Privacy Commissioner of Canada

Commissaire à la protection de la vie privée du Canada

Privacy

Annual Report to Parliament 2005-2006

Report on the *Privacy Act*

Canada

Office of the 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. IP50-2006
ISBN 0-662-49235-8

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

June 2006

The Honourable Noël A. Kinsella, Senator
The Speaker
The Senate of Canada
Ottawa

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Privacy Act* for the period from April 1, 2005 to March 31, 2006.

Yours sincerely,

Original signed by

Jennifer Stoddart
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

June 2006

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 of the Office of the Privacy Commissioner of Canada on the *Privacy Act* for the period from April 1, 2005 to March 31, 2006.

Yours sincerely,

Original signed by

Jennifer Stoddart
Privacy Commissioner of Canada

Table of Contents

Foreword

Next year will be the 25th anniversary of the *Privacy Act*, Canada's first comprehensive privacy legislation. Revised from the 1977 part IV of the *Human Rights Act*, which recognized the basic principles and established a Privacy Commissioner who was a member of the Human Rights Commission, the *Privacy Act* was framed in the kind of thinking we had about government in the 1960s and 1970s. We worried about big central databases, run on huge mainframe computers. We talked about files, and we thought of records systems as paper files in filing cabinets. All that was before the personal computer, the Internet and powerful search engines like Google. Public servants did their work on paper, armed with typewriters filled out forms in triplicate.

Why am I wandering down memory lane? Because the world has changed in ways that are profound, and deeply troubling from the perspective of individual privacy and human rights. When we imagined powerful central computers which could impact privacy, armed with the new social insurance number to secure reliable matches, we lived in a world that was strictly bounded by capacity… the limited capacity to store data, the limited capacity to match data, the limited capacity to move data around and expose people to risk of privacy breaches. The Office of the Privacy Commissioner was designed as a small agency, with very limited powers, and Treasury Board Secretariat and the Department of Justice were tasked with implementing the new legislation and helping public servants to interpret it.

Now we live in a world that is strictly bounded by our capacity to understand it, by our ability to keep up with the pace of technological change, and to manage the new risks and security challenges that come with limitless storage capacity, limitless

transmission capacity, limitless data mining capacity. We are bounded by our own limited capacity to understand, to imagine the implications of data flow and data aggregation, and our ability to teach. The challenge of protecting data is increasingly globalized, because actions in one distant part of the world now may directly impact the privacy of Canadians. A spammer sending unwanted e-mail with spyware from somewhere in Eastern Europe can cause havoc in a Canadian internet service provider, wiretaps to detect anything from terrorism to money laundering are global in scope and application, and Canadian travellers need identity documents and financial instruments that will help them establish credentials as they do business around the world. Life is complicated, and so is privacy in today's world.

We need to understand the implications of countless new information systems, new laws and regulations, new systems of surveillance which are being constructed in the name of public safety. We need to audit more of these applications, to bring earlier insight and assistance to government departments who have a myriad of complex decisions to make and may not be as well versed in privacy matters as we are. We are determined to move forward with new resources and further enhance our ability to provide advice and assistance to Canadians, to Parliament and to the many public servants who are working to improve life for Canadians.

But at the risk of sounding like Oliver Twist, I want to say "Please sir, can I have some more?" It is my sincere hope that we can celebrate the federal public sector privacy law's anniversary with the knowledge that Parliament will give us a new *Privacy Act*. We need one that can respond to the age of information, to the challenges of ambient computing, to the reality of huge government systems that are capable of a surveillance we could not have dreamed of in 1982. Poll results suggest that more than 70% of Canadians have a high sense of erosion of their privacy and the protection of their personal information, and predict that it is one of the most important issues facing the country.

Canadians deserve real redress when things go wrong, not a Privacy Commissioner who has no power to even take a wrongful collection or a shameless disclosure of personal information to the Federal Court for a judgment and damages. We had started down a path of providing rights for Canadians in 1982, and we went a step further with the coming into force of the *Personal Information Protection and Electronic Documents Act* for the private sector in 2001, but we must now go further and ask our government to meet the standards that the power the information age demands. It is not acceptable that the standards for privacy protection are higher for the private sector than they are for the public sector.

We are proud to be hosting the International Conference of Data Protection and Privacy Commissioners in the fall of 2007 in Montreal. More and more, other countries, many of which will be attending this important event, are looking to Canada as a model for data protection. As an illustration of the interest other countries have in our data protection regime, we have had professional development activities with the authorities in Mexico, France and the U.K. Canada must keep its place as a leader in this area, and in my view this requires an update of the public sector law. It is simply not acceptable that we have higher standards for privacy protection in the private sector.

Real privacy demands a real balance of power between the citizen and the state, with real oversight and real power to intervene. We can do it, and we are anxious to get on with the real work it entails. As we committed, we have recently tabled with the Standing Committee on Access to Information, Privacy and Ethics our recommendations for amendments to the *Privacy Act* shortly, and we look forward to a fruitful dialogue.

Since my appointment as Privacy Commissioner in December of 2003, and certainly in the past fiscal year, my focus and that of my team has continued to be the institutional renewal of this Office. Rebuilding the Office had to take precedence. We also devoted our energies last year to a Business Case for long-term, stable funding, which involved an independent review of our activities and a presentation to a special Parliamentary Panel for their recommendation. I am pleased to report that the Office has now turned the page. We are moving forward with renewed vigour. We will continue our collaborative efforts with our provincial and territorial counterparts, as well as with our international colleagues, so that we can truly take on the significant privacy challenges ahead.

Our Strengthened Mandate

Our Office is responsible for overseeing compliance with both the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act (PIPEDA).* Although they are two separate laws, we manage the resources as a single pool. To date, our Office has not received permanent funding to carry out its duties under *PIPEDA* and the funding level for the *Privacy Act* has remained unchanged for many years. Funding for *PIPEDA* was granted for three years only. *PIPEDA* came into force in stages, beginning in 2001 and reaching full implementation in 2004, and we thought it important to let the dust settle before we attempted to identify long-term financial needs. *PIPEDA* has now been in full force for two years, and the demands made of us under both laws are increasing.

Funding levels for the administration of both Acts left us unable to carry out our multi-faceted mandate. We now have a significant backlog of complaints particularly under the *Privacy Act*, and complainants are, quite understandably, becoming impatient. The small size of our team of auditors makes it impossible to conduct effective audits to ensure compliance. Even though we have adopted a risk-based approach, we need to intensify our audit activities. Funding limits also mean that our communications strategy has been primarily reactive, when proactive public education about privacy rights and obligations is required instead. Similarly, our Policy and Research Branch and our Legal Services Branch have been confined to putting out existing privacy fires, rather than anticipating and therefore more effectively addressing emerging privacy issues.

In the past few years, the Office went through an extremely challenging period. However, every cloud has a silver lining. In this case, the silver lining was an opportunity to review the functioning of the Office, in detail, from top to bottom. The result is an Office of the Privacy Commissioner of Canada that is pointed in the

right direction. It is now time to put forward the Office's new vision and we need the full set of tools to implement it.

We are attracting new and highly specialized talent to our team. We have pursued an ambitious agenda to correct deficiencies in management of the organization. Audits and evaluations of our Office – by the Auditor General of Canada, the Public Service Commission and the Canadian Human Rights Commission – have so far been positive. And we have implemented a thoughtful, systematic process to determine our organizational needs. This Office is a stable institution worthy of the trust of Parliament and the Canadians it serves.

The Vision of the Office of the Privacy Commissioner of Canada

The Office has prepared two analyses of significance – a Vision and Institutional Service Plan, and a Business Case for Permanent Funding. Together, these describe who we need to be, for Canadians and on behalf of Parliamentarians, and what it takes to get us there.

If funded appropriately, the Office can accomplish the following in relation to the activities regulated under the *Privacy Act* and *PIPEDA*:

- undertake a meaningful number of audits and reviews to encourage greater compliance, and assist in developing a robust privacy management regime;
- work with government institutions, and conduct legal and policy analyses of bills and legislation to assist Parliament;
- make more proactive, extensive and effective use of the enforcement tools entrusted to us by Parliament, including Commissioner-initiated complaints, court actions and public interest disclosures;
- carry out research into emerging privacy issues and trends to help citizens and policy makers understand current and future privacy challenges;
- engage in public education to better inform individuals of their rights, and organizations of their obligations;
- through a streamlined investigation process, tackle the growing backlog of privacy complaints; and, finally,
- sustain institutional renewal efforts.

Business Case: Resources

This past year, our Office was pleased to take part in an innovative and entirely new process for seeking funding approval for the operations of Officers of Parliament. We embraced the opportunity to engage Parliament in a constructive dialogue about our

funding needs. But before doing so, we certainly did our homework. Our Vision and Institutional Service Plan and our Business Case for Permanent Funding provided a comprehensive framework for protecting the privacy rights of Canadians and residents, and for serving Parliament in meeting its needs for privacy expertise as it considers legislation. The Service Plan and Business Case are the Office's blueprint for a stronger and more effective institutional role.

Parliamentarians agreed with this vision. The new House of Commons Advisory Panel on the funding of Officers of Parliament was supportive of our request for funding. The Office will now be in a better position to serve Canadians with close to a 50% increase in human and financial resources. At the end of 2005-2006, on which we are reporting, we planning for that increase within the next two years.

Policy Perspective

The Year in Parliament

2005-06 has been a busy year in Parliament for the Office. A key component of the work we do involves appearing before Committees of the Senate and House of Commons to provide our expert advice on the privacy implications of bills and other policy matters under consideration by Parliament.

The Office was called on to appear before Parliamentary Committees a total of eleven times in fiscal year 2005-06 (sixteen times in calendar year 2005). For a small organization such as our own, this represents a considerable amount of work, but because the Privacy Commissioner is an Officer of Parliament it is central to our mandate. Ten of these eleven appearances were on bills and policy issues that fall under the purview of the *Privacy Act*, although some appearances, such as those on funding, also pertain to the *Personal Information Protection and Electronic Documents Act.*

Bill S-18, *An Act to Amend the Statistics Act*. (Before the House of Commons Standing Committee on Industry, Natural Resources, Science and Technology.)

- This enactment removes a legal ambiguity in relation to access to census records made between 1910 and 2005. It allows unrestricted access to those records, beginning 92 years after the census was taken. Starting in 2006, the consent of Canadians is required in order for their census information to be released 92 years after the census is taken. The OPC did not oppose the release of census records after 92 years and would be pleased to see consent provisions included in the Act, noting that Canadians should have the right to decide for themselves if they want their personal census records to be made publicly available in the future. The bill came into force when it received Royal Assent on June 29, 2005.

- Bill C-37, *An Act to Amend the Telecommunications Act*. (Before the House of Commons Standing Committee on Industry, Natural Resources, Science and Technology.)

This enactment aims to reduce the volume of unsolicited telemarketing calls Canadians receive at home by providing the Canadian Radio-television and Telecommunications Commission (CRTC) with the ability to establish a national Do Not Call List (DNCL). Under the legislation, the CRTC has the power to levy substantial penalties against telemarketers who do not follow the rules. The OPC expressed its strong support for the general intent underlying this bill when it was first introduced in Parliament. However, Bill C-37 also sets out a list of telemarketers who are exempt from the CRTC's requirements or prohibitions in relation to a national DNCL. The OPC expressed opposition to the inclusion of these exemptions. We suggested instead that the House of Commons delay the inclusion of any exemptions until such a time as Parliament had more fully consulted with Canadians on the matter, as was originally recommended by the then minister responsible for the Bill. This advice was supported by the majority of our provincial counterparts. Nevertheless, Parliament decided to incorporate exemptions. Bill C-37 received Royal Assent on November 25, 2005, and will come into force on a day to be fixed by order of the Governor in Council.

- Bill C-16, *An Act to Amend the Criminal Code (impaired driving) and to make consequential amendments to other Act*. (Before the House of Commons Standing Committee on Justice, Human Rights, Public Safety and Emergency Preparedness.)

This enactment amends the Criminal Code to clarify that the reference to impairment by alcohol or a drug in paragraph 253(1)(a) of that Act includes impairment by a combination of alcohol and a drug. It authorizes specially trained peace officers to conduct tests to determine whether a person is impaired by a drug or a combination of alcohol and a drug and also authorizes the taking of samples of bodily fluids to test for the presence of a drug or a combination of alcohol and a drug in a person's body. The OPC expressed support for the intent of the legislation, which is to make our roads safer and to protect Canadians against the effects of impaired driving. However, we had some concerns about the way in which the Bill proposed to address the problem. In particular, these concerns related to the effectiveness and the proportionality of the measures that were being proposed. One of the fundamental principles of fair information practices underlying the *Privacy Act* is that personal information should not be collected unless it can be used

to achieve the specific purpose for which it has been collected. Forcing people to provide bodily fluids is intrusive; the intrusion is compounded when the samples cannot, with confidence, be used to measure impairment. Nevertheless, we noted that if, despite these concerns, the government decided to move ahead with the legislation, provisions needed to be made to ensure that the bodily fluids collected and the results derived from tests were adequately protected. Bill C-16 died on the Order Paper at committee report stage.

- Review of the *Anti-terrorism Act*. (Before the Senate Special Committee on the *Anti-terrorism Act,* and the House of Commons Subcommittee on Public Safety and National Security.)

