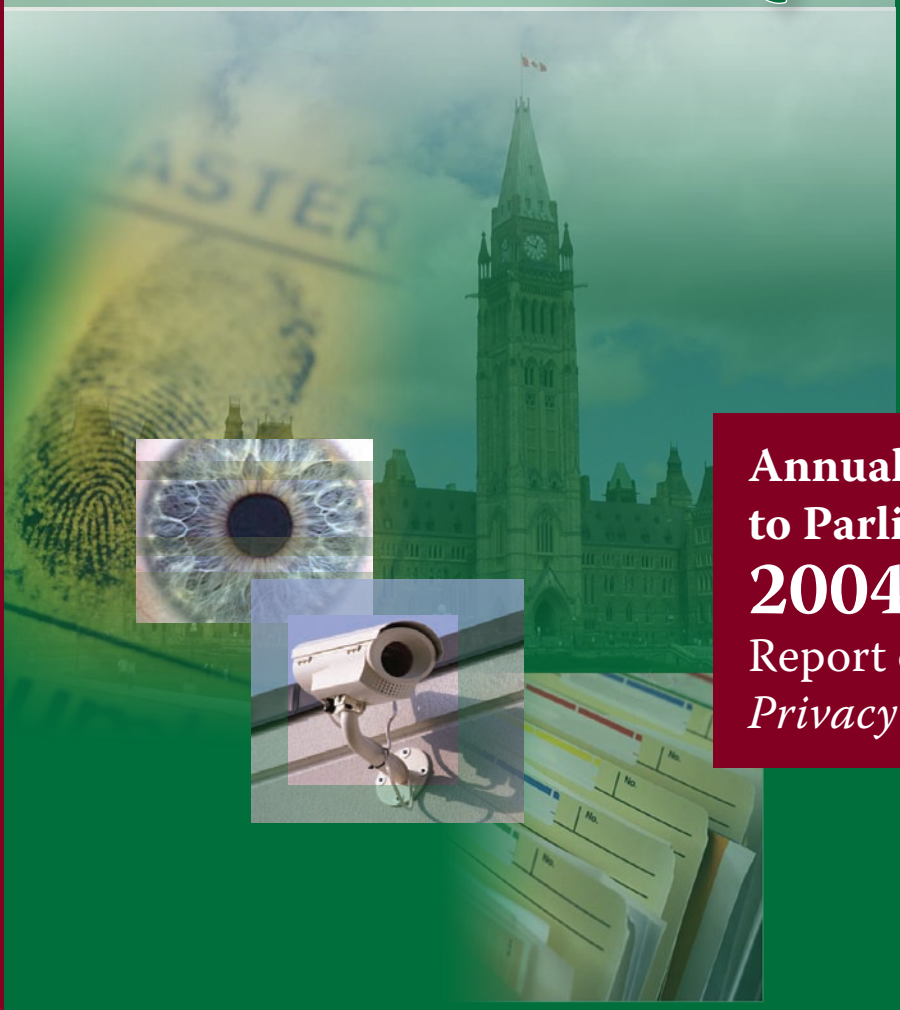
Privacy Commissioner of Canada

Commissaire à la protection de la vie privée du Canada

Privacy



Annual Report to Parliament 2004-2005

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. IP50-2005
ISBN 0-662-68763-9

This publication is also available on our Web site at www.privcom.gc.ca, in addition to our 2004 Annual Report on the *Personal Information Protection and Electronic Documents Act*.

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

October 2005

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

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Privacy Act* for the period from April 1, 2004 to March 31, 2005.

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

October 2005

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, 2004 to March 31, 2005.

Yours sincerely,

Original signed by

Jennifer Stoddart
Privacy Commissioner of Canada

Table of Contents

Foreword

If Canada had optimal privacy protection, the Annual Reports from the Office of the Privacy Commissioner would be a detailed account of successful interventions to protect the rights of individuals, of audits of well run federal institutions with mature business processes incorporating privacy requirements, and a thorough policy analysis of new information systems and technologies. Instead, reports from this office have too often lamented the steady erosion of rights and the assault of new surveillance technologies on the daily lives of Canadians, and our impotence to reverse the trends.

This year is no exception. Increasingly, the phenomenon of outsourcing and public-private partnerships means the data of Canadians may be in the hands of the private sector even when under the control of the government.

We are generally pleased with the results of our interventions, and with the cooperation of business and government alike to try to comply with fair information practices and legal requirements, but the privacy threats seem to be multiplying like a bad virus, threatening to overwhelm us.

