disclosures about had been limited to three simple facts: (1) that he had an account with the branch; (2) that his account was to be terminated; and (3) that there had been a scene with the teller.

In the bank's view, none of this should have been considered the complainant's personal information. The bank pointed out that the scene itself had been acted out in a public place, and in a small community, where a person does his banking is hardly a matter of secrecy. The bank took the position that the disclosures in question fell into the category of "normal public discourse," comparable to "small-town gossip." The bank even suggested that it

had a right to make such disclosures for the sake of extending "business courtesy" and protecting its own business interests. Citing section 5(3) and Principle 4.3.5, the so-called "reasonableness" provisions of the *PIPED Act*, the bank also suggested that the complainant had not had a reasonable expectation of privacy, and that reasonable people would have considered the disclosures appropriate in the circumstances.

Although we were not unsympathetic to the bank and were willing to concede the reasonableness of the bank's position up to a point, the former Commissioner had to draw the line somewhere. In the letter of findings to the complainant, the former Commissioner commented as follows:

> *"In my view, … the reasonableness of the situation ends exactly at the point where the [bank] manager, in the full knowledge that you had been acting on your own behalf at his branch that morning, nevertheless picked up the telephone at his office during business hours to inform your employer. This was not casual or inadvertent disclosure. This was not small-town gossip. This was a deliberate act of disclosure of personal information to a third party by a person who was acting in an official capacity and who had no right to make such disclosure. Moreover, the Act puts the rights of individuals above such notions as 'business courtesy' and makes no distinction as to the size of one's community. Would any reasonable person anywhere expect his bank manager to disclose information about his personal banking affairs to his employer? The answer to this question is obviously no."*

Credit score fraud

In the course of investigating complaints about credit reporting and scoring, we learned a great deal about the workings of the credit-granting industry at large.

In two particular cases, individuals had made formal requests under the *PIPED Act* for access to certain personal information on file with their banks. Specifically, each requester had wanted to know his credit score. The banks in question had refused access, each invoking the exemption provided in section 9(3)(b) of the *Act*. This provision says in effect that an organization does not

have to give access to personal information if doing so "would reveal confidential commercial information."

In the course of investigating complaints about credit reporting and scoring, we learned a great deal about the workings of the credit-granting industry at large.

The requesters, believing to the contrary that credit scores were personal information to which they were fully entitled to have access, filed complaints with the Office. Our main task in each case was to decide whether the exemption cited by the bank was valid.

A credit score is a numerical indication of credit-worthiness, generated by means of an algorithmic model. For most people familiar with the notion, the term "credit score" mainly conjures up the vision of credit-reporting agencies. These agencies are in the business of providing banks and other credit-granting institutions with background credit information, sometimes including credit scores, on prospective clients. In considering an application for credit, a credit-granting institution will often obtain the applicant's credit history from a credit-reporting agency. In some cases, the institution will also request a credit score for the applicant. Credit-reporting agencies do not themselves generate credit scores, but rather provide scores that another company generates from the agency's information.

Up to a point, the complainants had good grounds for their position. In prior cases, we had already considered the matter of access to personal credit information, at least as far as credit reporting agencies were concerned. We had already concluded that credit scores *are* personal information according to the definition in the *Act*, and that individuals *do* in principle have a right of access to them. We had determined that credit-reporting agencies in particular are required to comply with Principle 4.9 of the *Act* by giving individuals access on request to personal information in their credit files. We had further

determined that banks, if they have obtained an individual's credit information from a credit-reporting agency, must likewise give the individual access on request to the information, including any credit score provided by the agency.

But the more recent cases were not nearly as straightforward. The special problem they presented was that the credit scores sought by the complainants were not the usual agency-provided credit scores. They were in fact scores that the banks themselves had generated and assigned internally.

It is perhaps less widely known that banks, too, have credit scores, distinct from those provided by credit-reporting agencies. Banks generate their own internal credit scores by means of their own internal credit-scoring models, very different from those associated with agencies. Whereas agency scores are generated by means of standardized models based almost exclusively on credit information, a bank develops its own customized models, unique to the bank and incorporating not only credit information on the individual, but also many other elements pertaining to the bank's own strategic business priorities. Because banks regard and treat their internal credit-scoring models as proprietary confidential commercial information, such models are much more problematic in terms of the *Act*.

By citing section 9(3)(b), the banks in question were not suggesting that an internally generated credit score was itself confidential commercial information. Rather, they were saying that the model used to generate such a score was confidential commercial information. And they were saying in effect that internal credit scores, if made available to individuals, would reveal the model by which the scores had been generated.

The special problem they presented was that the credit scores sought by the complainants were not the usual agency-provided credit scores.

We accepted the banks' arguments that an internal credit-scoring model constituted confidential commercial information. But we were far less persuaded of the more crucial proposition – that releasing the credit scores would somehow reveal the credit-scoring model itself. How could merely letting a person know his credit score possibly lead to his knowing the inner workings of such a complicated, technical and algorithmic apparatus as a credit-scoring model?

As it turned out, it was not the average customer that the banks feared. It was fraudsters intent on "cracking" a bank's internal credit-scoring model for nefarious purposes. According to the banks, fraudsters could employ devious means to acquire a number of credit scores and then would extrapolate the model from the scores. Either the fraudsters would be working for the banks' credit competitors, trying to gain competitive advantage. Or they would be operating on their own behalf, trying to procure credit for themselves on false pretenses.

In their submissions to the Office, the banks presented an independent forensic analysis of the risk of fraud contingent upon the availability of credit scores. This analysis concluded that, if credit scores were readily available, the integrity of a bank's internal credit-scoring model could be compromised on the basis of a relatively small number of credit scores generated by the model.

The fraud scenarios outlined by the banks struck us as farfetched. To be fair, however, we sought the advice of an expert in the field of algorithms. This expert confirmed that access to customized credit scores would definitely make it easier to approximate a bank's internal credit-scoring model.