The *Anti-terrorism Act* received Royal Assent on December 18, 2001. It amended the *Criminal Code*, the *Official Secrets Act*, the *Canada Evidence Act*, the *Proceeds of Crime (Money Laundering) Act* and a number of other Acts, and enacted the *Charities Registration (Security Information) Act*, in order to combat terrorism. In 2005, a House Committee and a Senate Committee both independently undertook a comprehensive review of the Act, as mandated by the legislation to take place three years after it received Royal Assent. The OPC appeared before both Committees reviewing the legislation. Our remarks focused primarily on the lack of facts and evidence to suggest that the measures provided for by the *Anti-terrorism Act* are necessary. We also urged the Committees to critically assess the issue of proportionality and to consider a number of practical recommendations proposed by our Office to address the cumulative impact of anti-terrorism measures on the privacy rights of Canadians.

A key Committee for the Office is the relatively new Standing Committee of the House of Commons on Access to Information, Privacy and Ethics (ETHI). Established in late 2004, this Committee is significant in that with its creation, Canadians now have a Standing Committee of the House of Commons dedicated to privacy matters. The Privacy Commissioner of Canada and other OPC officials appeared three times before the ETHI Committee in 2005-06. While a common reason for these appearances was to question us on the operations of our Office through examination of our Estimates and Annual Reports, Members of the Committee also had many questions and concerns regarding some of the key privacy challenges and opportunities facing Canadians. The OPC looks forward to a continued, productive working relationship with this Committee in the 39th Parliament. As privacy issues continue to grow in number and complexity, it is vital that Parliament have a focus to examine these issues and reflect on the concerns expressed by Canadians.

Finally, a new House of Commons Advisory Panel on the Funding for Officers of Parliament was created this year. The new Panel was responsible for assessing and making recommendations on the OPC request for additional resources. The OPC appeared twice before this Panel to present its Business Case.

Privacy Act Reform

Recommendations for reform of the *Privacy Act* have been made ever since the first legislated review, which resulted in the 1987 report of the Standing Committee on Justice and Solicitor-General, *Open and Shut: Enhancing the Right to Know and the Right to Privacy.* Despite the fact that the report, containing more than 100 recommendations, was unanimously supported by members of the Committee, none of the recommended changes have been enacted, although, in its response, the government committed to move on amendments by the fall of 1988.

In his last report, for 1999-2000, then-Commissioner Bruce Phillips pointed out that Parliament had not turned its mind to the *Privacy Act* in 14 years, although numerous recommendations had been made during the 1990s by the Privacy Commissioner. He called the weaknesses of the *Privacy* Act

> "… all the more striking now that Parliament has passed the *Personal Information Protection and Electronic Documents Act.* This act (which regulates personal information handling in the private sector) contains many features that are superior to the *Privacy Act*, making a comprehensive review of the existing law both urgent and unavoidable."

A detailed review of the Act, *Privacy Act Reform: Issue Identification and Review*, was completed by this office in December 1999, released in June 2000 and submitted to the Department of Justice in anticipation of that "urgent and unavoidable" review.

That review has yet to take place.

Canadians have become much more familiar with the privacy protection principles underlying the private sector law and no doubt expect that personal information in the hands of the government has at least as much protection as personal information in the hands of businesses. If the review of the Act was "both urgent and unavoidable" in 2000, it is even more so today.

To that end, the latest report produced by this Office focuses on the obligations of government institutions. This report was prepared at the invitation of the Standing Committee on Access to Information, Privacy and Ethics, an invitation extended when the OPC appeared before the Committee last fall to discuss our annual reports for 2004-05. *Government Accountability for Personal Information: Reforming the Privacy Act* was recently submitted to the Committee.

The *Privacy Act* was introduced as, and should remain, to the extent possible, the companion of the *Access to Information Act*. The new government has made accountability a centerpiece of its mandate and it is our hope that the long-postponed review and amendment of the *Privacy Act* will finally take place. In preparing *Government Accountability for Personal Information*, our Office has been informed by the proposals for reform presented to the Committee by the Information Commissioner in September 2005 and the report of the Special Advisor to the Prime Minister, Mr. Gérard La Forest, submitted in November.

Since the *Privacy Act* came into being over 20 years ago, the privacy landscape has become much more complex. Technological and social changes in the last 20 years – the creation of the Internet and the World Wide Web, new information and communication technologies, globalization, global positioning systems, video surveillance, outsourcing, data mining and the commodification of personal information – have not just changed the landscape, they have put us on another planet.

As a quasi-constitutional statute, the *Privacy Act* must have primacy over other legislation, except in the most exceptional circumstances. All federal government institutions must be subject to the *Privacy Act* – not just departments and agencies. Officers of Parliament, Crown corporations, the various Foundations set up in recent years, and other entities which carry out important functions related to public health and safety must also be subject to the *Privacy Act*. Any person, not just Canadian citizens or other persons present in Canada, must have the right to apply for access to their personal information held by a Canadian government institution. The definition of personal information must, in this technological and digital age which permits real-time surveillance, include unrecorded as well as recorded information about an identifiable individual. In addition, a person must be able to challenge in court not just a refusal of access to their personal information, but also inappropriate collection, use or disclosure of that information.

The Privacy Commissioner must have as broad a mandate under the *Privacy Act* as it does under the private sector legislation, including the power to use mediation and conciliation to resolve complaints, to conduct research on privacy-related issues, and to educate the public and government institutions about their rights and obligations. The duties of government institutions concerning collection, use and disclosure of personal information must be more clearly specified. Important policies for achieving the goals of the *Privacy Act* have been developed by Treasury Board. These obligations respecting data matching, the management and security of government information, the establishment of privacy management frameworks, the conduct of privacy impact assessments for new programs and guidance for protecting privacy in outsourcing contracts should have the authority of legislation behind them. Without such authority, these policies remain exposed to the vagaries of executive government.

To increase accountability and transparency of government institutions with respect to personal information, reporting requirements need to be strengthened and Parliamentary committees need appropriate support and resources to review the personal information practices of government institutions, as well as their performance of *Privacy Act* responsibilities. Institutions must remain accountable for personal information they are permitted to collect, even though it may be collected or processed by others, especially by contractors outside of Canada.

Although not within this reporting period, it is important to note the new government's *Federal Accountability* Act, introduced April 11, 2006. This bill includes the first set of proposed amendments to the *Access to Information Act*, with parallel amendments to the *Privacy Act*. These amendments extend the scope of the Acts to include additional Crown corporations and the Officers of Parliament (including this Office). The government has further confirmed its commitment to move ahead with comprehensive reform of the *Access to Information Act*. This will necessarily require consideration of the parallel provisions in the *Privacy Act*. It is our hope that this will be the year the government finally carries out the "urgent and unavoidable" review and updating of the *Privacy Act*, not just concerning issues in common with the access legislation, but also including the broader range of issues addressed in *Government Accountability for Personal Information: Reforming the Privacy Act.*

The Merger Issue

In July 2005, former Supreme Court of Canada Justice, the Hon. Gérard V. La Forest, was appointed as a special advisor to the Minister of Justice to assess the merits of merging the offices of the Information Commissioner and the Privacy

Commissioner into a single office. Mr. La Forest was also to examine the merits of cross-appointing a single Commissioner to both functions while maintaining two separate Commissions.

A shift in the structure of dealing with access to information and privacy issues at the federal level could have implications on several fronts, not the least of which was the quality of protection of the privacy rights of Canadians.

In our formal response, delivered to Mr. La Forest in October 2005, we concluded that this is not the appropriate time to consider merging the two offices. In reaching this conclusion, we noted the general lack of scholarly literature on the merits and problems associated with either a "twinned" model or the current federal model. The decision to move towards a particular model must necessarily be based more heavily on assumptions than on a historical record.

We also cautioned that the discussion about the potential framework for asserting access to information and privacy rights at the federal level should not detract from other important concerns affecting these rights. Among those concerns were an appropriate legislative framework, adequate resources to fulfill legislated functions, and a broad mix of tools and processes to foster a culture of compliance that shows respect for the values represented by privacy and access laws. We argued that a review of privacy and access to information legislation was paramount and should precede the discussion of organizational models. The important issue was perhaps not the shape of the container surrounding privacy and access to information, but the quality of the product inside.

In his November 15, 2005, report, Mr. La Forest stated that the burden of persuasion lies with those advocating a merger of the offices of the Information and Privacy Commissioners or a cross-appointment of a single commissioner to both offices. He concluded that this burden had not been met. Each of the one- and two-commissioner models has advantages and disadvantages, he concluded, and in the abstract, neither is demonstrably superior to the other. "But considering the unique features of the federal access to information and privacy environments, and the investments that interested parties have made in the existing structure, moving to a single commissioner model would, in my estimation, have a detrimental impact on the policy aims of the *Access to Information Act*, the *Privacy Act*, and the *Personal Information Protection and Electronic Documents Act*."

Policy Issues

Public Interest Disclosures

Protecting personal information from unwarranted disclosure is an ongoing task for this Office. However, there are circumstances when personal information held by government institutions can and should be disclosed, even without the consent of the person to whom the information relates. Certain disclosures in the public interest fall into this category.

The *Privacy Act* allows for "public interest" disclosures of personal information in limited circumstances. Section 8(2)(m) of the Act permits "disclosure of personal information without the consent of the individual where, in the opinion of the head of the institution:

- the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure; or
- disclosure would clearly benefit the individual to whom the information relates."

This provision has been used, for example, to make public details about an individual who is being released from custody and who poses a threat to the community.

The head of the institution decides whether the public interest outweighs the right to privacy. The institution must notify the Privacy Commissioner that it will be disclosing personal information in the public interest. The Commissioner may express concerns with the proposed disclosure and may, if she thinks it appropriate, notify the individual whose information will be disclosed. However, the decision to release the information in the public interest, and how much to release, rests solely

with the head of the institution. The Privacy Commissioner has no authority to prevent the disclosure.

The *Privacy Act* is therefore abundantly clear about allowing public interest disclosures. Unfortunately, the public disclosure provision is not well understood and, on occasion, the Act is perceived as standing in the way of safety and security by blocking the release of personal information. Too often we hear representatives of government institutions arguing that the *Privacy Act* prevents them from releasing personal information, when in fact the head of the institution could release the information in the public interest. This inaccurate explanation of the role of the Act wrongly paints the Act as the villain.

We do have some sympathy for the predicament facing government institutions on this point. In some situations – for example, following a natural disaster or crime – a reporter may confront a spokesperson for the institution and ask for the name and other personal information about a victim. The spokesperson may simply err on the side of caution and refuse to release that information.

We have no quarrel with this caution, since the spokesperson has no authority under the *Privacy Act* to order the release of the personal information in the public interest, and the decision to release should not be taken lightly in any event. Only the head of the institution or the head's delegate can make the decision to release information in the public interest. In many cases, the information will later be released, but only after the head of the institution has decided that the release is appropriate.

Our concern lies instead with the simplistic characterization of the *Privacy Act* as the barrier to disclosure. It would be more appropriate, and a more accurate interpretation of the *Privacy Act*, for the spokesperson to say that the authority to release personal information rests with the head of the institution, not with the spokesperson. We encourage government institutions to remind spokespersons to respond in this manner when pressed for personal information.

Transborder Data Flows

Last year we wrote about the concerns registered in Canada about the impact of the *USA PATRIOT Act* on data held by US based companies. The *USA PATRIOT Act* has become the symbol of the increasing concern of Canadians about the security of their personal information when it leaves Canada. The *USA PATRIOT Act* was passed rapidly by US Congress shortly after the events of September 11, 2001, with a number of provisions that were scheduled to "sunset" in five years unless the US

Government could persuade Congress to make them permanent. They succeeded in doing so in March 2006, and the controversial clauses became permanent. This Office has certainly expressed concerns about our own Anti-terrorism Act in previous Annual Reports, and noted the growing concern about the impact of foreign legislation on personal data that has left Canada.

This issue has certainly caught the imagination of Canadians, and we have received inquiries and complaints which focus on it as a threat to the privacy of Canadians where transborder dataflow is an issue. It is perhaps appropriate to remind everyone that once data is outside of Canada, the ultimate control of it rests in the hands of the authorities in that state. It is subject to the Court systems in that country, and is accessible under local laws. This is why the European Union passed its Directive 95/46 on Privacy, which directs EU data protection commissioners to block dataflows to foreign states without "adequate" data protection. Adequate data protection includes not merely data protection law, but independent data protection authorities who can provide redress for the citizen.

This is old hat to those who follow data protection matters, because these provisions caused a tremendous stir in 1990s when the Directive was first introduced, but 15 years later we still only inching our way closer to finding solutions for disputes arising from global data flows. The Privacy Commissioner of Canada has agreed to sit on a committee of the Organisation for Economic Co-operation and Development (OECD) which is investigating the need for greater cooperation among independent authorities in handling cross border violation of data protection laws.

This Office has dealt with complaints about cross border marketing of information, and it is clear that dealing with jurisdictional issues is going to be a growing concern in data protection, just as it is in cybercrime. The Justice Minister in the last Parliament had indicated his support for ratifying the Council of Europe's Cybercrime Treaty, which facilitates cooperation among signatories in fighting cross-border crime. We need privacy matters to be included in this agreement as well, or we need other administrative tools such as Mutual Legal Assistance Treaties and Memoranda of Understanding with other states.

We followed up the debates of 2004 on transborder data flow in early 2005. We wrote a letter to the President of the Treasury Board urging the federal government to review the implications of its outsourcing of personal information and to develop contractual clauses to protect personal information transferred to third parties for processing. In the following months we were consulted by the Treasury Board

Secretariat as it crafted a federal strategy in response to privacy concerns about the *USA PATRIOT Act* and the possibility that foreign legislation could reduce the protection of Canadians' personal information. The review of outsourcing contracts among 160 federal institutions revealed that more than 80% rated their contracts as having "no" or "low" risk. The review also helped departments and agencies identify measures to further mitigate privacy risks. One of the key documents released by the Treasury Board Secretariat was a set of guidelines for government institutions. The guidelines set out rules for outsourcing activities in which personal information about Canadians is handled or accessed by private sector agencies under contract with government institutions.