If there is one central message we want to convey this year, it is that we are not going to allow that to happen. We mean business, and we are counting on the support of all institutions to help us grapple with these issues and preserve and maintain the privacy of the individuals in this country.

Canadians are anxious, and they expect us to enforce the law and their government to respect the values inherent in our Constitution, as recent polling data shows. We will do our part, but the defence of these fundamental rights of information protection demands a shift in public policy such as has started to take place with respect to the

environmental movement. Over the last twenty years it has become well accepted that it is not alright to pollute, that it is expected behaviour to recycle. We need the same thing to happen with respect to personal information: it is not alright to gather information without consent, it is not alright to share it promiscuously, it is not alright to hide your information practices from your public.

Three main themes will be found throughout this report, because they are the most significant issues we have faced: security and the voracious appetite for personal information and surveillance that has sprung up in the post-911 environment, sharing of information and outsourcing of data operations across borders, and the need to modernize our *Privacy Act*. Whether you read this report as an individual member of the public, a public servant, or a Parliamentarian, there is a message we want to convey to you:

Start caring about privacy now, before it is too late. Citizens' involvement in the debate will determine the course our country takes with regard to the protection of personal information. Do your part to control the flow of everyone's personal information. We are here to help, but we cannot do the job alone.

This year, we have published two separate reports, dividing the Privacy Act from the Personal Information Protection and Electronic Documents Act (PIPEDA). We felt this was more appropriate given that the Privacy Act requires us to report on the fiscal year (2004-2005), while under PIPEDA we are required to report on the calendar year (2004). As well, each Act provides a separate framework for investigations and audits. Both our reports detail efforts we have taken to meet the growing demands on our Office to act as the guardians of privacy for Canadians on behalf of Parliament. There is much overlapping between these reports because many of our activities are not particular to one law or another and, increasingly, the policy issues are common across the two regimes.

Our Multi-Faceted Mandate

The Office of the Privacy Commissioner (OPC), oversees both the *Privacy Act*, which applies to federal institutions, and *PIPEDA* which governs personal information management in commercial activities in the private sector.

Parliament has given the Office a mandate to ensure that both the federal public sector and private sector (in most provinces) are held accountable for their personal information handling and that the public is informed about their privacy rights. The mandate is not always understood.

As an independent ombudsman, we are:

- An *investigator* and *auditor* with full powers to investigate and initiate complaints, conduct audits and verify compliance under both Acts;

- A *public educator* and *advocate* with a responsibility both to sensitize businesses about their obligations under *PIPEDA* and to help the public better understand their data protection rights;

- A *researcher* and *expert adviser* on privacy issues to Parliament, government and businesses; and

- An *advocate for privacy principles* involved in litigating the application and interpretation of the two privacy laws. We also analyze the legal and policy implications of bills and government proposals.

Although the *Privacy Act* does not give the Privacy Commissioner a formal legal mandate to conduct public education, the Commissioner often needs to inform the public and government in order to achieve her mandate to hold federal government departments and agencies accountable for their personal information-handling practices.

Policy Perspective

Parliament's Window on Privacy

The Privacy Commissioner of Canada is an Agent of Parliament who reports directly to the Senate and the House of Commons. As such, the OPC acts as Parliament's window on privacy issues. Through the Commissioner, Assistant Commissioners and other senior OPC staff, the Office brings to the attention of Parliamentarians issues that have an impact on the privacy rights of Canadians. The OPC does this by tabling Annual Reports to Parliament, by appearing before Committees of the Senate and the House of Commons to comment on the privacy implications of proposed legislation and government initiatives, and by identifying and analyzing issues that we believe should be brought to Parliament's attention.

The Office also assists Parliament in becoming better informed about privacy, acting as a resource or centre of expertise on privacy issues. This includes responding to a significant number of inquiries and letters from Senators and Members of Parliament.

➤ *Appearances before Parliamentary Committees*

Appearances before committees of the Senate and the House of Commons constitute a key element of our work as Parliament's window on privacy issues. During the period covered by this report, the Privacy Commissioner and other senior OPC staff appeared 11 times before Parliamentary committees: six times on bills with privacy implications; four times on matters relating to the management and operations of the Office; and once before a Senate committee studying consumer issues in the financial services sector.