We were still doubtful. In particular, we were mindful that section 9(3)(b), by using the phrase "would reveal" rather than "could reveal", set a very high standard for the withholding of personal information. On the word of the algorithm expert, we were willing to concede that a model could be approximated from knowledge of a certain number of scores, but we remained unpersuaded that it would ever happen. The banks' submissions had failed to convince us that fraudsters would actually go the lengths described to deceive a bank. We found it particularly difficult to accept the apprehension, evidently

shared by all banks, that even one's competitors in the credit-granting community would as a matter of course resort to such tactics in order to "crack" one another's models for the sake of competitive advantage.

Nevertheless, the fact remained that two banks had strongly expressed what we took to be genuine belief and fear that their internal credit-scoring models would inevitably be revealed and fraudulently manipulated if individuals were given access to credit scores. However unlikely it seemed to us, it was undeniably a prospect that the banks took very seriously. Moreover, it was a prospect that we were unable to wholly refute.

In the end, the former Commissioner decided to give the banks the benefit of the doubt. He did so primarily out of consideration for his responsibility to achieve a balance between the privacy rights of individuals and the legitimate informational interests of organizations. Seeing little informative value in a credit score on its own and no significant harm ensuing to Canadians' privacy rights from the inability to obtain internal credit scores, we thought it only fair in the circumstances to accept the banks' position.

The former Commissioner found that the banks had appropriately cited section 9(3)(b) to refuse the complainants access to their internal credit scores.

Customers beware: Your conversation may be recorded

The practice of taping customer telephone calls – common among many organizations – was the subject of two complaints. These cases illustrate two very different approaches taken by organizations to inform customers of the practice and obtain their consent. In both cases, as in those involving secondary marketing, reasonable expectations played a role in the former Commissioner's findings.

In the first case, an individual called his bank in the intended role of guarantor of his daughter's loan application. At the end of the conversation, he learned that his call had been tape-recorded. He had not been informed, either by the customer service representative or via a recorded message, that

his call would be taped. Nor was he asked, upon learning that the call had been recorded, if he agreed.

The bank had an interesting take on the issue of consent in this case. In its view, only one party had to consent to calls being recorded. It therefore required its customer service agents to sign a consent form for the taping of these calls.

The bank's purpose for recording the call was that it needed confirmation of the customer's records and evidence that the customer had consented to the product or service. In its view, the taped call is the equivalent of a signed form and is used for record-keeping purposes.

We agree that information exchanged during the conversation should be recorded in some way. However, the reasonable expectations of the customer should also be considered, and most individuals would want to know *beforehand* that their call is going to or may be taped. In this case, the bank clearly did not meet those expectations and did not have the father's consent to record his call, thus contravening the consent principle of the *PIPED Act*.

In the other complaint, an individual also alleged that his bank had recorded his telephone conversations without his knowledge and consent. This individual had taken the bank to court over liability for certain withdrawals made on his bankcard. During this process, the bank introduced a tape-recording of a telephone conversation between him and a bank employee.

The bank argued that it had this individual's consent to tape his calls. It referred to an agreement, signed by him when he opened his account, that acknowledged the bank's practice of recording telephone calls. There were also the privacy brochures given to him – five in all – which specified

…most individuals would want to know beforehand that their call is going to or may be taped.

the bank's purposes for collecting personal information. The complainant, however, did not read any of this information.

Then, there was a conversation between a bank employee and the complainant (also taped), in which the employee explained the bank's practice of recording conversations. To the complainant, "recording" did not necessarily mean electronic recording, and so he stood by his original complaint.

The former Commissioner determined that the bank had made a reasonable effort to inform the complainant of its practice and purpose and that it had his consent to record his calls by way of the agreement form that he had signed. We then found that the bank had complied with the relevant provisions of the *Act*.

Clearly, organizations such as this one, which have made the effort to inform customers and to obtain their consent, have the reasonable expectation that customers will read what is put in front of them.

Nevertheless, the bank in the second case was keen on improving its practices regarding the taping of telephone calls. In response, the Office developed a "best practices" guideline for recording customer telephone calls. Essentially, the guideline states that the taping of telephone calls involves the collection of personal information – a practice that should meet fair information principles. In other words, conversations should not be taped unless it is for a purpose that a reasonable person would consider appropriate in the circumstances. The customer must be informed of the purpose for taping the call and must consent, except in certain limited cases where consent is not required, before the taping begins. The customer should also be offered an alternative, such as not taping the call, visiting a retail outlet, writing a letter, or conducting the transaction over the Internet.

A tape recording captures more than just the specifics needed for the purpose of the call. It records comments, accents and attitudes – information that may not be relevant to the material required. For these reasons, it is important for organizations to be open with customers – to advise them that they record,

explain why they record, and offer them options if they do not want to be recorded.

In both complaints, we provided the banks with our "best practices" guideline and both organizations undertook improvements to their recording practices. In the first case, the bank now notifies customers at the beginning of a call that the conversation is being taped and provides them with alternative means of communicating their information should they not wish to proceed with the call. In the second case, the bank introduced a recorded message to inform all callers that conversations would be tape-recorded.

ISP holds e-mails "hostage"

A customer had complained when she learned that her Internet service provider (ISP) was continuing to receive and store her incoming e-mails while her account was suspended. This is in fact standard industry practice. Many ISPs use continued receipt and storage of e-mails as leverage in collecting on overdue payments.

In this case, the former Commissioner determined that the ISP had not properly informed the complainant of purposes related to the use of her personal information during an account suspension and had thus used her personal information without her informed consent for purposes other than those for which the information had been collected. On this basis, we concluded that the complaint was well-founded.

But this case left the Office highly concerned about the practice at issue, which we knew to be widespread in the industry. In the letters of findings, the former Commissioner commented as follows:

> *"… As Privacy Commissioner, I am concerned about the implications of storing and withholding potentially important messages without informing the intended recipient of their existence or the sender of their non-delivery. As an occasional sender of e-mails myself, rather than be falsely led to believe that a certain message had gone through unimpeded, I would much prefer to have it*

returned with a notification of non-delivery so that I could try to reach the intended recipient by other means. Indeed, returning the message with a notification strikes me as the most appropriate and responsible course of action for an Internet service provider to take in such circumstances."