We see the federal strategy as a very positive step toward addressing Canadians' concerns about the flow of their personal information across borders and the possible privacy risks posed by foreign legislation, or even the absence of any privacy legislation. Personal data increasingly circulates the globe and is an important part of global commerce. International data protection rules, such as those of the OECD or the European Union, were created to facilitate the transfer of data across boundaries under appropriate conditions. The recent Treasury Board guidelines attempt to meet the same objectives and we hope that they will be an integral part of a reformed *Privacy Act*.

International Liaison

Over the past year, we have had several visits from colleagues in other countries, with a view to sharing our experiences in the field of data protection and assisting in the development of data protection law. In a world of global dataflows, it is increasingly important that despite differences in legal approach, we achieve harmonious results in our expectations of business practice. As we share data about our citizens, it will be important that we can count on the oversight of similar authorities outside our own jurisdiction, who will look after the protection of the privacy of Canadians.

In October-November we hosted a policy analyst from the *Commission nationale de l'informatique et des libertés* (CNIL), the data commission of France. We were honoured by a visit by the President of the CNIL, M. Alex Türk, and compared our different approaches to enforcement of law. In December we hosted two senior officers from the Mexican Federal Institute for Access to Public Information, who were interested in learning how our regime functions at the ground level, because Mexico is contemplating the enactment of data protection law, and indeed has a bill in Congress. Following their visit, we prepared for a much larger delegation who ultimately arrived for a three day visit in May 2006.

We look forward to hosting the International Conference of Data Protection and Privacy Commissioners in September 2007, where many world experts in privacy and data protection will gather in Montreal. This is a tremendous opportunity for Canadians in government, business, civil society and academe to gather and benefit from the assembled expertise. We will continue to work with colleagues to develop the individual exchange program, a highly useful and relatively inexpensive way to develop harmonized approaches, share knowledge, and build effective relationships.

Radio Frequency Identification Devices (RFIDs)

We have been analyzing the potential impact of Radio Frequency Identification Devices on personal privacy, and how our legislation would apply. The devices have potential for widespread use in consumer products in Canada. With respect to the public sector, there have been suggestions to put RFIDs in passports and border crossing cards. We put a fact sheet up on our web site, and are working on further guidance which will appear this coming year.

Videosurveillance Guidelines

The Office has been working with the Royal Canadian Mounted Police (RCMP) to develop video surveillance guidelines for the use of cameras to monitor public spaces. We have put the guidelines on our web site, and continue to study both increasing use of cameras, and the technical advances that have helped make such surveillance so prevalent now, not only in public spaces, but in retail environments, the workplace, and near all kinds of facilities that have importance with respect to critical infrastructure protection, from gas pipelines to nuclear sites. The increasing power of these cameras, the decreasing costs of data storage, the development of good facial recognition and computer programs that do movement pattern recognition, coupled with the ease with which even remote cameras can now be linked to the world wide web have certainly created the potential of a powerful web of surveillance. We are witnessing an increasing appetite for video-surveillance in Canada and will be developing further guidance on the issue.

Identity Management and the War on Crime and Terror

One of the recurrent themes of this year's research and policy analysis has been identity management. This Office has written about this issue from many perspectives over the past twenty-three years, from discussions on the use of the Social Insurance Number to the OPC's submission on biometric identity cards. This year, we decided that identity management will be a focal point for next year's

research and policy agenda. Here are a few of the experiences of 2005-06 that have led us to this conclusion.

We have been immersed in issues surrounding border security, whether through the audit we conducted of the Canada Border Services Agency which is described later in this report, through commenting on speculation about the proposed Canada-US border card, or in our questions to Transport Canada on no-fly lists. While it is perfectly legitimate for sovereign states to want to positively identify who is crossing into their countries, we are concerned that once a card is introduced, it will be swiped or presented in a host of new situations. It is our observation that when we are frightened about potential terrorist and criminal activity, the impulse is to throw the lights on and identify everything, like a child frightened in the dark. It has not been made clear to us that uniquely identifying each person will enable us to predict who is good or bad, although it may indeed help to prevent fraud in some cases. Nevertheless, teasing apart the reasons for new cards, new identity schemes, new registers of people, and responding to the fresh losses of anonymous transactions in our daily lives is occupying a significant part of our time.

It seems obvious to observe, in relation to the no-fly list for instance, that surely if a person is too dangerous to be allowed to sit in an aircraft, they might be also too dangerous to sit on a subway or board a train. Where are we going with this kind of thinking? As we examine the application in other jurisdictions of RFID chips in motor vehicle licence plates, reporting on where and when vehicles are traveling on the streets and highways, is it not natural to inquire when we will see these devices on people? Someone has to ask these questions, perhaps it is our duty.

With respect to the questions we sent to Transport Canada on the no-fly list issue, the Commissioner stated publicly in August 2005 that this could be a "serious incursion into the rights of travellers in Canada, rights of privacy and rights of freedom of movement." In May 2006 we received a privacy impact assessment for the project and it is currently under review.

At the routine, day to day level, the federal government is working to improve electronic service delivery. Service Canada is working to roll out integrated service delivery, responding to the needs of Canadians for something that feels like the one-stop shopping they now get at the supermarkets. The architecture behind these offerings will continue to challenge us as we try to ensure streamlined process without facilitating the development of a Panopticon in government, where the central authority can see everything.

Technology leaders such as Microsoft and IBM are presenting new schemes for identity management, to deal with issues of fraud, SPAM, and consumer usability, among others. Telecommunications companies, responding to our own concerns about providing personal information only to the person it concerns, are initiating newer and tougher authentication regimes. Banks are being asked by government to provide more data about individuals and their transactions. We have examined the Financial Crimes Reporting legislation, in anticipation of the review of the Act in 2006, and we are concerned about the degree of surveillance of financial transactions which this Act has mandated. Who among Canadians have any idea where their financial data is going, and what is happening with the information reported by banks, accountants, lawyers, and other private sector players about their customers? Even if the data is perfectly managed, and we had time to audit the relevant players to determine this, the point is that in this democracy there are very few who understand the extent of the growth of surveillance and data gathering, and that in itself is a worry.

Sometimes when we meet with our colleagues in government to discuss new initiatives, we ask questions that may seem a little offensive. Canada is not by any means an oppressive state, and officials in the federal government are absolutely impressive in their desire to maintain privacy protections, to understand the impacts of complex technological implementations, and in their respect for human rights and civil liberties. But the price of freedom is, indeed, eternal vigilance. Where will the thirst for identification and transactional surveillance lead us? Is it possible for us to manage all of this disparate activity and come up with an approach to identity and authentication that we could dare to call comprehensive?

We are certainly going to try. There has been a lot of work done in other jurisdictions. We are encouraged that the Treasury Board Secretariat is looking at some of these issues here in Canada, and we hope to play our part in contributing the privacy perspective to the dialogue. Indeed, identity is not that easy.

Complaints

Since 1983 this Office has investigated complaints dealing with personal information held by federal government departments and agencies. The *Privacy Act* governs the collection, use, disclosure, retention and disposal of personal information in the administration of government programs and provides individuals with the right of access to their government-held personal information. The Privacy Commissioner of Canada normally deals with complaints filed by individuals, but she may initiate a complaint and investigate a situation where she has reasonable grounds to believe the *Privacy Act* has been violated.

The Privacy Commissioner is an ombudsman who resolves complaints through mediation, negotiation, and persuasion whenever possible. However, the *Act* gives the Commissioner broad investigative powers to carry out her mandate. She may subpoena witnesses, compel testimony, and enter premises to obtain documents or to conduct interviews. The Commissioner can and does recommend necessary changes to the information-handling practices of government institutions.

Definitions of Complaint Types

Complaints received in the Office are categorized into three main groups:

Access:

- **Access –** All personal information has not been received, either because some documents or information are missing or the institution has applied exemptions to withhold information.
- **Correction/Notation –** The institution has failed to correct personal information or has not placed a notation on the file in the instances where it disagrees with the requested correction.

- **Language –** Personal information was not provided in the official language of choice.
- **Fee –** Fees have been assessed to respond to a *Privacy Act* request; there are presently no fees prescribed for obtaining personal information.
- **Index –** INFOSOURCE [1] does not adequately describe the personal information holdings of an institution.

Privacy:

- **Collection –** Personal information collected is not required for an operating program or activity of the institution; personal information is not collected directly from the individual concerned; or the individual is not advised of the purpose of the collection of personal information.
- **Retention and Disposal –** Personal information is not kept in accordance with retention and disposal schedules (approved by the National Archives and published in INFOSOURCE): either destroyed too soon or kept too long.

  In addition, personal information used for an administrative purpose must be kept for at least two years after the last administrative action unless the individual consents to its disposal.
- **Use and Disclosure –** Personal information is used or disclosed without the consent of the individual and does not meet one of the permissible disclosures without consent listed in section 8(2) of the *Act*.

Time Limits:

- **Time Limits –** The institution did not respond within the statutory limits.
- **Extension Notice –** The institution did not provide an appropriate rationale for an extension of the time limit, applied for the extension after the initial 30 days had been exceeded, or applied a due date more than 60 days from date of receipt.
- **Correction/Notation - Time Limits –** The institution has failed to correct personal information or has not placed a notation on the file within 30 days of receipt of a request for correction.

1 INFOSOURCE is a federal government directory that describes each institution and the banks of information (groups of files on the same subject) held by that particular institution.

Complaints Received between April 1, 2005 and March 31, 2006

The Office received 1,028 complaints in 2005-06, 549 fewer complaints than the previous year. This 35% decline from the previous year reflected lower numbers of Access, Use and Disclosure and Time Limits complaints. As opposed to last year, the Office did not receive any groups of complaints, which may also account in part for the lower number of complaints received.

Complaint Type	Count	Percentage
Access	391	38.00
Collection	25	2.40
Correction-Notation	44	4.30
Correction/Notation - Time Limits	9	0.90
Extension Notice	22	2.10
Language	1	0.10
Retention and Disposal	10	1.00
Time Limits	411	40.00
Use and Disclosure	115	11.20
Total	1,028	100.00

As in previous years, the most common type of complaint concerned institutions not meeting the 30-day timeframe specified in the Act to respond to requests for access to personal information. Time limit complaints, along with complaints about denial of access to personal information and inappropriate use and disclosure of personal information, comprise 89% of the complaints received. In the 2004-05 fiscal year the distribution was similar, with these complaints constituting 85% of the total.

Top Ten Institutions by Complaints Received

The following table represents the institutions that received the greatest number of complaints in the fiscal year ending March 31, 2006.

Organization	Total	Access	Time Limits	Privacy
Correctional Service Canada	190	108	43	39
Royal Canadian Mounted Police	165	35	121	9
Immigration and Refugee Board *	121	32	85	4
Canada Revenue Agency	92	38	37	17
Citizenship and Immigration Canada	60	32	27	1
Canada Post Corporation	42	15	17	10
National Defence	41	13	21	7
Human Resources Skills Development	35	10	5	20
Canadian Security Intelligence Service	35	30	5	0
Canada Border Services Agency	34	12	19	3
Others	213	111	62	40
Total	**1,028**	**436**	**442**	**150**

* A significant portion of complaints regarding this institution were submitted by one individual in the course of dealing with the Immigration and Refugee Board.

The number of complaints filed against institutions does not necessarily mean that these institutions are not compliant with the *Privacy Act*. Because of their mandate, some of these institutions hold a substantial amount of personal information about individuals and are therefore more likely to receive numerous requests for access to that information. Holding a large amount of personal information increases the likelihood of complaints about the institution's collection, use and disclosure, retention and disposal of personal information, and the manner in which it provides access to that information.

Complaints Received by Institution

This table shows the actual number of all of the complaints lodged against the various institutions and agencies that were received in the fiscal year ending March 31, 2006.

	Total
Agriculture and Agri-Food Canada	32
Canada Border Services Agency	34
Canada Economic Development for Quebec Regions	13
Canada Firearms Centre	1
Canada Post Corporation	42
Canada Revenue Agency	92
Canadian Air Transport Security Authority	2
Canadian Food Inspection Agency	1
Canadian Heritage	1
Canadian Human Rights Commission	4
Canadian Security Intelligence Service	35
Citizenship and Immigration Canada	60
Commission for Public Complaints Against the RCMP	1
Correctional Investigator Canada	1
Correctional Service Canada	190
Elections Canada	1
Export Development Corporation	8
Fisheries and Oceans	1
Foreign Affairs and International Trade Canada	33
Health Canada	18
Human Resources and Skills Development Canada	35
Immigration and Refugee Board	121
Indian and Northern Affairs Canada	3
Indian Residential Schools Resolution Canada	1
Industry Canada	5
Justice Canada	29
Library and Archives Canada	7
National Defence	41
National Gallery of Canada	1
National Parole Board	4
National Research Council Canada	2
Office of the Commissioner of Review Tribunals	1
Pacific Pilotage Authority Canada	1
Pension Appeals Board Canada	2
Privy Council Office	1
Public Safety and Emergency Preparedness Canada	1
Public Service Commission Canada	7
Public Works and Government Services Canada	6
Royal Canadian Mounted Police	165
Social Development Canada	13
Statistics Canada	3
Transport Canada	3
Veterans Affairs Canada	6
Total	**1,028**

Complaints Received by Origin
From April 1, 2005 to March 31, 2006

The following table shows the province of origin of the complaints received in the reporting period. It should be noted that some complaints were received from persons living outside Canada. Canadians living outside the country whose personal information is held by the Canadian government are also covered by the *Privacy Act*.