The OPC appeared on the following bills before Parliamentary committees in 2004-2005:

- Bill C-2, *An Act to Amend the Radiocommunication Act* (May 6, 2004)
- Bill C-12, the *Quarantine Act* (November 18, 2004)
- Bill C-22, *An Act to establish the Department of Social Development and to amend and repeal certain related Acts* (December 9, 2004)
- Bill C-23, *An Act to establish the Department of Human Resources and Skills Development and to amend and repeal certain related Acts* (December 9, 2004)
- Bill C-11, the *Public Servants Disclosure Protection Act* (December 14, 2004)
- Bill C-13, *An Act to Amend the Criminal Code, the DNA Identification Act and the National Defence Act* (February 8, 2005)
- Bill S-18, *An Act to Amend the Statistics Act* (February 24, 2005)

Regarding the management and operations of the Office, OPC officials appeared before Parliamentary committees on the following matters in 2004-2005:

- Annual Report and Main Estimates 2003-2004 (November 17, 2004)
- Supplementary Estimates (December 1, 2004)
- Funding mechanisms for Agents of Parliament (February 10, 2005)
- Role and operations of the OPC (February 16, 2005)

➤ *Other Parliamentary Liaison Activities*

The OPC has undertaken a number of other initiatives over the course of the past year to improve its ability to advise Parliament on privacy matters.

In May 2004, we created a dedicated Parliamentary liaison function within the Office to improve our relationship with Parliament. This function resides in the Research and Policy Branch, reflecting the OPC's desire to focus its Parliamentary affairs activities on providing in-depth and accurate policy advice to Senators and Members of Parliament.

Improving on how we assess, monitor and forecast Parliamentary activity has been a priority for us in the past year. The OPC put in place a new and improved system for monitoring the status of bills on Parliament Hill, as well as keeping tabs on new and emerging developments of interest to privacy promotion and protection. Our goal is to build bridges to departments so that we can comment earlier in the legislative process, when our criticisms could be dealt with more effectively. It is often too late

when a bill has been introduced in the House of Commons, to rethink approaches to information issues.

The Office has responded to a significant number of inquiries and letters from Senators and MPs this year, and the Commissioner and Assistant Commissioners have also met privately with Senators and MPs who wished to discuss policy matters relating to privacy, or wanted to know more about the operations of the Office.

In late 2004, the OPC, in conjunction with the Office of the Information Commissioner, and in collaboration with the Research Branch of the Library of Parliament, held an information session for Parliamentarians and their staff on the roles and mandates of both Offices. This information session was well attended and raised many questions among participants. We believe such information sessions contribute to increasing awareness of privacy issues on Parliament Hill, and look forward to holding more such sessions in the future.

➤ *Priorities for the Coming Year*

The Office expects to be busy in the area of Parliamentary affairs over the next fiscal year. There are a number of bills of interest to us expected in the upcoming session, and the statutory review by Parliament of the *Personal Information Protection and Electronic Documents Act* is expected to start in 2006. The OPC plans to play a constructive role during this review, by providing thoughtful advice to Parliamentarians mandated with studying at how the Act has worked over the course of its first years of implementation, and how it may be modified and improved.

The OPC will continue to follow with interest the Parliamentary review of the *Anti-terrorism Act*. The Privacy Commissioner appeared twice before committee on this matter in fiscal year 2005-06—once before a Senate special committee reviewing the Act (May 9, 2005), and on another occasion before a sub-committee of the Commons Standing Committee on Justice (June 1, 2005).

We recognize that to act as an effective Agent of Parliament we need to have good working relationships with federal departments and agencies. The OPC plans to put more emphasis on identifying and raising privacy concerns when government initiatives are being developed rather than waiting until they reach Parliament, as this increases the possibility that privacy concerns will be taken into account.

National Security

In May 2004 Parliament passed the *Public Safety Act*. The Act, originally introduced in November 2001 in the wake of the September 11 terrorist attacks, allows the Minister of Transport, the Commissioner of the Royal Canadian Mounted Police (RCMP) and the Director of the Canadian Security Intelligence Service (CSIS) to compel, without a warrant, air carriers and operators of aviation reservation systems to provide information about passengers. While this may seem reasonable given the risks terrorists pose to air transport, authorities are not using this information exclusively for anti-terrorism and transportation safety. The *Public Safety Act* also allows law enforcement authorities to use the information to identify passengers with outstanding arrest warrants for a wide range of ordinary criminal offences. In other words, the machinery of anti-terrorism is being used to meet the needs of ordinary law enforcement, lowering the legal standards that law enforcement authorities in a democratic society must meet.