To answer the above question, then, what an ISP should do in cases of account suspension is what we recommended as best practices in the case in question, as follows:

- Cease collecting, storing, and denying access to, e-mails addressed to holders of accounts under suspension.
- Adopt instead the practice of deflecting such e-mails back to senders with notification to the effect that the messages could not be delivered.
- Make provision for giving the holder of a suspended account access to any e-mails already received by the company, but still unretrieved by the customer, at the time the suspension took effect.

Make sure to check those Government authorities

An individual's holiday memories were marred when he found out that the airline he had used for his trip released his itinerary to his boss. His employer, a federal Government department, was conducting an investigation into his use of sick leave. It approached the airline and requested confirmation of his travel itinerary.

The airline hesitated. Citing its responsibilities under the *PIPED Act*, it asked the department for proof that the individual had consented to such a disclosure. If that was not possible, the airline suggested that a specific exemption or exception under the *Act* would be needed before it would comply with the request.

In response, the department cited a directive under the authority of a specific federal statute, indicated that the information was needed to administer federal public servants' employment legislation, and asked the airline to disclose the itinerary. Satisfied that the department's request fit the exemption

provided in section 7(3)(c.1)(iii) of the *Act*, the airline duly released the information. This section allows an organization to release information about an individual to a Government institution for the purpose of administering a law.

There was just one problem. The department did not quote the correct directive as its lawful authority. Even though it later acknowledged its mistake, the department maintained that it nevertheless had the authority to collect the information – just under different legislation.

We agreed that the department had lawful authority. We were concerned, however, that the department had initially made an error and that the airline had not verified whether the cited directive was correct or not. Although the airline made the disclosure in good faith, an organization has a duty to be vigilant about checking authorities cited by Government organizations before releasing personal information. In his letter of findings the former Commissioner stated:

> *"…where requests for disclosure of personal information are concerned, I consider it incumbent upon any private-sector organization not to take the submissions of any government institution at face value, but rather to be vigilant about checking authorities cited."*

Fees for access: Should you have to pay for your own information?

Responding to requests for access to personal information may entail some costs for organizations. Should it also entail costs for the individual? In fact, there is a provision in the *Act* that allows organizations to charge a fee in responding to requests. But how much is reasonable? This question was addressed in two cases where the complainants accused organizations of charging excessively high fees.

The complainants were involved in disputes with their respective banks concerning money they had borrowed. Both individuals requested their personal

information. The banks responded by demanding fees of $150 and $200 respectively to cover the costs of processing the documents in question. The first individual wanted to know what he would get for his money and when told what this would be decided to file a complaint. The second individual is on a fixed income and could not afford to pay for his personal information.

These cases are good examples of the private sector adjusting to the expectations of the Act.

These cases are good examples of the private sector adjusting to the expectations of the *Act*. The banks were reminded that Principle 4.9.4 of the *PIPED Act* stipulates that an organization must respond to an individual's request at minimal or no cost to the individual. As a result, one bank released the information free of charge, while the other asked for a nominal fee of $10.

Additionally, the bank's position in the first complaint seemed to be based not only on cost-recovery but also on its desire to have the complainant meet with it to discuss the dispute that had prompted the access request in the first place. We emphasized to the bank, however, that the *Act* does not require an individual to explain why he or she wants access to personal information or require that he or she enter into any discussions with an organization. In other words, personal information cannot be held for ransom.

Based on the findings in these cases, the bottom line for organizations when it comes to fees is this: cost-recovery does not apply to access to information requests.

A security clearance becomes a job requirement

Protecting nuclear sites from terrorist attacks is a grave concern, particularly in the wake of September 11, 2001. The federal agency that oversees the operations of all nuclear facilities in Canada responded to the terrorist threat by instructing its licencees to implement enhanced security measures. One of

the new measures in place is to limit entry to nuclear facilities to persons with the proper security clearance. If a licencee fails to comply, the federal agency will revoke its operating licence.

A company's nuclear products division informed its employees of the new security requirement and asked them to consent to a security clearance check. Along with a consent form, each employee received an information package that specified the type of information to be collected, the purpose, and the organization that would carry out the collection. Employees were also told that the organization collecting the personal information was bound by a confidentiality agreement.

In order to be granted a security clearance, employees with at least ten years of service were required to pass a criminal records check. Employees with less than ten years of service had to pass a full background check that included employment history, professional qualifications, and personal references, as well as a criminal records check.

Some employees were unhappy and complained to the Office. They felt they did not really have a choice – if they refused, they faced job loss. If they consented but failed the security check, they would lose their current positions and be reassigned, possibly to lower paying jobs. Under those circumstances, they felt their consent was coerced.

The former Commissioner had to determine whether the company was collecting personal information with the employees' knowledge and consent as required under Principle 4.3 of the *PIPED Act*. Clearly, the employees knew of the collection. But was their consent voluntary? In the letters of findings, the former Commissioner assessed the issue as follows:

> *"[The company] expressly asked you for your consent, and it is entirely up to you whether to give it or not. That there may be unpleasant consequences in either case does not alter the fact that you do have a choice in the matter. Refusal to give consent to the collection of personal information may very often entail unpleasant consequences for the individual. But in this case, as in most*

decisions in life where the prospect of unpleasant consequences is a factor, the pressure you may feel to consent to the collection does not amount to duress. Under the Act, the key consideration is not whether there may be unpleasant consequences to an individual's refusal to give consent, but rather whether the collection is itself reasonable."

Was it reasonable for personal information to be collected for the purposes of a security clearance as stipulated by section 5(3) of the *Act*? The former Commissioner concluded that it is entirely reasonable for the federal agency to impose an enhanced security requirement upon its licencees, given the greatly enhanced concern about possible acts of terrorism at nuclear facilities. Had the company not complied, it would have lost its licence to produce nuclear fuels and would no longer have been able to conduct its nuclear products business, leading to substantial financial losses and staff lay-offs. Under these circumstances, we determined that it was entirely reasonable for the company to comply with the order and thus collect personal information from employees to conduct security clearance checks.

Aeroplan: Opt-out consent is not enough

When Air Canada mailed out privacy brochures to 60,000 Aeroplan members, several members complained to the Office.