Province/Territory	Total	Percentage
Quebec	249	24.00
Ontario	225	22.00
British Columbia	182	18.00
NCR	159	15.00
Alberta	68	7.00
Manitoba	53	5.00
Saskatchewan	35	3.00
International	17	2.00
New Brunswick	15	1.50
Nova Scotia	16	1.60
Newfoundland	5	0.50
Prince Edward Island	2	0.20
Yukon Territory	2	0.20
Total	**1,028**	**100.00**

Almost 80% of complaints originated in the provinces of Quebec, Ontario and British Columbia, as well as in the National Capital Region. This pattern is consistent with what we have seen over the last five years in that Quebec, Ontario, and British Columbia have, with one exception, been the source of the vast majority of complaints received. The exception was in the 2003-04 year, when Alberta bumped Ontario out of third place.

Complaints Completed between April 1, 2005 and March 31, 2006
In the past fiscal year, we closed 1,040 complaints, approximately the same number of complaints that we received in that year.

Despite closing as many *Privacy Act* complaints as received, the Office is carrying a significant number of ongoing cases –1,263 at fiscal year-end. A major Business Process Review of the Branch was finalized at the beginning of the year to establish appropriate resource levels and to find solutions to our aging caseloads. A requirement for additional resource levels was identified and intensive staffing activities are underway to recruit, hire and train additional investigators. We are determined to deal with the backlog of cases within two years.

Definitions of Findings and other Dispositions under the *Privacy Act*

The Office has developed a series of definitions of findings to explain the outcome of its investigations under the *Privacy Act.*

Early resolution: applied to situations in which the issue is dealt with before a formal investigation is undertaken. For example, if an individual complains about an issue that the Office has already investigated and found to be compliant with the *Privacy Act*, we explain this to the individual. We also receive complaints in which a formal investigation could have adverse implications for the individual. We discuss the possible impact at length with the individual and should he or she choose not to proceed further, the file is closed as "early resolution".

Not Well-founded: the investigation uncovered no or insufficient evidence to conclude that the government institution violated the complainant's rights under the *Privacy Act*.

Well-founded: the government institution failed to respect the *Privacy Act* rights of an individual.

Well-founded/Resolved: the investigation substantiated the allegations and the government institution has agreed to take corrective measures to rectify the problem.

Resolved: after a thorough investigation, the Office helped negotiate a solution that satisfies all parties. The finding is used for those complaints in which well-founded would be too harsh to fit what essentially is a miscommunication or misunderstanding.

Settled during the course of the investigation: the Office helped negotiate a solution that satisfies all parties during the investigation, but issues no finding.

Discontinued: the investigation was terminated before all the allegations were fully investigated. A case may be discontinued for any number of reasons —the complainant may no longer be interested in pursuing the matter or cannot be located to provide additional information critical to reaching a conclusion.

Findings by Complaint Type

The following charts show the outcome of our investigations of the different types of complaints we receive. The first chart represents all types of complaints; the second represents access and privacy complaints, and the third represents complaints strictly related to time limits. This is the first time we have isolated our statistics in this way to demonstrate the significant number of complaints we receive that are related strictly to time limits.

Complaints (All Types) Closed
From April 1, 2005 to March 31, 2006

	Discontinued	Early Resolution	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Well-founded-Resolved	Total
Access	54	12	143	12	63	1	23	308
Collection	2	2	19	0	9	1	0	33
Correction-Notation	24	1	3	0	5	0	0	33
Correction/ Notation - Time Limits	0	0	0	0	0	5	0	5
Extension Notice	2	1	37	0	0	4	0	44
Language	0	0	0	1	0	0	0	1
Retention and Disposal	0	0	2	0	4	1	0	7
Time Limits	47	5	22	11	8	395	0	488
Use and Disclosure	12	2	51	2	29	25	0	121
Total	**141**	**23**	**277**	**26**	**118**	**432**	**23**	**1,040**

Access and Privacy Complaints Closed
From April 1, 2005 to March 31, 2006

	Discontinued	Early Resolution	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Well-founded-Resolved	Total
Access	54	12	143	12	63	1	23	308
Collection	2	2	19	0	9	1	0	33
Correction-Notation	24	1	3	0	5	0	0	33
Language	0	0	0	1	0	0	0	1
Retention and Disposal	0	0	2	0	4	1	0	7
Use and Disclosure	12	2	51	2	29	25	0	121
Total	92	17	218	15	110	28	23	503

Clearly, there are far more not well-founded complaints than well-founded complaints: 218 and 51 respectively. This includes well-founded resolved. In addition, a significant number of complaints are resolved in some way (discontinued, early resolution, resolved or settled in the course of investigation): 234 out of 503 complaints, or 47%. Another way of viewing this is that only 10% of complaints to our Office under the *Privacy Act* are well-founded. We believe this speaks well for overall compliance with the Act by federal institutions.

Appendix 1 provides a detailed breakdown of access and privacy complaints closed by department.

Time Limit Complaints Closed
From April 1, 2005 to March 31, 2006

	Discontinued	Early Resolution	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Well-founded-Resolved	Total
Correction/ Notation - Time Limits	0	0	0	0	0	5	0	5
Extension Notice	2	1	37	0	0	4	0	44
Time Limits	47	5	22	11	8	395	0	488
Total	**49**	**6**	**59**	**11**	**8**	**404**	**0**	**537**

It is important to note that of a total of 537 complaints, 75% of these were well-founded. By their very nature, the majority of Time Limit complaints are well-founded. Organizations have 30 days from the date of receipt to respond to requests from individuals for access to their personal information. Individuals do not complain unless there has been a delay in responding to their requests. The exceptions to well-founded findings are as a result of appropriately applied Extension Notices to allow for an additional 30 days to respond and instances where the complainants did not allow for mailing time; e.g. a request must be received by the institution before starting the 30-day count.

The OPC remains concerned, however, about the numbers of Time Limit complaints lodged against some institutions. The OPC is aware that some of these institutions have taken steps to address resourcing deficiencies. Experience shows that public service staffing takes considerable time, as does training of new staff. There is therefore some lead time between identifying a requirement for resources and having that translate into increased productivity and a decrease in backlogs. The OPC will continue to monitor and assess compliance with the Time Limit requirements of the *Privacy Act* in the coming year.

Appendix 1 provides a detailed breakdown of time limit complaints closed by department.

Complaint Investigations Treatment Times - *Privacy Act*

The following tables show the average number of months taken to complete a complaint investigation, from the date the complaint is received to when a finding is made. The first table breaks this down by finding, the second by complaint type.

By Finding
For the period between April 1, 2005 to March 31, 2006

Disposition	Average Treatment Time in Months
Early Resolution	3.61
Well-Founded	7.18
Not Well-Founded	13.22
Discontinued	8.96
Settled in the Course of Investigation	16.46
Well-Founded, Resolved	23.09
Resolved	14.27
Overall Average	**10.49**

By Complaint Type
For the period between April 1, 2005 to March 31, 2006

Complaint Type	Average Treatment Time in Months
Correction/Notation - Time Limits	9.20 *
Extension Notice	8.45
Time Limits	6.49
Access	15.14
Language	25.00 **
Use and Disclosure	14.25
Collection	14.64
Retention and Disposal	23.86
Correction/Notation	9.73
Overall Average	**10.50**

* The treatment time for this complaint type is based on five cases.
** The treatment time for this complaint type is based on one case only.

The treatment times reflected above are of concern since our average time elapsed from the date of complaint to the date of finding is ten and a half months. The breakdown by finding shows that complaints that require full investigation – that is,

the complaints that result in findings of well-founded/resolved, resolved, not well-founded or settled – take on average more than a year to complete. The delay in completing settled complaints reflects the long standing practice of this Office not to settle cases until the investigation has been finalized. However, we are pleased to report that we have changed this practice and now a case can be settled at any point during the investigation, which should reduce treatment times for settled cases.

Follow-up after Investigations

Once a complaint is investigated and completed, the story does not necessarily end there. All complaints dealing with improper collection, use, disclosure and retention that are well-founded are sent to the Audit and Review Branch for its review. This allows the Branch to identify any trends and patterns dealing with privacy breaches and use this information in planning and developing its audits for the next year.

Select Cases under the *Privacy Act*

The following summaries provide a sample of the types of complaints received and the approach taken by this Office to address various issues with regard to personal information protection in the public sector. These cases demonstrate how important it is for government institutions and agencies to be ever vigilant in handling personal information and what can go wrong when this does not occur.

Subscribers required to provide information to renew e-mail news subscription

A subscriber to an e-mail media news service complained that he had to provide more information than was necessary in order to re-subscribe. It was the Department of Foreign Affairs and International Trade (DFAIT) that offered the subscription service. Specifically, the complainant objected to providing his postal code, telephone number and company affiliation. He also was upset that although DFAIT's privacy notice said the provision of information was voluntary, it was actually obligatory.

The Office learned that DFAIT had been asking Canadian subscribers to its e-mail media releases to provide their e-mail address, city, province, postal code, telephone number and company affiliation. International subscribers were only being asked for their e-mail address and country of origin. We confirmed that the on-line subscription application would not accept the subscription without this information.

DFAIT explained that telephone numbers are required so that the department can contact subscribers in the event of any technical problems with e-mail addresses. Postal code and company affiliation information is required so that some media releases can be targeted to a particular region or a particular type of business.

Our Office concluded that DFAIT was allowed under the Act to collect the subscriber information in order to facilitate access to and distribution of the media releases. The complaint was therefore considered to be not well-founded. However, we were pleased that DFAIT agreed that the use of the word "voluntary" in its privacy notice was somewhat misleading; it was, in fact, the participation in the subscription activity itself that was voluntary. DFAIT subsequently changed the notice to make it more accurate.

Unnecessary requirement for a social insurance number

A caregiver complained that she had to give her social insurance number (SIN) to the father of a child in her care. It was required in order for the father to receive compensation under the Department of National Defence's (DND) Family Care Assistance (FCA) program.

Under DND's FCA program, certain members of the Canadian Forces can be reimbursed for child care costs when on duty away from home. In order to receive the benefit, members have to submit receipts and complete a DND form, which requests information concerning the caregiver, including the caregiver's name, SIN or business number.

During our investigation, DND explained that there was no actual requirement for the caregiver's SIN under the FCA program. It therefore agreed to change its form to reflect this. In the meantime, DND instructed its staff not to ask for the SIN. DND also confirmed that the father in question had not provided the caregiver's SIN on the form.

The caregiver was pleased with this outcome, and the matter was considered settled.

Human rights complaint investigation prompts release of employee information

An employee of the Canada Post Corporation (CPC) complained that the CPC had told another organization that she had taken disability leave from her job.

Our Office learned that the CPC employee had initiated a human rights complaint against her employer on the issue of duty to accommodate based on a medical disability. During the CPC's investigation into the circumstances that led to the human rights complaint, a concern emerged as to whether the employee had held another job while on disability leave from the CPC.

In accordance with the basic principles of procedural fairness in the conduct of any investigation, an investigator is obligated to explain the nature and scope of the matter under investigation in order to elicit accurate and relevant information.

In order to check the facts, the CPC contacted the other organization to inquire about the individual's employment. The CPC informed the organization that it was investigating a human rights complaint filed against it based on a medical disability and the type of information it was seeking. Before releasing any of the complainant's information to the CPC, the other organization requested her consent and referred to her having taken disability leave. However, we determined that this statement was an assumption on the organization's part as there was no evidence that anything was said by the CPC about the complainant being on disability leave.

As this individual's information, which the CPC gave to the organization, was necessary and directly related to the conduct of the human rights investigation, our Office concluded that the complainant's privacy rights were not affected and this matter was not well-founded.

Collection officer did not divulge debtor personal information

An individual complained that a Canada Revenue Agency (CRA) collection officer improperly disclosed her personal information to another person.

Our Office learned that the complainant owed the CRA for overpayment of the Canada Child Tax Benefit (CCTB). She had been entitled to the benefit while she was married. However, she continued to receive the benefit following her divorce, even though she had not been awarded custody of her children. The CRA discovered the overpayment when her ex-husband and mother-in-law, who was the children's

caregiver, applied for the benefit. The CRA was able to recover a portion of the overpayment but, after a while, its letters requesting payment of the remainder of the debt were returned unopened.

A CRA collection officer then reviewed the file, and phoned the mother-in-law, whose name was on record as the current recipient of the CCTB. Our Office was informed by the collection officer that she identified herself to the mother-in-law and stated that she was trying to track down the daughter-in-law's current contact information. The complainant maintained that the collection officer then divulged her personal tax information concerning the CCTB. However, both the CRA officer and the mother-in-law denied this. Both maintained that the mother-in-law immediately guessed why the officer was trying to contact the daughter-in-law, and, upon being questioned, the officer said she could not disclose any details.

Under the *Income Tax Act*, CRA collection officers have been delegated responsibility for collecting tax debts owed to the Government of Canada. In this instance, the evidence indicated that the CRA's collection officer did not provide any details regarding the complainant or her tax file to the complainant's mother-in-law. In our view, the Collections Officer followed the basic principles of an investigator's obligations of procedural fairness. The person merely introduced herself as a CRA Collections Officer and requested contact information for the complainant. Our Office therefore considered the complaint not well-founded.