Another provision in the *Public Safety Act* amends *PIPEDA* to allow private sector institutions to collect personal information, without clients' consent, and disclose it to government, law enforcement and national security agencies. The amendment applies not just to transportation companies but to any institution subject to *PIPEDA*—financial institutions, telecommunications companies and retailers. These disclosures effectively co-opt private sector institutions, pressing them into the service of law enforcement activities and dangerously blurring the line between the private sector and the state.

Not only is the private sector being deputized by law enforcement; an anti-terrorism mindset is permeating more conventional law enforcement and public safety initiatives. This mindset threatens to erode our privacy rights and other freedoms because the constraints under which national security agencies operate—for example, the requirement for judicial authorization—are often weaker than those governing law enforcement agencies.

Debates about public safety are nothing new. They have been underway for several years, certainly before 9/11. However, we now hear explicit messages about "intelligence-based policing" and vigilance to prevent terrorism from taking hold in our society. The proliferation of these messages without an equal attention to the need to protect civil liberties is of concern. Implicit in the debate is a general acceptance of various types of surveillance, and a marked shift towards the reduction of our civil liberties. A state which routinely accepts threats to civil liberties and Charter-protected autonomy rights is on spongy ground.

While our society must deal with legitimate security concerns, we must also guard against fear-mongering and intolerance which threaten a liberal democracy.

Anti-terrorism Act

The *Anti-terrorism Act* (passed in the fall of 2001) requires a Parliamentary review after three years. The Senate has appointed a Special Committee to conduct its review while the House of Commons has referred the review to the Public Safety and National Security Subcommittee of the Standing Committee on Justice, Human Rights, Public Safety and Emergency Preparedness.

In participating in this review, we define the most important questions for the review to be: Are the additional law enforcement and surveillance powers necessary and proportional to the threats they were intended to address? Have the security benefits justified the sacrifice of privacy and other rights?

We face several challenges preparing for the review, one of which is trying to determine whether the extraordinary powers the *Anti-terrorism Act* granted law enforcement and national security agencies are really needed and effective. We have found no empirical assessments of their effectiveness in detecting, preventing or deterring terrorist acts. Our challenge is compounded by government simultaneously granting new powers to law enforcement and national security agencies while weakening transparency and accountability.

The *Anti-terrorism Act* cannot be viewed in isolation. In the Spring of 2005 we urged the two Committees reviewing the Act to interpret their mandates broadly, examining the cumulative impact on Canadians' privacy rights of all the measures passed in the wake of the September 11 attacks—amendments to the *Aeronautics Act* (passed in late 2001), the Public Safety Act and the *Immigration and Refugee Protection Act*.

Transborder Flows of Personal Information

The *Anti-terrorism Act* is by no means the only government initiative that threatens privacy. Government is collecting, analyzing and sharing more personal information helped along by improved technology, new legislation, government reorganization, and greater co-operation with foreign states. Flows of personal information are likely to have increased significantly among government departments and agencies both within and outside Canada.

All these factors have fundamentally shifted the relationship between national security, law enforcement and informational privacy with a corresponding loss of privacy and due process protections for individuals.

In April 2004, the government issued its first-ever National Security Policy. The Policy promised to create an "Integrated Threat Assessment Centre" to help collect, analyze and share intelligence and other information—effectively contributing to a more integrated international intelligence community. This Centre is housed in CSIS but staffed by employees from several departments and agencies.

Government has been reorganized; creating a new Department of Public Safety and Emergency Preparedness Canada, and new agencies such as the Canada Border Services Agency (CBSA). Reorganization will intensify information sharing among what were once separate entities.

Some have cited the *Privacy Act* as a barrier to sharing critical personal information. The *Privacy Act* does not need to be reformed, to facilitate information sharing—that is already possible. It needs to be reformed to counter the greater surveillance and the intensive transactional data collection we now see.

Privacy Act reform is not a new idea. Calls for reform date back to the late 1980s, long before the advent of today's surveillance and information technologies. Instead of strengthening the Act, the Government has weakened its provisions by measures such as those in the *Anti-terrorism Act*.

Integrating Information Systems

Even less visible has been the government's investment in integrated information systems that collect and analyze significant amounts of personal information about our travel patterns, financial transactions, and even in some cases the people with whom we associate. The systems analyze and mine the personal data in an attempt to find patterns that might suggest an individual is a security threat, a money launderer or is financing a terrorist group.

As law enforcement and national security agencies collect more information, from more sources, about more individuals, the probability increases that authorities will make decisions based on information of questionable accuracy or take information out of context. Misuse, misinterpretation or improper disclosures of personal information can have serious adverse consequences for individuals, families, and even communities.