The individuals who complained to the Office did not mind that the company had made the effort to seek their consent to information-sharing practices under the Aeroplan program. What they did object to, however, was having the onus put on *them* to tell Air Canada if they did *not* consent to the practices outlined in the brochure. Nor did they appreciate that the company was presuming, in the meantime, that they did consent.

The former Commissioner concluded that Air Canada was not in compliance with the *PIPED Act* and that the complaints were well-founded.

The 60,000 brochures accounted for only about one per cent of Aeroplan's total membership at the time. In the letters of findings, the former Commissioner

remarked that the *Act* required organizations to observe every individual's privacy rights and did not allow for token compliance. Since Air Canada had in effect left 99% of Aeroplan members in the dark about its information-handling policy and practices, the former Commissioner found its attempt at seeking consent to have been entirely inadequate.

Even if all plan members had been consulted, the brochure itself failed to seek consent in an appropriate form. It described five ways in which Air Canada was intending to share Aeroplan members' personal information under the program. Each description was accompanied by a check-off box, and the plan member was instructed to check the box only if he or she did not consent to having personal information shared in the manner described. Any plan member checking off one or more of the five boxes was then expected to mail the brochure back to the company by way of expressing non-consent. Conversely, any plan member who did not return the brochure was considered to have consented to all five information-sharing situations.

This form of consent has come to be known as "negative" or "opt-out" consent. It correlates to the "negative option" marketing practices that consumers have been so quick to condemn in the past. In effect, such practice is based on presumption – the individual is presumed to agree to a proposition unless he or she takes the initiative to refuse it.

Like most other people involved in the protection of privacy, and indeed like most informed consumers, we hold a very low opinion of the negative option as it is used

Like most other people involved in the protection of privacy, and indeed like most informed consumers, we hold a very low opinion of the negative option as it is used by organizations in their handling of personal information.

by organizations in their handling of personal information. The Office considers opt-out to be a weak form of consent – one that unfairly puts the onus of initiative on the wrong party and reflects at best a mere token observance of what is perhaps the most fundamental principle of the *Act*. We would prefer that organizations adopt an exclusively "positive" or "opt-in" approach – a much more respectful approach whereby individuals would be deemed to have consented only if they have expressed a definite "yes" to a proposition.

On the other hand, the Office is also well aware that opt-out is a form of consent expressly permitted by the *Act* in certain circumstances – notably, where the personal information is of a demonstrably non-sensitive nature. The problem here is that the *Act* itself refrains from precisely defining the notion of sensitivity. Although it does instruct that an individual's financial and medical information is almost always to be considered sensitive, it also goes on to suggest that any information can be sensitive, depending on the context. In the Aeroplan complaints, therefore, the Office's task was essentially one of assessing the context. In other words, the former Commissioner had to determine whether the circumstances justified Air Canada's recourse to opt-out consent.

In the letters of findings, the former Commissioner made a point of stating that the intention is always to keep strict limits upon the circumstances in which opt-out could be deemed appropriate. It was also made clear that the Office intends to be guided in all such deliberations by due consideration for both the sensitivity of the information and the reasonable expectations of the individual. It was on these considerations that the Aeroplan privacy brochure ultimately failed.

The language of the brochure failed to demonstrate that any of the information-sharing situations described was strictly non-sensitive in nature or context. Two of the situations were of a particularly high order of sensitivity. The other three seemed by their descriptions to allow for considerable marketing to individuals on the basis of information customized according to potentially sensitive criteria. As it was put in the former Commissioner's letters:

> *"Although in my view the practice of sharing plan members' information for purposes of offering special promotions and products remains unobjectionable in itself, I am satisfied that a reasonable person would not expect such practice to extend to the 'tailoring' of information to the individual's potentially sensitive interests, uses, and preferences without the positive consent of the individual."*

The former Commissioner concluded that it had been inappropriate for Air Canada to seek negative or opt-out consent to Aeroplan's information-sharing policies and practices as described in the brochure.

To its credit, Air Canada took the Commission's findings and recommendations very seriously. With some guidance from the Office, in a process that we found to be both positive and productive, the company undertook to rethink and rewrite its information-sharing policy under Aeroplan. We have reviewed the finished product, and have verified that the policy now addresses our concerns in the following ways:

- It explains to Aeroplan members, in clear and understandable terms, the purposes for the collection, use, and disclosure of personal information under the program.
- It explains clearly that Aeroplan does not collect any details of the transactions whereby members accumulate points under the program.
- It specifies that Aeroplan does not provide individualized profiles of members to partner companies or other third parties, and further clarifies that any information provided to partners can be used only for purposes related to the Aeroplan program.
- It explicitly and clearly states that members who wish to have their personal information used only for redemption of Aeroplan points can so stipulate, and it identifies an easily-executable procedure for members to exercise this option.

As for the matter of consulting the full Aeroplan membership, Air Canada also set out a very specific plan whereby all active members of the program would

receive a copy of the revised policy with their next account statements. Moreover, the policy was to be made available on the Aeroplan Web site.

We were satisfied that Air Canada had responded appropriately to our recommendations, and pleased with the spirit of co-operation the company has shown.

A case of deception

It is one thing to do a poor job of informing individuals of the purposes for which their information would be used, as three of the above-mentioned organizations did. It is quite another to deliberately misinform, as we found to be the case in a complaint against a market research firm.

This firm mails questionnaires for what it calls "consumer product surveys" to households across Canada. The questionnaires ask about household preferences among various categories of products. The literature accompanying each questionnaire explains the purpose of the survey strictly in terms of "fact-finding," seeking householders' "opinion" and understanding consumer "preferences and attitudes," all with a stated view to improving the quality, life and value of products.

However, the surveys were truly intended for the purpose of selling products to the survey respondents. What the survey firm mainly intends to do with the personal information it collects in the questionnaires is compile customized mailing lists, which it will then give to the third-party companies that have commissioned the given survey. These commissioning companies will then attempt to sell products to the survey respondents by directly marketing them according to the information they have provided in the questionnaires.

The *PIPED Act* says that an organization has to identify its true purposes for collecting personal information. It also says that consent to the collection of personal information must not be obtained through deception.