PSC discloses information in an audit

Three individuals complained that the Public Service Commission (PSC) disclosed information about them in an audit that it had conducted and released to the public.

The PSC audited the staffing actions of a small government organization. In its report of findings, it cited examples of specific staffing actions that it had examined. Our Office found that, while the report did not contain any names, it provided enough detail about some specific cases that the individuals could be identified. Furthermore, as the audit was made public, its findings were reported in the media.

Audits are generally negative in nature, and it is not unusual that they should contain examples of scenarios portrayed in negative terms. This is not problematic when speaking of staffing processes for federal institutions with hundreds of employees in particular job classifications. However, when it is a small institution,

it is a different matter. Furthermore, calling into question the selection process of a position when the individual is identifiable directly reflects on the person's competence and qualifications.

Our Office concluded that the information released by the PSC in its audit was clearly the individuals' personal information and should not have been disclosed without each person's consent. The complaints were therefore well-founded.

Our Office is pleased to report that the PSC now requires all of its audits to be reviewed by its Access to Information and Privacy Branch before they can be released to determine if they contain information which is subject to the *Privacy Act*.

Government has right to monitor use of its e-mail systems

A Canada Border Services Agency (CBSA) employee was annoyed that each time he logged on to his CBSA computer system, he had to agree to an online statement or else be denied access to the system. The statement in question indicates that the CBSA may monitor the use of its systems. The complainant maintained that the use of e-mail should receive the same privacy considerations as use of the telephone. In his view, monitoring his e-mails violated his privacy rights.

Our Office ascertained that the CBSA's monitoring policy is drawn from two Treasury Board policies: the Government Security Policy and the Policy on the Use of Electronic Networks. These policies clearly state that government departments must conduct active monitoring and internal audits of their security programs. As such, electronic networks may be monitored for operational reasons and for assessing compliance with the policies. While normal routine analysis does not involve reading content, if due to routine analysis or a complaint the institution reasonably suspects that an individual is misusing the network, the matter is referred for investigation and action that may involve special monitoring and/or reading the content of the e-mails. In this case, the CBSA confirmed that the complainant's personal e-mails were never read.

The CBSA pointed out that e-mail is a corporate communications tool provided to employees for the purpose of conducting official government business. The department allows limited personal use when it complies with CBSA's policies and legislation, and when employee performance is not adversely affected.

Our Office concluded that the CBSA displayed fairness and transparency by informing its employees of its monitoring practices through the online statement, and by making the electronic network policy guidelines readily available on its intranet. Employees therefore have clear expectations of the level of privacy they can expect from the employer. Our Office determined that the complaint was not well-founded.

Incidents under the *Privacy Act*

In addition to individual complaints, our Office investigates incidents of mismanagement of personal information. These are typically brought to our attention from various sources including the media and directly from institutions themselves, and may involve matters of improper collection, use or disclosure of personal information. They often highlight a systemic issue, or an unrecognized privacy breach that needs to be corrected as soon as possible. Last year, the Office completed 54 such investigations.

There were a number of incidents involving computer theft or briefcase theft, three incidents involved information on shared computer drives and two incidents involved the sale of fax machines that retained personal information in a memory component. These cases are described below.

Thermofax rolls containing personal information sold by Crown assets

There have been a couple of incidents in which fax machines purchased at Crown Assets Distribution Centre sales were found to hold rolls that still contained personal information. For example, in 2005, Human Resources and Skills Development Canada (HRSDC) reported to our Office that a member of the media had obtained a thermofax roll containing the names and/or Social Insurance Numbers of 65 individuals. A thermofax roll comes in a cartridge that is loaded into the fax machine. It contains a combination of a thin sheet of paper and a clear film-like substance. When the paper on the cartridge has all been used and the cartridge needs to be replaced, the used film has the negative image of every single fax that came through that machine from the time the roll was installed until it was removed. The thermofax roll had been sold as part of a fax machine at a Crown Assets sale and was later acquired by an individual who passed the roll on to the media. Following HRSDC's investigation, the purchaser assured officials that he had destroyed the thermofax roll and all records that had been retrieved from it.

HRSDC took several steps to ensure that this type of situation does not recur. An amended policy was circulated to HRSDC, Social Development Canada and Service Canada that reinforced the need for the inspection of business equipment being declared surplus and the need for the removal and suitable destruction of 'memory instruments'. Officials agreed to undertake a complete physical inventory and reconciliation of all fax machines. They also contacted Crown Assets to retrieve any unsold equipment of this type to check it for personal information. Our Office was satisfied that all appropriate action had been taken to remedy the situation and to prevent future occurrences.

However, during our investigation, we discovered that two fax machines with thermofax rolls intact and originating from the Canada Revenue Agency (CRA) had also been sold by Crown Assets. Again, the staff was simply unaware of the need to sanitize such equipment. CRA too has amended its policies and procedures with respect to disposal of equipment with memory capability.

Given the far-reaching implications of this matter and the likelihood that every department and agency is using some type of equipment with memory that requires special disposal, our Office advised the Information, Privacy and Security Policy Directorate at the Treasury Board Secretariat. It too is pursuing the matter and will be issuing a bulletin to all government departments and agencies.

In conclusion, this highlights the importance of all institutions ensuring that personal information is properly erased from electronic data storage devices. The subject is not straightforward but there are three ways for "media sanitization" or destruction of electronic data:

- **Overwriting** – overwriting with 1s and 0s where the data was located
- **Degaussing** – magnetically erasing the data with an electric degausser
- **Destruction** – physical destruction of the storage medium

Two technical documents provide advice on these topics:

- Communications Security Establishment *Clearing and Declassifying Electronic Data Storage Devices*, available online at http://www.cse-cst.gc.ca/documents/publications/gov-pubs/itsg/itsg06.pdf
- U.S. Department of Defense Standard 5220.22-M – Advising Users on Computer Systems Technology, available online at http://www.qsgi.com/usdod_standard_dod_522022m.htm

Although these documents do not provide specific guidance on the destruction of thermofax rolls, the general techniques outlined in the documents (e.g. shredding) should be readily adaptable.

Laptop with NCC festival security-pass information stolen

An incident concerning computer theft occurred in the spring of 2004, involving a laptop computer and related accessories stolen from a National Capital Commission (NCC) facility. The laptop contained personal information consisting of two security databanks for security passes to various NCC festivals. The information, including names, photos, dates of birth, occupations and names of employers, was protected by two levels of passwords.

The NCC's internal investigation revealed that there had been major construction work going on in the building in question when the laptop was stolen. More people than normal had access to the premises where the computer was located, and it was very difficult to ascertain who might have taken it. The NCC undertook to increase the level of security in its facility. Our Office confirmed that the NCC also sent out letters to the employees whose information was compromised, referring them to a number of websites, including ours, for information on how to protect themselves from identity theft. They were also referred to the NCC's Access to Information and Privacy Office for further advice. In addition, our Office recommended to the NCC that it make an archive copy of this particular Information Bank in order to prevent any future loss in cases of theft or destruction of equipment.

Briefcase and knapsack containing offender information stolen from trunk of car

During the winter of 2005, two Correctional Service Canada (CSC) employees put a locked briefcase and a knapsack in the trunk of their personal car after leaving a meeting. Upon arriving home, they did not remove the items from the trunk. Two days later, one of the employees parked the vehicle at a mall, and upon return, discovered that it had been broken into. The next day, both employees checked the trunk and found that the briefcase and knapsack were missing. They immediately notified the RCMP and their employer. The RCMP did not conduct an investigation as CSC was to conduct its own.

Among the missing documentation was a report that contained information about eight federal offenders. CSC advised only two of the offenders about this incident, as the others were deceased. CSC's review concluded that it was not appropriate to transport protected information in a knapsack, and that neither the car trunk nor

the briefcase is an approved storage container for protected information. A briefcase, however, can be used to transport such information. In addition, the employees responsible for the protection of the information should have removed it from the vehicle when they reached their destination. As a result of this incident, CSC decided to establish more specific guidelines to provide direction concerning the transportation and storage of information outside of CSC premises.

DND employee finds own grievance information on shared computer drive

There have been a number of incidents regarding shared computer drives that resulted in personal information being accessible to people with no right to see it. In one instance a DND employee discovered a grievance chart on a shared drive. On the grievance chart was his name, the file number assigned to his grievance complaint and the status of his grievance. Similar information appeared on the list about other grievers as well.

During its investigation into the matter, DND learned that the information was originally on a protected drive with access shared on a controlled basis, limited to people who needed the information in order to do their jobs. At one point, servers were migrated, thus removing the firewall protection and making the information available on a shared drive for a limited time. This resulted in the employee being able to find the list.

Once DND was notified of the problem, it took immediate steps to remove and destroy the list. The grievance list has since been modified so that it no longer contains the identity of the grievers. DND reminded the group responsible for the list of the need to protect personal information. It also wrote to the employee, informing him of the situation that led to his information becoming available on the shared network. DND also advised him of his right to file a formal complaint with our Office.

Public Interest Disclosures under the *Privacy Act*

Heads of government institutions have the discretion to disclose personal information without an individual's consent when the disclosure benefits that individual or when a compelling public interest outweighs the invasion of the individual's privacy. The head of the institution is required to notify the Privacy Commissioner of such disclosures, in advance, unless the some urgency dictates otherwise. The Office reviews the proposed disclosures and, if deemed necessary, the Privacy Commissioner notifies the individual to whom the information relates. The Office also advises institutions when it believes the amount of personal information proposed for release is more than is needed to address the public interest and thus, we recommend measures to minimize the intrusion into the individual's life. Issues surrounding this provision in the *Privacy Act* are discussed earlier in this report.

We completed reviews of 66 such notices, a large number of them in two categories. The first category concerns individuals who were either unlawfully at large or being released from custody at the end of their sentences. All were considered at high risk to re-offend and therefore a danger to the community. We received 17 notices of this type, the majority of which came from the Royal Canadian Mounted Police and the Correctional Service Canada (CSC).

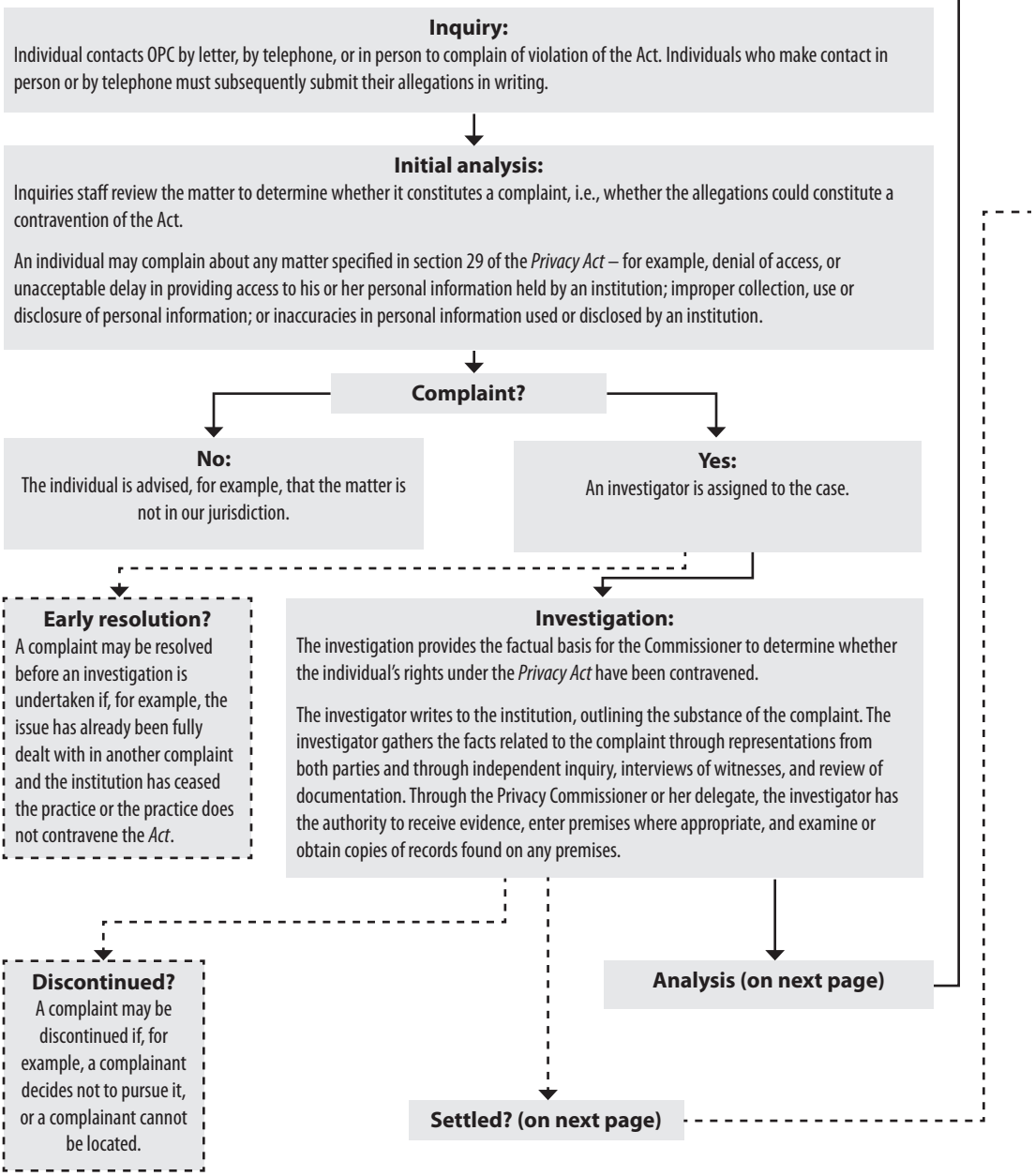
The second significant group – 13 – came from the CSC, National Defence and the National Parole Board. They concerned the disclosure of personal information to family members of recently deceased individuals to provide them with the circumstances of death and with some modicum of closure.