The problem is aggravated when secrecy provisions and a lack of transparency prevent us from determining where the system broke down or why individuals were wrongly targeted.

Not surprisingly, the new "Smart Border" approach to border security has increased co-operation and information sharing with the United States. For example, both countries have created Integrated Border Enforcement Teams and Integrated Marine Enforcement Teams of law enforcement agencies to co-ordinate efforts to target cross-border criminal and terrorist activities.

Increasingly though, Canadians are concerned about information sharing with the United States, particularly given American federal departments' and agencies' lack of oversight on the collection, use and disclosure of personal information. In addition, the United States *Privacy Act of 1974* does not apply to foreign nationals, thereby depriving Canadians and citizens of other countries of certain privacy protections—including access and redress rights—under U.S. law. An EKOS Research Associates survey commissioned by our Office in March 2005, found 85 per cent of those surveyed reporting a moderate or high level of concern about Canadian government agencies transferring personal information to foreign governments to protect national security.

The Impact of the *USA PATRIOT Act*

These concerns have been highlighted by a provision in the *USA PATRIOT Act (*Section 215) that allows a special court to secretly issue an order requiring "the production of any tangible things", possibly including an individual's personal information, to the Federal Bureau of Investigation (FBI). The Act also prohibits anyone served with such a secret order from disclosing that they have complied with it, or even that it exists.

In 2004 the British Columbia Information and Privacy Commissioner, David Loukidelis, announced that he was examining whether "the *USA PATRIOT Act* permit[s] United States authorities to access personal information of British Columbians that is, through the outsourcing of public services, in the custody or under the control of USA-linked private sector service providers."

The B.C. Commissioner began the review following a proposal that a Canadian subsidiary of an American company take over administration of the province's Medical Services Plan and PharmaCare programs. Critics of the proposal argued

that that this could potentially allow American agencies such as the FBI to obtain personal information about Canadians from the American company under the *USA PATRIOT Act*.

In August 2004, we made a submission to the B.C. Commissioner entitled "Transferring Personal Information about Canadians Across Borders —Implications of the *USA PATRIOT Act*". The submission explained that a company holding personal information about Canadian residents in Canada would not be required to provide this information to a foreign government or agency in response to a court order, even if the company was a subsidiary of a company based in the foreign country. In fact, the company would violate *PIPEDA* if it did disclose the information without the individuals' consent. An exception would allow disclosures of information under legislation such as the 2001 amendments to the *Aeronautics Act* that allow airlines to disclose passenger information to foreign states.

PIPEDA provides further protection by requiring institutions that transfer personal information to a third party for processing to use "contractual or other means" to ensure that a company located in another country provides comparable protection of personal information to that provided in Canada.

However, our submission acknowledged that companies holding personal information about Canadians in a foreign country must comply with that country's laws and would have to disclose personal information in response to a court order. This means that a Canadian company outsourcing its personal information processing to the United States effectively exposes the information to U.S. law.

The B.C. government responded to the controversy by passing legislation amending the *Freedom of Information and Protection of Privacy Act (FOIPPA)* and nine other Acts. The legislation places restrictions on B.C. public bodies and service providers when storing, accessing or disclosing personal information outside Canada.

Of course, the B.C. legislation does nothing to protect the personal information that the federal government transfers outside the country, nor does *PIPEDA* apply. We urged the federal government to examine the circumstances under which it allows personal information about Canadians to be processed outside Canada and to explain the nature of these transfers to Canadians. The Commissioner observed that "Canadians need to understand the full extent to which their personal information is transferred across borders and the full extent to which personal information about them can be and is made available to foreign governments and institutions".

We followed up early in 2005 with 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.

The Canada Border Services Agency Audit

We also began planning an audit of the Canada Border Services Agency (CBSA) that will focus on its exchange of information with the United States. The audit's overall objective will be "to assess the extent to which the CBSA is adequately controlling and protecting the flow of Canadians' personal information to foreign governments or institutions thereof". A key element will be reporting and mapping, as much as practicable, what information about Canadians CBSA transmits to the United States and for what purposes.

The audit will examine several key operational systems CBSA uses to process the personal information collected and shared with U.S. counterparts. The audit will also assess the overall robustness of CBSA's privacy management as well as how it reports its privacy management responsibilities to Parliament and the public.