If an organization intends to give information it collects to direct marketers, it has to say so, in no uncertain terms and in a manner that people can reasonably understand. In the survey literature in question, there is neither an explicit statement nor even a reasonably understandable implication to the effect that personal information of individual respondents will be disclosed to third parties.

If an organization intends to give information it collects to direct marketers, it has to say so…

The questionnaire does ask for the respondent's consent to further mailings and offers, but says nothing about where such communications would come from. In the absence of any indication that the survey firm intends to share the respondent's mailing address with other possible mailers, the most reasonable inference would be that any further mailings would come from the same source as the original – that is, from the survey firm itself.

Furthermore, the consent mechanism is a problem in itself. Given that many of the survey questions are highly sensitive in nature (notably, several have to do with personal health and finances), the "opt-in" form of consent should be used in the circumstances. But the consent mechanism has two check-off boxes, one for "yes" and the other for "no", and is thus ambiguous as to the form of consent intended. What happens in fact, however, in the not-infrequent cases where the respondent checks off neither box, is that the individual is presumed to give consent to further mailings. Thus, the survey firm is using the "opt-out" form of consent in a situation that clearly calls for "opt-in."

The survey literature also does mention that companies have commissioned the survey. However, it does not name the commissioning companies. Nor does it in any discernible way suggest that these anonymous companies are direct marketers, or that what they have in effect commissioned from the survey firm is the collection of prospective customers' personal information on

their behalf. Indeed, there is nothing in the literature that gives the individual householder any substantial grounds to believe that the survey is anything other than what it purports up front to be – that is, strictly a fact-finding, opinion-seeking market study aimed at product improvement.

On the basis of such a description, respondents might reasonably expect that the survey's sponsors would receive results in the form of aggregated, anonymized analytical data. But respondents are given no legitimate reason to expect, and every good reason to resent, that as a result of their participation in the survey they may soon be subject to intrusive and unwanted direct-marketing efforts by third-parties who have been made privy to their sensitive personal information.

It may seem paradoxical to some that, despite the overwhelming case against the survey firm on these and other counts, what troubled us most was evidence of the firm's *compliance* with the *Act*.

The firm does, in fact, have an official written privacy policy pertaining to its household surveys posted on its Web site. This policy does a relatively good job of identifying the true purposes for collecting the survey information. However, not only is this policy not included or otherwise reflected in the survey literature mailed to households, but it is not made reasonably accessible to householders. The survey literature does not even mention the existence of the Web site, let alone that of the policy.

What troubled us specifically were the implications of the vast discrepancy in compliance between the Web site and the survey literature. In the letters of findings, the former Commissioner raised the concerns as follows:

> *"Why would [the firm] make reasonably clear in a remote and unadvertised privacy policy, but not at all clear in survey materials actually provided to individuals, that respondents' personal information would be disclosed to third parties for marketing purposes? Why in the survey materials would [the firm] explain the purposes of its surveys only in such limited terms as fact-finding, opinion-gathering, and product quality improvement, and relegate to a document*

that no one would ordinarily ever see the further purpose of direct marketing by third parties? Indeed, why would [the firm] take pains to formulate a more or less compliant privacy policy and then not draw attention to that policy when it truly mattered, in effect hiding the policy from customers?

"In brief, I find it difficult to comprehend this discrepancy, except in terms of deception. [The firm] has suggested that its survey materials serve to produce a reasonable expectation of disclosure to, and direct-marketing by, third parties. I cannot see, however, that any previously unsuspecting person could reasonably infer such a purpose from the scant, vague, and misleading indications provided. Rather, in my considered view, far from being conducive to a reasonable understanding of how personal information will be used or disclosed, the survey materials serve only to deceive individuals as to the true purposes of the surveys and to detract from the fairness of [the firm's] collection of personal information."

An advocacy group's expectations about consent

The *PIPED Act* states, at Principle 4.3.5 of Schedule 1, that the reasonable expectations of the individual are relevant in matters of consent. But it does not elaborate.

Rather, it leaves us the difficult task of interpreting this provision. In the circumstances of any consent-related complaint, it is often up to the Commissioner to determine the reasonableness of a complainant's expectations and the extent of their relevance. Fortunately, fairly early in the life of the *Act*, a body of complaints arose that we found useful in formulating a general position on what an individual may reasonably expect in matters of consent.

An individual filed complaints on behalf of an advocacy group against two banks, a telecommunications company, and a company that ran a frequent-buyer program. All the complaints were basically the same – that the organizations in question were not obtaining valid informed consent from individuals to disclosures of their personal information for marketing purposes.

To us, these assumptions clearly represented "expectations" on the complainant's part.

The complaints consisted of two main allegations. The first was that the organizations were not making reasonable efforts to inform clients that their personal information was to be disclosed to third parties for secondary marketing purposes – that is, purposes additional to those for which the information needed to be collected in the first place. The complainant's contention was that, if individuals were not being properly informed of secondary purposes, the organizations had no valid basis for presuming the individual's consent to such purposes. The second main allegation was that, despite their reliance on the "opt-out" form of consent, the organizations were not providing reasonable opportunities for individuals to opt out of third-party marketing.

As interesting as the allegations themselves were their underlying assumptions, which the advocacy group had presented in a position statement supporting the complaints. To us, these assumptions clearly represented "expectations" on the complainant's part. Before determining whether or not the organizations in question were in compliance with the relevant consent provisions of the *Act*, we thought it prudent to consider whether the group's expectations regarding consent were themselves reasonable in relation to the *Act*.

After analyzing them, the former Commissioner concluded that the group's expectations were entirely reasonable. Notably, the former Commissioner found it reasonable to expect the following from organizations that use or disclose personal information for secondary purposes:

- It is not enough to identify purposes in privacy policy documents and make such documents generally available. An organization should bring its secondary purposes directly to the attention of the individual at the time of

collecting personal information. During an application or a subscription process, for example, the individual should be presented with the necessary information and should not be referred to sources not immediately at hand. (These expectations are supported by Principles 4.2.3 and 4.3.1 of the *Act*, which instruct that identification of purposes and seeking of consent be direct and coincident with the collection of personal information.)