Another seven notices dealt with government accountability on matters such as the Ipperwash Inquiry with respect to the shooting of Dudley George, and the Board of Inquiry into the fire on HMCS Chicoutimi.

Also of interest were six notices concerning health issues, including one from Public Safety and Emergency Preparedness Canada and one from the Department of Foreign Affairs and International Trade Canada (DFAIT) on health risks to the public from individuals with tuberculosis.

There were also a variety of other notices, including one from the CSC regarding Karla Homolka, which provided information to her victims' lawyer about her release.

Investigation Process under the *Privacy Act*



Note: a broken line (- - - -) indicates a *possible* outcome.

Analysis:

The investigator analyzes the facts and prepares recommendations to the Privacy Commissioner or her delegate. The investigator will contact the parties and review the facts gathered during the course of the investigation. The investigator will also tell the parties what he or she will be recommending, based on the facts, to the Privacy Commissioner or her delegate. At this point, the parties may make further representations.

Analysis will include internal consultations with, for example, Legal Services or Research and Policy Branches, as appropriate.

Settled?

The OPC seeks to resolve complaints and to prevent contraventions from recurring. The Commissioner encourages resolution through negotiation and persuasion. The investigator assists in this process.

Findings:

The Privacy Commissioner or her delegate reviews the file and assesses the report. The Privacy Commissioner or her delegate, not the investigator, decides what the appropriate outcome should be and whether recommendations to the institution are warranted.

The Privacy Commissioner or her delegate sends letters of findings to the parties. The letters outline the basis of the complaint, the relevant findings of fact, the analysis, and any recommendations to the institution. The Privacy Commissioner or her delegate may ask the institution to respond in writing, within a particular timeframe, outlining its plans for implementing any recommendations.

The possible findings are:

Not Well-Founded: The evidence, on balance, does not lead the Privacy Commissioner or her delegate to conclude that the complainant's rights under the *Act* have been contravened.

Well-Founded: The institution failed to respect a provision of the *Act*.

Well-Founded, Resolved: The investigation substantiated the allegations and the institution has agreed to take corrective measures to rectify the problem.

Resolved: The evidence gathered in the investigation supports the allegations raised in the complaint, but the institution agreed to take corrective measures to rectify the problem, to the satisfaction of this Office. The finding is used for those complaints in which Well-Founded would be too harsh to fit what essentially is a miscommunication or misunderstanding.

In the letter of findings, the Privacy Commissioner or her delegate informs the complainant of his or her rights of recourse to the Federal Court on matters of denial of access to personal information.

Where recommendations have been made to an institution, OPC staff will follow up to verify that they have been implemented.

The complainant or the Privacy Commissioner may choose to apply to the Federal Court for a hearing of the denial of access. The Federal Court has the power to review the matter and determine whether the institution must provide the information to the requester.

Note: a broken line (- - - -) indicates a *possible* outcome.

Inquiries

The Inquiries Unit responds to requests for information from the public about the application of the *Privacy Act* and *PIPEDA*. The Office receives thousands of inquiries each year from the public and organizations seeking advice on private sector privacy issues.

In the 2005-06 fiscal year, the Office received 2,506 inquiries relating to the *Privacy Act*. This is somewhat less than the number of inquiries in the previous year, when we received 2,976 inquiries. In comparison, we received more than double the number of inquiries on issues relating to *PIPEDA* (see statistics in our 2005 Annual Report to Parliament on *PIPEDA*).

The inquiries staff may be responding to fewer calls, but they are providing more information. A decision in 2004 to no longer accept e-mail inquiries has led to a refocusing of staff time on telephone inquiries, during which callers tend to seek longer and more in-depth explanations in response to their questions. In addition to this, an automated telephone system answers the public's most frequently asked questions, such as those about identity theft, telemarketing and the Social Insurance Number. Our web site also provides a wide range of information.

Approximately 25% of *Privacy Act* inquiries are answered in writing and 75% are answered by telephone. On average, written inquiries received a response within three months. The majority of telephone inquiries received an immediate response. The remainder, which may have required some research, received a response within three days.

Inquiries Statistics
April 1, 2005 to March 31, 2006

***Privacy Act* Inquiries Received by the Inquiries Unit**	
Telephone inquiries	1,929
Written inquiries (letter, e-mail, fax)	577
Total number of inquiries received	2,506

***Privacy Act* Inquiries Closed by the Inquiries Unit**	
Telephone inquiries	1,933
Written inquiries (letter, e-mail, fax)	631
Total number of inquiries closed	2,564

Audit and Review

The OPC is responsible for carrying out audits of federal departments and agencies subject to the *Privacy Act.* It may also carry out audits of private sector organizations pursuant to section 18(1) of Canada's *Personal Information Protection and Electronic Documents Act* (*PIPEDA*). The OPC also evaluates Privacy Impact Assessments (PIAs) prepared by federal departments and agencies. It also undertakes a variety of other projects relating to privacy practices in both the public and private sectors.

The audit and review function of the Office serves its role as privacy guardian. The objective of this function is to conduct independent and objective audits and reviews of personal information management systems for the purpose of promoting compliance with applicable legislation, policies and standards and improving privacy practices and accountability.

During fiscal year 2005-06, the Office completed one major audit pursuant to the *Privacy Act,* substantially completed three other audit projects and initiated a review of federal entities not subject to either the *Privacy Act or PIPEDA*. It also completed 43 PIA reviews, as well as16 other projects. Staff also monitored the privacy-related activities of the Treasury Board Secretariat (TBS) and other federal departments and agencies.

Stronger Privacy Management Framework Needed to Ensure Sound Privacy Management

Last year the Office reported on the need for building a privacy management framework for the federal government. We outlined what a framework was, why it was important and described the features of a good privacy framework. We

also commented on some specific issues that needed to be addressed as part of strengthening privacy management in the federal government.

The Treasury Board of Canada Secretariat (TBS) is responsible for setting privacy policy direction and providing guidance to federal institutions. Last year the OPC recommended that TBS develop a model framework to guide privacy management in federal departments and agencies. TBS management accepted this, indicating that it was committed to the concept and that it would examine the scope and process for a project.

While the OPC is pleased to note good progress being made, all parties recognize there is considerable work yet to be completed.

In December 2005, TBS informed us that officials have begun to examine preliminary concepts for the design and development of a privacy management framework to set out the government's privacy vision and strategy. The framework will provide the foundation for a comprehensive privacy risk management and accountability infrastructure to ensure the right balance between the privacy rights of Canadians and the requirements to fulfill other public interest goals and program mandates. An initiative was underway to consolidate and update various privacy policies relating to privacy impact assessments, data matching, data protection and use of the SIN – all areas of concern to the OPC.

The OPC was consulted by TBS in developing a federal strategy to address concerns about the *USA PATRIOT Act* and Transborder Data Flows, mentioned earlier in this report. The government has responded well to the issue. In late March 2006, TBS published its strategy and issued guidance to federal government institutions for taking privacy into account before making contracting decisions. These documents are available on the TBS web site at **www.tbs-sct.gc.ca**. Among the activities reported as completed are the following:

- The government made all of its 160 institutions subject to the federal *Privacy Act* aware of the privacy issues raised by the *USA PATRIOT Act*.

- Institutions were asked to review their contracting and outsourcing arrangements to identify any risks under the *USA PATRIOT Act*, assess the seriousness of those risks, take corrective actions as needed, and report to TBS. It is reported that 83% classified their contracting as either "no risk" (77 institutions) or "low risk" (57 institutions).

- Best practices are promoted in outsourcing arrangements and a policy guidance document is available to federal institutions. It includes a privacy checklist, upfront advice on the importance of considering privacy prior to initiating contracts, ways of maximizing privacy protection and help in the development of clauses that can be included in requests for proposals and contracts.

The federal strategy also indicates additional steps to further mitigate risk to privacy. Some are listed below, and they illustrate the considerable amount of work required in fully dealing with the issue.

- Development of a privacy management framework to establish high standards for privacy protection throughout the federal government
- Follow-up assessment of federal contracting activities and ongoing contract advice from TBS
- Exploring technology and data architecture solutions to protect information flows, including the use of encryption technology and electronic audit trails
- Development of additional guidelines to cover government-to-government information sharing (within Canada and abroad), auditing of contracts, and technical solutions to protect privacy
- Increased awareness and training related to transborder data flows and existing federal safeguards
- A scheduled 2006 review of *PIPEDA* and the determination of whether the federal *Privacy Act* should also be reviewed (something the OPC strongly believes is long overdue)
- Addressing privacy and transborder data flows for the recently announced Security and Prosperity Partnership (SPP) between Canada, Mexico and the U.S.
- Sharing of best practices in protecting transborder data flows with provincial and territorial governments, as well as the private sector and foreign governments

We also applaud recent efforts by TBS to develop a privacy protection checklist – a set of principles and questions to guide government institutions in developing appropriate access to information and privacy clauses in contracts.

When contracting out, the management of a government program or service must ensure the contract does not weaken the right of public access to information or significantly impact on their department's ability to protect personal information

of individuals. This responsibility does not change when departments contract out services. An effective means to require that an outside service provider respects the requirements of the *Privacy Act* is to insert, when appropriate, relevant clauses in the contractual agreement. In this way, the contract helps ensure that the government institution's responsibility for the protection of personal information continues to be fulfilled by the contractor.

In March 2006 the OPC suggested that TBS pursue further enhancements to government contracting processes by considering the introduction of ways and means for businesses to report on their privacy management capabilities when seeking to become eligible to contract with the federal government. We see opportunity for further inculcating privacy management principles by incorporating privacy self assessment requirements into contracting arrangements with the federal government. This offers a powerful incentive to encourage businesses to comply with data protection principles as part of the social responsibility for doing business with the federal government.

The significance of transborder data flow is underscored by our audit of the Canada Border Services Agency, also discussed in this chapter. This reminds us that protection of personal information is integral to the operations of departments and agencies, and is not just a matter for contracting out to third parties. The OPC urges better management, as well as greater accountability to Parliament and the Canadian public.

The work of TBS on transborder data flow has advanced the building of a Privacy Management Framework. TBS indicates that such a framework would include best practices, sound risk management approaches and tools. The objective would be to ensure that federal institutions meet sound privacy management standards. We understand that TBS will establish an interdepartmental Privacy Committee that will collaborate on the continued development of the Privacy Management Framework.

We will continue monitoring developments and will examine how departments and agencies are adapting new contracting guidance when carrying out audits of federal entities subject to the *Privacy Act.*

Better Control and Accountability Required for Transborder Data Flow

A major audit of the Canada Border Services Agency (CBSA) has now been completed. The following is a summary of the audit results. The full report can be found on the OPC's web site at **www.privcom.gc.ca**.

Our audit of the CBSA and the review of public information about transborder data flow generally leads us to conclude that better control and accountability is required overall. Greater transparency should be given by government in order to allay public concern.

The audit of the CBSA is important since Canadians are concerned about the flow of their personal information to the United States and about the possibility that it may be used for reasons unrelated to anti-terrorism or trans-national crime prevention objectives. The public, as well as Parliament, want to know whether the CBSA, which is the federal government agency most directly involved in maintaining border security, is sharing personal information with its foreign law enforcement and intelligence partners in a way that complies with privacy legislation and that protects the privacy rights of Canadians.

Sound privacy management and accountability are essential in dealing with public concerns about the flow of personal information from Canada to other countries. Accordingly, the objective of the audit was to assess the extent to which the CBSA is adequately controlling and protecting Canadians' personal information as it flows to foreign governments. The audit focused on specific CBSA program areas and systems associated with the its management of personal information relating to travellers. Lines of examination included:

1. Customs enforcement and intelligence activities (land border and airports);
2. Integrated Customs Enforcement System (ICES);
3. Passenger Information System (PAXIS); and
4. National Risk Assessment Centre (NRAC).

The OPC also looked at the CBSA's overall framework for managing privacy and how it reports publicly on its sharing of personal information with other countries.

The approach and methodology included interviewing CBSA staff, examining documents (including records of trans-border sharing of personal information) and reviewing treaties, agreements, policies and practices which provide the framework for sharing this information between governments or their agencies. A special external advisory committee for the audit was formed to guide the work.

The audit reports findings are effective as of November 2005, the date when the examination was substantially completed.

Our Key Findings

The OPC found that the CBSA has policies, procedures and systems in place for managing and sharing personal information with other countries. However, much can be done to better manage the Agency's privacy risks and achieve greater accountability and control over personal information that flows across Canada's borders. Key findings are as follows.

- While written requests for assistance from foreign governments seeking CBSA documents are processed in accordance with Agency requirements, much of the information shared between the CBSA and the United States at the regional level is verbal, and not based on written requests. This contravenes CBSA policy and the Canada-United States *Customs Mutual Assistance Agreement* (CMAA) of June 1984.

- The CBSA needs a coordinated method of identifying and tracking all flows of its transborder data. The Agency cannot, with a reasonable degree of certainty, report either on the extent to which it shares personal information with the United States, or how much and how often it shares this information. By extension, it cannot be certain that all information-sharing activities are appropriately managed and that they comply with section 107 of the *Customs Act* and section 8 of the *Privacy Act*.