In closing, the Privacy Commissioner is not opposed to fighting terrorism and improving our security; we are not opposed to information sharing. However, we must ensure that the steps we take to enhance our security do not end up weakening the freedoms that define the society we are defending. We need well-designed laws, increased oversight and accountability — and effective checks and balances.

When we diminish our rights without enhancing security, no one wins. But enhancing security without eroding legitimate privacy rights — that's a win for all.

Privacy Act Reform

This section elaborates on the situation and explains some of the important things for the government to consider in updating the *Privacy Act*; something long overdue.

The privacy landscape is infinitely more complex today than it was a decade ago. Faced with increased globalization and extensive outsourcing of personal information processing and storage, Canada's *Privacy Act* lags woefully behind.

Today's commonplace information technologies—the Internet and new surveillance technologies such as digital video, linked networks, global positioning systems, black boxes in cars, genetic testing, biometric identifiers and radio frequency identification devices (RFIDs) —did not exist when the federal *Privacy Act* came into force in 1983. Characterizing the current Act as dated in coping with today's realities is an understatement — the Act is tantamount to a cart horse struggling to keep up with technologies approaching warp speed.

New technologies designed for, or capable of, surveillance of individuals are widespread and are used not only by law enforcement and national security agencies. Businesses, individuals—even your new car—are gathering personal data using surveillance cameras, spyware, infrared heat sensors and data mining, often without your knowledge or consent.

Personal information has become a lucrative commodity. Protecting that information particularly in the public sector is an ongoing challenge for privacy advocates — one that is exacerbated by a federal *Privacy Act* that contains no effective controls on the export of personal information.

How We Got Here

As early as the 1960s, Canadians began questioning the relationship between information, privacy and political power. They began to worry that our increasing use of computers could lead to loss of individuality or enforce conformity.

In 1971, in the face of growing concerns, the Departments of Justice and then-Communications struck a joint task-force to examine the social and legal implications of computer technology. Their study produced the watershed report *Privacy and Computers* whose recommendations led to embedding privacy rights in the *Canadian Human Rights Act* in 1978.

The current *Privacy Act* built on and strengthened those rights. It also reflects privacy guidelines adopted in 1980 by the Organization for Economic Co-operation and Development (OECD), of which Canada is a member.

Canada is a signatory to several international instruments that stress the seminal importance of privacy. The *Universal Declaration of Human Rights* and the *International Covenant on Civil and Political Rights*, both speak of the right to the protection of the law against arbitrary interference with privacy. Our own Supreme Court is gradually fleshing out a privacy right through the *Canadian Charter of Rights and Freedoms*. But faced with 21st century threats, the *Privacy Act* is now an outdated and often inadequate public sector data protection law.

It did not need to be this way. In 1987, three years after the *Privacy Act* took effect, Parliament conducted a required review and issued a comprehensive report recommending significant changes. Ten years later, another Parliamentary committee recommended a substantial overhaul. Repeated submissions and reports by Privacy Commissioners have flagged the toll technology is taking on Canadians' privacy rights.

The weaknesses are even more striking when the *Privacy Act* – a first generation data protection law – is measured against the new *Personal Information Protection and Electronic Documents Act (PIPEDA)*. In fact, several of the Office of the Privacy Commissioner's concerns could be remedied by adopting provisions similar to those in *PIPEDA*.

The New National Security Paradigm

As mentioned earlier in this report, the events of September 11, 2001 seem to have led to national security trumping all else. Of course, Canadians want to protect their own safety, as well as that of their allies. The risk—as always—is that vastly expanded surveillance systems will steadily erode our privacy (and other) rights, lower our reasonable expectation of privacy and autonomy, and ignore the critical question of where we must draw the line.

Both the *Anti-terrorism Act* and the *Public Safety Act, 2002* have established an atmosphere conducive to broader surveillance of both individuals and institutions. Much of the highly sensitive information about the lives of individuals, families and communities is stored in integrated information systems with broad access to law enforcement and security communities.

The cumulative impact of the new legislation is worrying. First, the surveillance powers of security and law enforcement agencies have been overly broadened. Second, the constraints on use of surveillance powers—including by the Court—have been unduly weakened. And finally, government accountability and transparency have been significantly reduced. We risk trying to defend our society by means that abrogate the fundamental freedoms that define it.

Transborder Data Flows

The *Privacy Act* must now grapple with a world in which "globalization" means not just international trade in goods; it also means an extensive traffic in personal information for off-shore processing and storage by both governments and the private sector. Effectively this moves the information out from under the umbrella of Canadian law and potentially into a legal vacuum.