- Purposes should be stated in clear, plain language understandable to the ordinary consumer and in adequate detail for the consumer to appreciate the nature and extent of the intended collections, uses, and disclosures. (These expectations are supported by Principle 4.3.2, which instructs that purposes be stated in such a manner that the individual can reasonably understand how personal information will be used or disclosed.)
- If purposes are identified in writing, the individual should not be required to read fine print in dense passages.

Where an organization intends to presume the individual's consent to secondary purposes, the organization should provide a convenient opportunity for the individual to opt out. The opportunity and the procedure for opting-out should likewise be brought to the individual's attention at the time of collecting the personal information. The opting-out procedure should be easy, immediate, and inexpensive.

On this basis, and upon investigation of the actual policies and practices of the organizations, the Commissioner concluded that two of the complaints were well-founded and two were not. The former Commissioner found that the telecommunications company was not making any disclosures of the kind alleged, since it was prohibited from doing so by the CRTC. One bank was indeed disclosing personal information for secondary marketing purposes as alleged, but the former Commissioner found it to be making reasonable efforts on the whole to inform account applicants of the practice, obtain their consent to it, and provide them with an opt-out opportunity.

In the well-founded cases, the non-compliance of the frequent-buyer program was largely a matter of inconsistency in enrolment procedures. The case of the second bank, however, was much more serious. This bank's efforts at obtaining informed consent from account applicants did not in any respect meet the requirements of the *Act* or the reasonable expectations of the individual. In the letter of findings, the former Commissioner commented on the various materials used by the bank to communicate purposes, and on the nature and extent of the failed compliance in this case:

> *"The wording … is so broad in each case as to virtually preclude understanding, unless the individual is to understand that the bank intends to use personal information however it may see fit and disclose it to whomever it may see fit. This would hardly be a purpose that any reasonable person would expect or consider appropriate in any circumstances."*

By positive contrast, it should be noted that, in the case of the first bank, the former Commissioner complimented the bank on its approach to obtaining informed consent from account applicants. For those applying in person at branches, this bank's application procedure involved sitting the individuals down, providing them with the appropriate privacy information on the spot, drawing their attention specifically to statements of secondary marketing purposes, asking whether they consented or not to specific marketing practices, and recording and abiding by their responses. We regard such procedure as exemplary, amounting to the positive form of consent that we prefer.

Consent to secondary purposes

What follows is a summary of the deliberations to date in cases relating to consent to secondary purposes.

- Positive or opt-in consent is always to be preferred as the form of consent that is strongest, most respectful of individuals, and best in keeping with the spirit of the *Act*. Organizations are encouraged to adopt this form of consent exclusively.

- Positive or opt-in consent to secondary purposes is a requirement in situations where the personal information is sensitive in itself or where there is a significant potential for the information to be rendered sensitive in the context of the information-handling activities.
- Since the *Act* indicates that personal information of a financial or medical nature is almost always to be considered sensitive, these types of information will almost always be deemed to warrant positive consent. However, since the *Act* also stipulates that any personal information may be sensitive in a given context, no further attempt should be made to precisely define the notion of sensitivity. Rather, the context should be considered in each case, with a view to determining the potential for sensitivity.
- Two prime considerations in determining the potential for sensitivity of personal information are the intent to disclose the information to third parties and the intent to categorize or otherwise process the information according to personal criteria.
- Negative or opt-out consent, also known as presumed consent, despite being the weaker and less preferable form, is recognized under the *Act* as being acceptable in certain circumstances. The scope of circumstances in which this form of consent is allowable will remain limited.
- An organization's use of the negative or opt-out form of consent to secondary purposes will be deemed justified only under the following conditions:
    - The personal information must be of a demonstrably non-sensitive nature and context and must be identified by item or type.
    - If the information is to be disclosed to third parties, the parties must be identified by name or type.
    - The organization must state its purposes in full accordance with Principles 4.2, 4.2.3, 4.3.1, and 4.3.2 and with the individual's reasonable expectations as deemed relevant in Principle 4.3.5. Specifically, the identified purposes must be brought directly to the individual's attention, either orally or in writing, at the time the personal information is collected (e.g., during the subscription, application, or enrolment process); in clear, specific, unambiguous terms; in

a format easy to read (where text is used); and in a manner conducive to the individual's understanding of how exactly the personal information is to be used or disclosed.

- The organization must provide an appropriate "opt-out" mechanism – that is, a convenient opportunity and procedure for withdrawal of consent. The mechanism must be brought to the individual's attention at the time the personal information is collected and should be inexpensive, easy to execute, and immediately effective in withdrawing consent. Where feasible, it should include a toll-free number.

INCIDENTS UNDER THE *PIPED ACT*

Checking up on telephone calls

A journalist contacted the Office about a survey being conducted on behalf of a telephone company by a research firm. It appeared as though the company was gathering information from customers about their telephone calls.

The research firm had a contract with the telephone company to carry out random checks for quality assurance purposes. The telephone company provided the firm with the phone number of customers who had made calls seeking assistance by dialing "0" or "411." The firm was not given the names of the customers or other identifying information. The company has a non-disclosure contract with the research firm, which requires the firm to destroy the information it collects once the results of the survey are compiled.

The former Commissioner was satisfied when it was determined that the telephone company was complying with a CRTC requirement to conduct regular quality of service measurements of the accuracy of Directory Assistance services.

Dumpster find

A bank alerted the Office that confidential client documents had been found in a dumpster located near a branch that had closed some time earlier. The building had been leased to a new tenant and was being renovated. Apparently the renovators found the documents during the reconstruction and disposed of them. Upon hearing of the matter, the media retrieved some of the documents from the dumpster.