- Generally, the IT and management controls are sound for the Integrated Customs Enforcement System (ICES) and Passenger Information System (PAXIS). These systems contain sensitive personal information about millions of travellers. Notably, foreign jurisdictions did not have direct access to these systems. Secondly, electronic releases of information to the United States under the High Risk Travellers and Shared Lookout Initiatives of the CBSA are transmitted over secure communications channels. However, opportunities exist to strengthen the controls to further reduce the risk that personal information could be improperly used or disclosed.

- The CBSA needs to explore ways to improve the quality and control of data it acquires under the Advance Passenger Information/Personal Name Record (API/PNR) initiative to ensure that personal information used for fulfilling the Agency's customs mandate is as accurate and complete as possible.

- The CBSA has not yet evaluated the effectiveness of the High Risk Travellers (HRTI) initiative with the United States because this project has not yet

been fully implemented. In particular, the Agency should assess the extent to which inaccurate or incomplete data may affect individuals or the Agency's ability to identify, deter or apprehend "high-risk" travellers. An evaluation would help the Agency demonstrate that the HRTI initiative has achieved its enforcement and intelligence objectives and, accordingly, that its collection, use and sharing of vast amounts of personal information about millions of travellers are justified.

- Since the CBSA is a new agency, the time is ripe for the Agency to build and integrate a comprehensive privacy-management framework into its day-to-day information handling practices. In particular, the Agency should work toward updating and strengthening the obligations contained in its personal information sharing agreements with the United States. The Agency should also consolidate its reporting of privacy incidents and look for ways to improve its mechanisms for monitoring cross-border disclosures of personal information to foreign law-enforcement agencies and other institutions.

- Finally, the activities associated with sharing data across borders should be as transparent as possible. A clear and complete picture is not readily available with respect to what information is shared with whom, and for what purpose. As is the case for departments generally, the CBSA does not provide enough detail on the transborder flows of personal information, or account in a meaningful way for these flows to Parliament and the Canadian public.

Our audit resulted in 19 recommendations to the CBSA, which are available in our full report. Within two years the OPC will follow up to assess the progress the Agency has made in implementing the recommendations.

Importance of Privacy Impact Assessments

The Office reviews the Privacy Impact Assessments (PIAs) and Preliminary Privacy Impact Assessments (PPIAs) prepared by government institutions for various projects, and we make recommendations on ways to reduce the privacy risks to Canadians' personal information.

Privacy Impact Assessment is a tool that helps ensure that privacy protection is a core consideration when a project is planned and as it is being implemented. PIAs are meant to describe and document what personal information is collected, how it is collected, used, transmitted and stored, how and why it can be shared, and

how it is protected from inappropriate disclosure at each step. In short, it is a risk mitigation tool.

According to policy of the Treasury Board of Canada Secretariat (TBS), PIAs must be included in proposals for all new programs and services that raise privacy issues, and when existing programs are redesigned in a way that affects the collection, use or disclosure of personal information. This includes the conversion of government services for on-line use and delivery.

The TBS policy, which came into effect in 2002, also requires federal government institutions to submit their PIAs and PPIAs to our Office for review. This allows the OPC to analyze the data flow and the steps taken to address potential privacy concerns. We check to make sure an authority is in place that allows the collection and use of Canadians' personal information, and that the regulations and principles of the *Privacy Act* are being respected. We make comments to departments and agencies to identify potential problems that may have been overlooked and, as appropriate, we make recommendations for improving privacy protections. In some cases, we request that projects be considerably modified.

The OPC believes the PIA policy has had a great impact on improving the overall awareness of privacy within government institutions. In our view, it has focused attention on potential privacy issues of a number of government programs. The whole process provides a greater level of protection for the personal information that Canadians give to the federal government. A well functioning PIA practice is key for a sound Privacy Management Framework.

We are pleased to note that many of the PIAs we receive are becoming more precise and thorough in the years since the policy was first introduced. However, there is still considerable room for improvement. For example, the OPC has been encouraging departments to include in their submissions the action plans for implementing privacy protection strategies.

This fiscal year the OPC looked at a wide range of projects undertaken by a number of departments, including Human Resources and Skills Development Canada (HRSDC), Health Canada, the Royal Canadian Mounted Police (RCMP), Transport Canada, Indian and Northern Affairs Canada, Citizenship and Immigration Canada, Revenue Canada, the Canada School of the Public Service, Social Development Canada, Veterans Affairs Canada, Public Works and Government Services Canada (PWGSC), Statistics Canada, the Canadian Air Transport Security Authority, the

Canada Border Services Agency (CBSA), National Defence, Farm Credit Canada and the Canada Firearms Centre. As varied as the responsibilities of these departments are, the projects share a common characteristic – they all collect, retain, share or disclose the personal information of Canadians.

The following examples of PIAs offer an indication of the range and depth of the various projects we reviewed:

- The RCMP Integrated Query Tool, a web application that brings together information from several discrete police information data bases into a central repository to allow a single search capability and a consolidated report on an individual

- The RCMP Canadian Police Information Centre (CPIC) Renewal project and its sharing agreements with other jurisdictions

- A system which allows Employment Insurance (EI) claimants to complete and submit their required reports online, using computers at home or in employment centres

- A PWGSC project to contract foreign banking services in order for Canadians living overseas to receive government payments, such as pensions, in a timely fashion

- A Children's Respiratory Health Study, surveying 25,000 elementary school children

- A High Risk Traveller Identification Project in which the CBSA collects and shares with the United States information on individuals travelling by air to that country, and collects and analyses information on individuals arriving by air to Canada

- A pre-boarding screening project involving remote video surveillance of passengers in airport boarding areas across the county by the Canada Air Transport Security Authority (CATSA)

- An electronic health record project for the Canadian Armed Forces with the potential to contain the medical, dental and psychological health information for more than 80,000 Armed Forces personnel

- Citizenship & Immigration Canada's use of biometrics (fingerprints and photos) in field trials at border crossings and as a method of cross-checking refugee claimants

As illustrated above, the projects reviewed are diverse and in many cases require specific recommendations that pertain to the type of information collected and the type of systems being used. However, there are similarities in the types of privacy risks encountered, and general best practices for risk mitigation.

For example, PIAs may only state in fairly general terms that accountability for protecting personal information "will be communicated" to staff, or that staff involved will be "made aware of" their responsibilities. The OPC prefers a much more specific and proactive approach, and has recommended the issuance of binding guidelines, protocols and well documented procedures.

Similarly, PIAs submitted to us may not include a process for the departments or agencies to inform affected individuals if personal information has been found to be inappropriately disclosed either accidentally or as a result of theft. We recommend that every department have a clear policy in place to guide managers and other staff in instances where personal information has gone astray.

Other examples of common recommendations to help mitigate privacy risks include:

- Asking government institutions to ensure that privacy protections are built into contracts for processing or storing personal information, including regular departmental audits of contractors' practices

- Recommending the inclusion of clear acknowledgement of responsibility for safeguarding personal information in service agreements

- Ensuring that PIA summaries are written in clear, non-technical language and that they are posted on departmental web sites

- Reminding institutions of their obligation to amend personal information banks to reflect new information being collected, or new uses for that information, as required under the *Privacy Act*

- Training all staff in privacy protective work habits, and ensuring that all office procedures are compliant with the *Privacy Act*

- Advising institutions to monitor the transaction logging programs that are in place to protect against unauthorized access to personal information

As a particular issue, the OPC notes a trend of increased sharing of information among police and national security agencies for law enforcement and anti-terrorism purposes. Several of the PIAs reviewed could be grouped into these categories. A concern is that this Office receives privacy assessments of large and potentially privacy invasive projects in disjointed pieces, rather than as part of a comprehensive overview. The OPC has recommended to entities such as Transport Canada, the CBSA and the RCMP that an overall privacy management framework and/or a comprehensive PIA be developed at the outset of such large, integrated projects.

The trend towards government institutions forming integrated networks to share personal information creates new privacy challenges. When several departments and agencies feed data into a network that is accessible to partners that span across jurisdictions, issues of governance, custody and control of information arise, as do issues around consent, right of access and correction.

The OPC will continue monitoring some of the large-scale projects through PIA review and updates, including the expansion of the Canadian Public Safety Information Network (CPISN). This initiative, which falls under Public Safety and Emergency Preparedness Canada (PSEPC), seeks to establish a national information sharing network for Canada's criminal justice system and law enforcement agencies, linking previously separated sources of data related to crime and offenders. The OPC will also monitor projects that collect and analyze the personal information of travelling individuals collected at border points and from passenger reservation systems.

As part of a privacy management framework, the OPC will continue encouraging departments to establish a formal administrative structure such as an internal committee or working group that is specifically responsible for reviewing departmental initiatives to determine whether they require a PIA, and for implementing privacy risk reduction measures after a PIA has been done. The OPC is actively considering undertaking an audit of the government-wide PIA system in order to establish whether institutions are doing PIAs when they should, are following up on risk assessment findings, and fixing privacy protection gaps when identified.

Other Work

Following are other audit and review projects from the past fiscal year.

Statistics Canada Census
Statistics Canada has been consulting this Office regarding the 2006 Census for the past several years. One new dimension for the Census was a proposal to rely on services of a third party contractor. In response to concerns of this Office and others about initially proposed contracting arrangements with a company based in a foreign jurisdiction, Statistics Canada significantly revised its approach to ensure that no census data would reside outside of the department.

Our monitoring of Census preparation included document review and a visit to the Data Processing Centre (DPC) of Statistics Canada. Based on this, we are satisfied that reasonable precautions are being taken to ensure the integrity and confidentiality of Census data. In addition to contract and policy means, these measures include independent IT security assessment of DPC, a threat risk assessment, and control of traffic in and out of the DPC. We did point out the need to amend documented procedures to clarify for the purpose of the 2006 Census that there should be no remote access to the DPC.

Canada Post Track-a-Package
In 2005 we investigated apparent vulnerabilities regarding Canada Post Corporation's (CPC) web-based Track-a-Package service. As a result, CPC agreed to undertake several practice improvements. This included procedures to authenticate the identity of clients requesting information, means to inform customers that their signature will be available on the internet and ensuring that their signature does not appear for registered mail when a customer objects to this, and ways of reminding customers of the importance of protecting their PIN.

Disclosure of certain personal information on CRTC web site
In response to concerns communicated to our Office about the Canadian Radio-television and Telecommunications Commission (CRTC) publishing on its web site the personal contact information of interveners in public proceedings, we engaged with the CRTC in reaching reasonable solutions regarding notification and limiting access to such information.

In the Courts

Privacy Act Applications

Once the Office of the Privacy Commissioner has investigated a complaint, section 41 of the *Privacy Act* allows the individual to apply to the Federal Court for review of the government's refusal to provide access to personal information. The following applications and appeals were filed in the past fiscal year. In keeping with our mandate, we have chosen not to reproduce the official style of cause of the cases in order to respect the privacy of the individual complainants. We are listing the court docket number and the name of the government institutions only.

Président de l'Agence spatiale canadienne
Federal Court File No.: T-1448-05

Solicitor General of Canada
Federal Court File No.: T-1724-05

Minister of Public Safety and Emergency Preparedness
Federal Court File No.: T-2123-05

Royal Canadian Mounted Police
Federal Court File No.: T-66-06

Solicitor General of Canada
Federal Court of Appeal File No.: A-111-05

Minister of National Revenue
Federal Court of Appeal File No.: A-270-05

Section 42 of the *Privacy Act* also allows the Commissioner to appear in Federal Court. The Commissioner may ask the Court to review an institution's refusal of access to personal information (with the complainant's consent). She may act on behalf of individuals who have applied for review themselves, or with the leave of the Court, be a party to any review sought under section 41. No such situation arose in the past fiscal year.

Judicial Review

Complainants will sometimes seek judicial review under section 18.1 of the *Federal Courts Act* against the Privacy Commissioner. This occurred in the case described below, where the Commissioner was required to explain her jurisdiction to the Court when the complainant sought remedies that the Commissioner had no authority to grant. This case illustrates the seriously limited remedies available under the *Privacy Act* for any breaches other than improper denials of access. The Commissioner finds herself in the unenviable position of having to demonstrate to the Court how she is unable to help the complainant. Clearly, this is an important issue for reform of the *Privacy Act*, which is discussed earlier in this report.

Royal Canadian Mounted Police and Privacy Commissioner of Canada
Federal Court File No.: T-1180-04 and Federal Court of Appeal File No.: A-183-05

The applicant complained to the Privacy Commissioner, that among other wrongful conduct, the RCMP had breached the *Privacy Act* by disclosing his personal information to his employer without his consent. The Assistant Commissioner responsible for the *Privacy Act* agreed that his disclosure complaint was well-founded, but indicated that, unfortunately, no remedy exists for such disclosures under the Act.

On June 18, 2004, the applicant sought a judicial review of the Assistant Commissioner's report on his disclosure complaint. Although the *Privacy Act* restricts remedies to questions of access, he argued that the Privacy Commissioner must necessarily have the authority to fashion remedial orders and relief in cases (like his) where the *Privacy Act* has been contravened.

In a decision dated March 29, 2005, the Court determined that the Privacy Commissioner had fulfilled her obligations under the *Privacy Act* and had correctly advised the applicant that the *Privacy Act* provides no remedy to address the

respondent's breach of his privacy. The applicant can obtain no further relief in the Court for the improper disclosure.

The applicant appealed the Federal Court decision in April 2005, but discontinued the appeal a few weeks prior to the scheduled appeal hearing.