As we noted above, there has been a steady increase in transfers of personal information from government to government, particularly since September 11, 2001, as well as from government to companies abroad. The *Privacy Act* imposes no obligations on third parties overseas which hold and process personal information about Canadians. There are now no Treasury Board policies governing government institutions on the issue, although some are being considered. While we applaud new policies, the *Privacy Act* should contain specific wording to define the responsibilities of those who transfer personal information outside the public sector and indeed, outside Canada.

Another implication of outsourcing is the exposure of Canadians' personal information to the reach of the *USA Patriot Act*, which we raised earlier in this report. Canadian and U.S. governments already have extensive information sharing agreements for law enforcement and security purposes, thus the impact on government records and transfers may be slight. However, a decision by a Canadian government institution or company to process and store customer data in the U.S. would now expose the information to U.S. agencies, effectively nullifying the protection provided by both the *Privacy Act* and *PIPEDA*.

Government On-Line or "E-Government"

The *Privacy Act* must also struggle with pressures from government agencies—and the public, it must be said—to deliver government services on-line. In fact, Canada has been remarkably successful. According to an annual survey of international government performance, by Accenture, a management consulting and technology services company, Canada ranked number one out of 22 countries for the fifth year in a row. Serving Canadians on-line is a government priority that promises less redundancy of information and better service to citizens.

However, the demands of e-government threaten the end of information silos which provide their own structural protection. Data silos may be antithetical to the concept of Government on-line or e-governments; there is no doubt that they are "less efficient". They duplicate information, and you can't get from one to another.

In contrast, government on-line may demand interoperable systems that pool personal information and make it available to more users for more purposes. The greater the amount of information, access, and number of users, the greater the vulnerability of the individuals to excessive government or bureaucratic surveillance.

Can we accept what amounts to a comprehensive personal file and still trust government not to misuse it—and, if so, how?

E-government may provide the critical push needed to make the *Privacy Act* a much more effective privacy framework. The Act must set out more stringent controls on access to the information pool. A better Act would also require greater justification for collecting information in the first place, one that needs to be clearly articulated. And a better Act would also demand a far stricter adherence to the principle that personal information be used only for the purposes for which it was collected.

E-government is upon us but the law is a long way behind. If government wants to become "the most connected to its citizens", it must also be more protective of its citizens.

Extending the Scope of the *Privacy Act*

More than age enfeebles the *Privacy Act*. Perhaps most critical is the law's function as a data protection statute, not a true privacy law. While not toothless, the best the law can manage in some circumstances is to "gum vigorously". The Act essentially is a set of checks and balances on government power. It establishes a set of "fair information practices" to regulate federal government collection, use and disclosure of individuals' personal data. And the law gives individuals the right of access to that information.

Expanding jurisdiction

As it is, there are gaps in the *Privacy Act*'s coverage: many institutions, including our own Office, are not subject to privacy law. Over the years, the federal government has created many entities that do not appear subject to either the *Privacy Act* or *PIPEDA*; they fall between the chairs. Such entities take the form of boards, tribunals, commissions, foundations, institutions, and corporations. They may operate as partnerships or joint ventures receiving funds from both the federal government and provincial governments. In our view, such a situation significantly weakens Parliament's control with regard to the protection of personal information. Starting in the next fiscal year, we have undertaken an audit to determine and confirm the full extent of the gap and to assess risks in more detail. So far, we count over 30 entities not clearly subject to privacy legislation.

And as government creates new institutions, a debate ensues on adding (or not) the new body to the schedule of those covered. Arguably, the process is clumsy and the right sufficiently vital in a democracy to warrant giving the *Privacy Act* primacy over any other Act of Parliament. Thus the law would apply to all federal institutions unless the enabling or other departmental legislation expressly declares that it applies notwithstanding the *Privacy Act*. A similar provision already appears in *PIPEDA*.

Protecting unrecorded information

Technology has effectively demonstrated that limiting the *Privacy Act's* application to personal information "recorded in any form" is well past its "best before" date.

The restrictive definition puts unrecorded information, such as from real-time electronic monitoring (live surveillance cameras) or from biological samples, beyond

the scope of the Act. Yet the technologies can yield intelligible information about identifiable individuals which should benefit from legal protection.

The proposal is workable; some provincial privacy laws and *PIPEDA* both apply to unrecorded information. For example, a security company in Northwest Territories and Nunavut mounted four security cameras on the roof of its building aimed at a main intersection in Yellowknife. For several days, 24 hours a day, staff monitored a live feed and reported a number of incidents to local police. The monitoring was intended to demonstrate the service and generate business for the company.