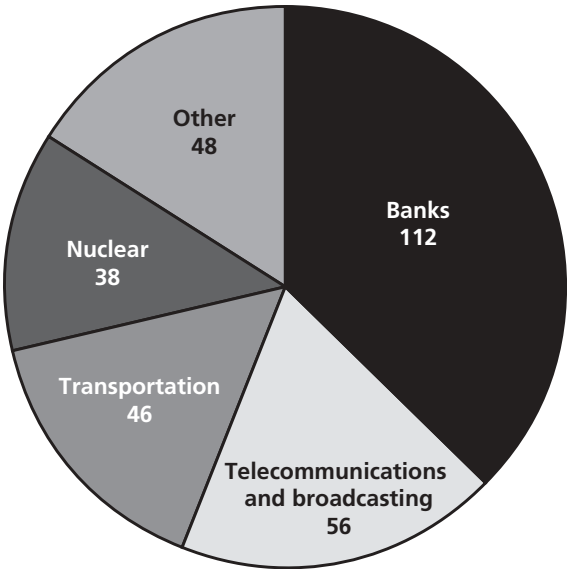
The bank took prompt action as soon as it became aware of the situation by recovering all of the documents from the dumpster and the journalists; then it verified that no other bank documents remained in the building. The bank also informed each of the affected customers, either in person or in writing, of the incident and of the steps it had taken to recover the documents. In addition, the bank apologized to each customer and assured each one that all of their information had been recovered.

It was determined that the branch in question was amalgamated with another, and a private company on contract to the bank was tasked with sorting through and processing records. The bank has established procedures for this, but the private company did not follow these properly, with the result that some documentation was not appropriately classified and was disposed of incorrectly. The bank subsequently clarified procedures with the private company.

The former Commissioner was satisfied that the bank acted promptly and appropriately in dealing with this sensitive situation.

Complaints Received by Sector

January 1, 2002 to December 31, 2002



Inquiries under the *PIPED Act*

January 1, 2002 to December 31, 2002: 8,381

We will attempt to provide a breakdown of these inquiries by subject in future Annual Reports.

PRIVACY PRACTICES AND REVIEWS

The *Personal Information Protection and Electronic Documents (PIPED) Act* enables the Commissioner to audit the compliance of private sector organizations if there are reasonable grounds to believe that they are in contravention of the *Act* or are not following a recommendation set out in Schedule 1 (ten principles). The Privacy Practices and Reviews (PP&R) Branch will conduct such compliance reviews and audits under section 18 of the *PIPED Act*, following accepted standard audit objectives and criteria. During the period under review, there were a number of issues that were brought to the Commission's attention that were successfully resolved without the necessity of conducting an audit. For example, Office of the Privacy Commissioner staff met and advised representatives of an industry association on the viability of obtaining direct consent and the proposed contents of such a consent form. We provided guidance to a business with respect to the use of the SIN as an identifier and the use of opt-out consent. As well, we provided a comprehensive review and analysis of a corporate privacy policy.

Apart from those issues, the former Commissioner was not aware of any other concerns that would provide sufficient grounds to initiate an audit under the law.

Nevertheless, the PP&R Branch has been involved in consulting with and providing advice to private sector organizations that come under the jurisdiction of the *PIPED Act*. It has also assisted those organizations that are not currently governed by the *Act* but that are preparing for January 1, 2004, when the *Act* will begin to apply to them.

IN THE COURTS

Under section 14 of the *Personal Information Protection and Electronic Documents (PIPED) Act*, an individual complainant has a right, following the Commissioner's investigation, to apply to the Federal Court of Canada for a hearing in respect of any matter that is referred to in the Commissioner's report. These matters must be among those in the listed Schedule clauses and sections of the *PIPED Act*.

Section 15 of the *Act* allows the Commissioner to apply to appear in Federal Court. The Commissioner may, with the consent of the complainant, apply directly to the court for a hearing in respect of any matter covered by section 14; appear before the Court on behalf of any complainant who has applied for a hearing under section 14; or, with the leave of the Court, appear as a party to any section 14 hearing.

Following is a list of all *PIPED Act* applications in the courts from January 1, 2001 to December 31, 2002:

Mathew Englander v. Telus Communications Inc.

Federal Court File No. T-1717-01

This is the first application for judicial review to be filed in the Federal Court under the *PIPED Act*. Mr. Englander argues that Telus uses and discloses customers' names, addresses and telephone numbers in its white pages directories and otherwise, without customers' knowledge and consent, and inappropriately charges customers for choosing to have their telephone number "non-published." He claims that these actions by Telus contravene subsections 5(1) and (3) of the *PIPED Act,* as well as several clauses of Schedule 1 of the *PIPED Act*.

Status

This Application was dismissed on June 2, 2003.

Ronald G. Maheu v. the Attorney General of Canada and IMS Health Canada

Federal Court File No. T-1967-01

Ronald Maheu applied for a hearing in the Federal Court arguing that IMS Health Canada improperly discloses personal information by selling data on physicians' prescribing patterns without their consent.

Status

Mr. Maheu filed an Amended Notice of Application in March 2002. IMS brought a motion seeking either to strike out the Application on the grounds that it was brought for an improper purpose or to have Mr. Maheu post security for costs. The Court ordered Mr. Maheu to post security for costs in the amount of $12,000 and noted that there appeared to be reason to believe that Maheu was using the *Act* for a collateral and improper purpose given that his own personal information was not at issue. On appeal, the former Commissioner appeared to assist the Court with respect to the proper interpretation of the *PIPED Act*, explaining that an individual may file a complaint concerning an organization's information practices regardless of whether that organization collects, uses or discloses personal information about the individual complainant. The Federal Court agreed with this position and granted Mr. Maheu's appeal on January 3, 2003. This decision is currently being appealed, and the original Application continues to proceed in Trial Division.

Diane L'Ecuyer v. Aéroports de Montréal

Federal Court File No. T-2228-01

Diane L'Ecuyer complained that Aéroports de Montréal had sent copies of a letter of response to access requests she had made to two union representatives and an employee relations co-ordinator and had, therefore, disclosed personal information without her consent. The former Commissioner investigated her complaint and, among the findings, recommended that individuals must be allowed to judge for themselves whether or not to share such a response with others.

Status

Madame L'Ecuyer applied to Federal Court on December 18, 2001, seeking an Order that the organization correct its practices to conform with the *PIPED Act* and that the organization publish a notice stating any action taken or proposed to be taken to correct its practices. On May 13, 2003 the Trial Division released its decision, finding that the issue arose from the administration of a collective agreement and therefore was not within the jurisdiction of the Privacy Commissioner. Madame L'Ecuyer filed an appeal of that decision on June 5, 2003 and the Privacy Commissioner is preparing to apply for leave to intervene in that appeal.