Public Education and Communications

The Office of the Privacy Commissioner of Canada is mandated specifically under *PIPEDA* to educate the public and organizations on rules that govern the collection, use and disclosure of personal information in the course of commercial activities. Although there is no specified mandate for public education and communications under the *Privacy Act*, clearly it is necessary to communicate with government institutions about the application of the Act and the implications of their actions on the privacy rights of Canadians, so they can be held accountable for their personal information handling practices. There is also an expectation for the Commissioner and her Office to comment publicly on federal government initiatives involving personal information.

Public Opinion Polling

In 2004-2005, the Office developed a comprehensive communications and outreach strategy for the coming fiscal years. One of the initiatives in this strategy involved public opinion research, so that we could better understand how Canadians view privacy issues, as well as their levels of awareness. A majority of Canadians surveyed expressed a strong sense that their privacy and protection of their personal information was being eroded. Among other findings of particular interest, Canadians expressed concern about the transborder flow of personal information and expressed lower confidence in new technology, especially in the area of electronic health records. Respondents were also of the view that privacy laws should be updated to address the rapid evolution of information technology. This past fiscal year (2005-06), we conducted a follow-up study. The findings suggest that the concerns outlined above are still very present, and also that privacy laws must be updated to keep pace with leading-edge, transformational technologies that have a significant impact on privacy. A report on the latest study will be posted to our Web site in the summer of 2006.

Speeches and Special Events

Speaking engagement opportunities have helped our Office promote privacy issues among diverse audiences and settings across Canada and abroad, including to professional and industry associations, non-profit and advocacy groups and universities. In the 2005-2006 fiscal year, the Commissioner, Assistant Commissioners and other senior officials delivered approximately 40 speeches. Our Office also continued to host an in-house Privacy Lecture Series approximately once a month. Privacy experts from Canada and abroad shared their observations on a wide range of issues with an internal and external audience of stakeholders.

Media Relations

Privacy issues continued to be of interest to the media in 2005-2006, with media coverage in Canada on issues such as government initiatives with privacy implications, privacy breaches, as well as surveillance technologies. These areas generated numerous media calls to and interviews with OPC officials. In addition, through other proactive media relations efforts, such as the dissemination of news releases, the Commissioner had an opportunity to share her views on federal government legislation and initiatives, such as the Passenger Project or the "No-Fly List", and the Office's views regarding transborder flows of personal information.

Web Site

The Office frequently posts new and useful information to its web site. Fact sheets, news releases, speeches, reports and publications, and case summaries of findings under the federal private sector law are posted to keep the site relevant to individuals and institutions. Since 2001-2002, we are pleased to report that visits to the site have more than quadrupled, and that we surpassed the one million visitors' mark in the 2005-2006 fiscal year.

Publications

Each year, the OPC produces and disseminates publications to individuals and organizations seeking information on privacy matters. These documents include annual reports, guides, as well as fact sheets and copies of both federal statutes. Not only were these materials sent to individuals upon request, they were also distributed at conferences and special events. Increasingly, individuals are also accessing these documents on our web site.

Internal Communications

Internal communications activities were also a focus of the Office in 2005-2006, increasing transparency between management and staff, especially throughout the Office's institutional renewal. Internal communications activities in 2005-2006 involved providing information on issues such as human resources, upcoming speaking engagements, Parliamentary appearances, senior management and labour management committee meetings, and special events. In 2005-2006 the Office also launched its Intranet site which serves as the internal communications portal, maximizing staff access to information.

Although public education and communications are an important part of our work, limited financial and human resources have constrained our ability to go much beyond simply responding to issues, rather than anticipating them and preparing public education strategies in advance. We have also discussed this in our recently tabled 2005 Annual Report to Parliament on *PIPEDA*. However, expected increases in funding will permit us to not only undertake the activities outlined above, but to undertake more extensive public awareness initiatives and to carry out the comprehensive proactive communications and outreach strategy mentioned earlier in this chapter.

Corporate Services

The Commissioner continues to focus on effective management renewal. During 2005-06, the main priority was the completion of the business case seeking long-term permanent resources. A second priority was strengthening our Human Resources management capacity.

Planning and Reporting

A foundation component of the Office's institutional renewal is a strategic planning, reporting and control process. In 2005-06 we completed our second year under this revised process. The strategic plan established at the beginning of the year was our road map for the year. One important part of the new process was reporting and review opportunities. We reviewed and made adjustments to plans and budgets throughout the year. To assist in our reporting, we continued work on our Performance Measurement Framework and our monthly performance report has been in place for 18 months. This serves as a critical management tool for the evaluation of branch results against targets.

Human Resources

We continue to work toward the development and implementation of changes to improve how the Office is run and the overall quality of the workplace. Significant changes and improvements have been made to the Human Resource management policies and practices.

We have implemented a number of Human Resource policies in consultation with central agencies and unions in line with the new *Public Service Employment Act* (PSEA) requirements. These policies will guide us as we build on the successes of the past year and as we continue on our path of institutional renewal. An Instrument

of Delegation of Human Resource Management was developed and will serve as a tool to inform and guide managers, and enable them to manage their human resources. A Strategic Human Resource Plan and a new Staffing Strategy, as well as an Employment Equity Action Plan, will help the OPC achieve its mandate and will ensure the recruitment of a highly qualified workforce that is diversified and representative of Canadian society. As part of the OPC's commitment to increase transparency in the staffing processes, a staff newsletter was developed; it is distributed on a monthly basis to all staff.

We made significant strides in the area of organizational learning, including the development of a learning strategy with the Canada School of Public Service (CSPS), training and information sessions in areas such values-based staffing, language, performance management, employee appraisals, and harassment awareness in the workplace. We have provided briefing sessions at our quarterly all-staff meetings, as well as to all managers on various aspects of the new PSMA and PSEA. The Learning Strategy and Curriculum with the CSPS enables staff to continue to develop the expertise and competencies required to fulfill their functions, which will position them to take on their new responsibilities and accountabilities. The learning strategy has been modified to reflect training requirements related to the new PSEA, including a Senior Management Committee Engagement Session and PSEA training for sub-delegated managers, both of which were offered in March 2006.

We continue to work collaboratively with the Public Service Commission and the Public Service Human Resources Management Agency of Canada on follow-up measures to the recommendations of their audit reports. This includes measures that will allow OPC the opportunity to regain its full staffing delegation authority.

Finance and Administration

The OPC received a clean opinion on Audited 2004-2005 Financial Statements by the Office of the Auditor General of Canada. Combined with the 2003-2004 clean opinion, this is a very positive indicator that the organization has indeed advanced on the path of institutional renewal. The organization has built on that success by establishing planning and review cycles, and by streamlining and improving the financial management policies and practices of the OPC.

Information Management / Information Technology

The IM/IT Division has accomplished many things over the past year. We have renewed our server infrastructure and increased data storage to allow for the scanning of documents. Good progress has been made on our Information Management project. Upgrades to our records management and correspondence tracking systems have been completed. Financial systems – Salary Management System (SMS) and FreeBalance - have been upgraded and the FreeBalance server has been upgraded as well. Five new tracking systems have been developed for the Audit and Review Branch to allow them to track their Audit files. We have completed the Action Plan for MITS Compliance and we are working steadily towards the December 2006 compliance deadline.

Our Resource Needs

As described in an earlier section of this report, the Office completed a thorough analysis that included a business process review of all OPC functions. Following that review we requested more than a fifty percent increase in resources which will bring our overall budget to approximately $18 million dollars and our full-time equivalents (FTEs) to a total of 140 over the course of the next two years. There will also be a shift in the relative distribution of resources to position the organization to be more proactive as opposed to reactive.

Financial Information

In past years the Annual Report was often produced later. This allowed us to provide financial tables relating to our expenditures at that time. The normal financial reporting cycle does not allow us to provide audited financial statements at the time of tabling this report. We will provide financial information in our Reports on Plans and Priorities, as well as our Departmental Performance Reports, both of which are tabled in Parliament. Furthermore, as we have in the past, we will also post to our web site the Audited Financial Statements for fiscal year 2005-06 once they are completed. For additional financial information, we encourage you to visit our web site at **www.privcom.gc.ca**.

Appendix 1

Access and Privacy Complaints Closed by Institution and Finding
From April 1, 2005 to March 31, 2006

Respondent	Discontinued	Early Resolution	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Well-founded – Resolved	Total
Bank of Canada	0	0	1	0	0	0	0	1
Canada Border Services Agency	1	0	4	1	1	0	0	7
Canada Customs and Revenue Agency	5	0	4	0	8	0	1	18
Canada Post Corporation	28	0	4	0	6	1	0	39
Canada Revenue Agency	0	2	30	2	6	2	1	43
Canadian Food Inspection Agency	0	0	0	1	0	0	0	1
Canadian Human Rights Commission	0	0	0	1	1	0	0	2
Canadian Nuclear Safety Commission	0	0	1	0	0	0	0	1
Canadian Security Intelligence Service	15	0	35	0	1	0	0	51
Canadian Space Agency	0	0	2	0	0	0	2	4
Citizenship and Immigration Canada	6	0	7	0	10	1	3	27

Access and Privacy Complaints Closed by Institution and Finding (cont.)
From April 1, 2005 to March 31, 2006

Respondent	Discontinued	Early Resolution	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Well-founded – Resolved	Total
Correctional Investigator	1	0	0	0	0	1	0	2
Correctional Service Canada	27	11	40	3	22	14	3	120
Farm Credit Canada	0	0	1	0	0	0	0	1
Fisheries and Oceans	1	0	3	0	1	0	0	5
Foreign Affairs and International Trade Canada	0	0	2	0	0	0	1	3
Health Canada	0	0	2	0	4	0	0	6
Human Resources and Skills Development Canada	0	3	5	0	9	1	2	20
Immigration and Refugee Board	0	0	8	0	1	0	1	10
Indian and Northern Affairs Canada	0	0	2	0	0	0	0	2
Industry Canada	0	0	1	0	0	0	0	1
Justice Canada, Department of	0	0	11	0	3	0	2	16
Library and Archives Canada	0	0	0	0	3	0	0	3
Military Police Complaints Commission	0	0	1	0	0	0	0	1
National Capital Commission	0	0	0	0	4	0	0	4
National Defence	1	0	1	2	3	2	1	10
National Gallery of Canada	1	0	0	0	0	0	0	1
National Parole Board	0	0	1	0	2	1	0	4

Access and Privacy Complaints Closed by Institution and Finding (cont.)
From April 1, 2005 to March 31, 2006

Respondent	Discontinued	Early Resolution	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Well-founded – Resolved	Total
National Research Council Canada	0	0	0	0	1	0	2	3
Natural Sciences and Engineering Research Council of Canada	0	0	0	0	1	0	0	1
Office of the Commissioner of Official Languages	0	0	0	0	0	0	1	1
Office of the Chief Electoral Officer	0	0	10	0	1	0	0	11
Pacific Pilotage Authority Canada	0	0	0	0	0	0	1	1
Pension Appeals Board Canada	0	0	0	0	1	0	0	1
Privy Council Office	0	0	1	0	0	0	0	1
Public Service Commission Canada	0	0	0	0	1	3	0	4
Public Works and Government Services Canada	0	0	1	1	0	0	0	2
Royal Canadian Mounted Police	5	0	36	4	12	1	1	59
Social Development Canada	1	0	3	0	4	0	0	8
Statistics Canada	0	0	0	0	2	1	0	3
Transport Canada	0	1	0	0	0	0	0	1
Treasury Board Secretariat	0	0	1	0	0	0	1	2
Veterans Affairs Canada	0	0	0	0	2	0	0	2
Total	**92**	**17**	**218**	**15**	**110**	**28**	**23**	**503**

Appendix 2

Time Limit Complaints Closed by Institution and Finding
From April 1, 2005 to March 31, 2006

Respondent	Discontinued	Early Resolution	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Total
Canada Border Services Agency	0	0	0	0	0	11	11
Canada Post Corporation	16	0	0	0	0	0	16
Canada Revenue Agency	4	0	7	10	0	17	38
Canadian Air Transport Security Authority	0	0	0	0	0	1	1
Canadian Food Inspection Agency	1	0	0	0	0	0	1
Canadian Security Intelligence Service	0	0	4	0	0	1	5
Citizenship and Immigration Canada	2	0	1	0	0	55	58
Correctional Service Canada	2	1	3	0	1	54	61
Environment Canada	0	0	0	0	0	1	1
Export Development Corporation	0	1	0	0	0	0	1

Time Limit Complaints Closed by Institution and Finding (cont.)
From April 1, 2005 to March 31, 2006

Respondent	Discontinued	Early Resolution	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Total
Foreign Affairs and International Trade Canada	0	0	6	0	1	20	27
Health Canada	0	0	0	0	0	9	9
Human Resources and Skills Development Canada	0	0	2	0	0	2	4
Immigration and Refugee Board	15	0	6	0	4	98	123
Industry Canada	0	1	0	0	0	0	1
Justice Canada	1	0	2	0	0	6	9
Library and Archives Canada	0	0	0	0	0	1	1
National Archives of Canada	0	0	0	0	0	1	1
National Defence	4	0	1	0	0	18	23
National Gallery of Canada	0	1	0	0	0	0	1
National Research Council Canada	0	0	23	0	0	23	46
Privy Council Office	0	0	0	0	0	2	2
Public Service Commission Canada	0	0	2	0	0	0	2
Public Works and Government Services Canada	0	0	1	0	0	1	2
Royal Canadian Mounted Police	4	0	1	1	2	83	91
Transport Canada	0	2	0	0	0	0	2
Total	**49**	**6**	**59**	**11**	**8**	**404**	**537**