Nancy Carter v. Inter.net Canada Limited

Federal Court File No. T-1745-02

Nancy Carter contacted the Office with concerns about the practice(s) of her Internet Service Provider (ISP). During a billing dispute with the complainant, the ISP had suspended her access to e-mail, but continued to keep the account active and accepted new e-mails into the mailbox. The claimant argues that she was therefore denied access to her personal information contrary to the *PIPED Act,* and lost a valuable business opportunity as a result. She is seeking damages under the *PIPED Act*.

Status

A settlement was reached in this case and accordingly a Notice of Discontinuance was filed on June 5, 2003.

Sylvain Gagné v. Bell Canada

Federal Court File No. T-1971-02

Sylvain Gagné complained to the Office that (a) that he had been denied access to some of his personal information and (b) of the improper disclosure of the personal information of others. Although the former Commissioner found the denial of access complaint to be not well-founded, agreeing that exemptions under 7(1)(b) and 9(3)(c.1) had been correctly applied, the complaint about the disclosure of personal information was well-founded and the former Commissioner issued recommendations as to change of practices.

Status

The Notice of Application was filed in Federal Court on November 25, 2002, requesting a variety of relief, including access to the withheld documents, damages to those affected, and Orders enforcing the Office's recommendations.

Bell Canada has now agreed to follow the Office's recommendations, and thus a Notice of Discontinuance was filed on March 14, 2003.

Dale Stuart v. the Toronto Dominion Bank

Federal Court File No. T-290-02

Dale Stuart believed that information about his banking affairs had been disclosed by employees of the TD Bank to his employer without Mr. Stuart's knowledge or consent.

Status

This application was discontinued by Mr. Stuart on December 2, 2002.

Yukon Hospital Corporation v. Attorney General of Canada

Federal Court File No. T-1814-02

This action was initiated in response to the former Commissioner's determination that he had jurisdiction under section 4(1)(b) to conduct an investigation of a complaint filed against the Yukon Hospital Corporation.

Status

A complaint was filed with this Office under the *Privacy Act*. Although the Yukon Hospital Corporation is governed by the *PIPED Act*, the complaint was originally made under the *Privacy Act*. After discussions with the Applicant to this effect, the former Commissioner withdrew his decision to investigate the complaint. Court proceedings were discontinued on February 21, 2003.

Keith Vanderbeke v. Royal Bank of Canada

Federal Court File No. T-2185-02

Keith Vanderbeke contacted the Office complaining that the Royal Bank of Canada had denied him access to three documents pertaining to a commercial mortgage for which he personally was the guarantor.

Status

In the application, the claimant is specifically seeking (among other things) interpretive Orders relating to the *PIPED Act*: an Order that a private corporation may be an "identifiable individual" under the *PIPED Act* with attendant access rights; and an Order that private corporation banking documents should be considered personal documents where a natural person has provided a personal guarantee to the creditor. It is uncertain whether this aspect will be allowed to continue because, among other things, the part of the Application apparently brought pursuant to section 14 of the *PIPED Act* improperly seeks review of the former Commissioner's findings. Under section 14 of the *PIPED Act*, the only proper respondent is the Royal Bank of Canada.

Part Three

Corporate Services

On April 1, 2002, the Office of the Privacy Commissioner of Canada ceased to share corporate services with the Office of the Information Commissioner of Canada, and established its own Corporate Services Branch.

The Corporate Services Branch provides advice and services in the areas of finance, human resources, information technology and administration to the Office's senior managers and staff.

As noted in the Foreword, the House of Commons Committee on Government Operations and Estimates has, in the course of examining the operations of the Office, uncovered a number of serious problems related to some of these areas. As well, the Office is the subject of reviews by both the Office of the Auditor General of Canada and the Public Service Commission of Canada.

I intend to use the results of these reviews to ensure that the Office is managed in a manner that is accountable to Parliament and respects the polices and regulations applicable to the public service.

At the beginning of fiscal year 2002-2003, the Office's budget was $11.1 million, the same as our budget for the previous year. During the course of the year,

our budget was adjusted upward by $773,000, primarily to offset increased legal costs, costs associated with the Government's new Privacy Impact Assessment Policy and collective bargaining salary increases, for a total budget of $11.9 million.

Our expenditures totalled $12.2 million. We exceeded our budget by $240,000 largely due to changes in accounting practices in order to be consistent with the principles of accrual accounting in the federal government.

The Office is currently reviewing its financial resources, in conjunction with the Treasury Board Secretariat, to ensure that it has the resources needed to fulfill its obligations in fiscal year 2003-2004 and beyond in anticipation of the full and final implementation of the *PIPED Act* on January 1, 2004.

Resources

April 1, 2002 to March 31, 2003

	Expenditure Totals ($)	% of Totals
Privacy Act	5,208,588	43%
PIPED Act	5,582,722	46%
Corporate Services	1,367,778	11%
Total	**12,159,088**	**100%**

Note that as of March 2003 there were 103 full-time staff at the Office of the Privacy Commissioner of Canada.

Detailed Expenditures[1]

April 1, 2002 to March 31, 2003

	Privacy Act	***PIPED Act***	**Corporate Services**[2]	**Total**
Salaries	3,462,955	2,845,391	808,513	**7,116,859**
Employee Benefits Program	657,386	595,000	240,220	**1,492,606**
Transportation and Communication	284,228	352,412	67,005	**703,645**
Information	25,649	315,406	34,592	**375,647**
Professional Services	679,897	700,870	65,526	**1,446,293**
Rentals	12,840	2,202	11,648	**26,690**
Repairs and Maintenance	8,607	41,249	5,447	**55,303**
Materials and Supplies	44,328	5,012	51,699	**101,039**
Acquisition of Machinery and Equipment	29,100	725,180	83,128	**837,408**
Other Subsidies and Payments	3,598	-	-	**3,598**
Total	**$5,208,588**	**$5,582,722**	**$1,367,778**	**$12,159,088**

Notes:

[1] Total expenditure figures are consistent with public accounts.

[2] Effective April 1, 2002, Corporate Services is part of this Office and resources are no longer shared with the Office of the Information Commissioner of Canada.