Although a public outcry quickly ended the demonstration, the Commissioner had the power to investigate and issue findings under *PIPEDA* which provides helpful guidance for other institutions. The Commissioner concluded that while monitoring public places may be appropriate for public safety reasons, there must be a demonstrable need, it must be done by lawful public authorities and done in ways that incorporate all legal privacy safeguards.

Extending access rights

Going global also means that Canadian government institutions now hold personal information about foreign nationals. For example, the CBSA collects Advance Passenger Information/Passenger Name Record of travellers entering Canada. The information includes name, date of birth, citizenship, passport or travel document number, reservation data and the traveller's itinerary. Airlines gather the information from passengers at the point of departure and send it to CBSA ahead of flight arrival.

However, under the *Privacy Act* only those present in Canada have the right to seek access to their personal information. This means overseas airline passengers, as well as immigration applicants, foreign student applicants, and countless other foreigners with information in Canadian government files, have no legal right to examine the information, to know how it is used or disclosed, or to complain to the Privacy Commissioner.

It is becoming increasingly difficult to justify hedging access rights in the face of international mobility and the ensuing exchange of personal data. Nor, in fact, does it appear balanced when other countries grant access rights to Canadians. For example, the European directive on privacy rights (with which 25 member states comply) grants access rights to "every data subject"—anyone whose information is held by a European entity.

The CBSA's collection of passenger information highlighted both the *Privacy Act's* shortcomings and the difficulties of ensuring even-handed treatment of the information. Although the CBSA has agreed "to administratively extend these rights to citizens who are not present in Canada", both the European Union's Working Group and the Privacy Commissioner would prefer that the law grant access to anyone.

Controlling data matching—effectively

Although government use of data matching (or "computer-matching") arguably poses the greatest threat to individuals' privacy, the *Privacy Act* is silent on the practice. Privacy Commissioners (bolstered by Parliamentary Committees) have all recognized the dangers inherent in excessive and unrelated data collection. All have recommended amending the *Privacy Act* to ensure that government institutions link personal records in discrete systems only when demonstrably necessary, and under the continued vigilant oversight of the Privacy Commissioner of Canada. The recommendations have not been followed through.

Granted not all improvements to the Act require legislative changes; administrative or policy directives often can fill the bill. But the Treasury Board issued guidelines in 1989 outlining the steps departments should take before matching data, including submitting a detailed proposal for the Privacy Commissioner's review. Given how few data matching proposals the Office of the Privacy Commissioner has received—and the likely extent of the practice—it is time to set out the obligations in law.

Limiting collection

Limiting collection is a fundamental principle of all data protection statutes. The *Privacy Act* requires government institutions to collect only personal information that is "directly related to" an operating program or activity authorized by Parliament. This gives government latitude to design programs with a defined set of personal information in mind. A more rigorous test would require institutions to demonstrate that the information is *necessary* for the program or activity.

Although the Treasury Board interprets the *Privacy Act* in this manner, Parliament should amend the law to put the matter beyond interpretation.

Government Transparency

The *Privacy Act* requires government institutions to inform individuals of the reason for collecting personal information. However, this response does not truly respect individuals' rights to control the collection, use and disclosure of their information.

A more meaningful explanation, and one more in keeping with modern data protection principles, should specify:

a) the authority under which the information is being collected;
b) the uses to which the information may be put;
c) the institutions with which the information may be shared;
d) whether the information is discretionary or mandatory;
e) the consequences of not providing the information; and
f) the individual's right to complain under the *Privacy Act*.

"Publicly available"

One exception to the *Privacy Act's* use and disclosure provisions is material that is "publicly available". This includes, for example, information available in public archives, libraries and museums. However, it also includes information contained in such public registries as the Bankruptcy Registry and the Lobbyist Registry. While there are good reasons for making these collections open to the public—transparency and accountability—few if any of the registries control the details they disclose or any subsequent uses made of the information. This has led to such abuses as bulk disclosures of personal information from the registries for marketing purposes.

Parliament should amend the *Privacy Act* to permit disclosures of personal information from these registries only in ways and for purposes consistent with the original purpose for establishing the registry.

Re-tooling the disclosure provisions

Perhaps the most evident demonstration of the weakness of the current *Privacy Act* in dealing with disclosures of personal information was provided by the Federal Court of Appeal in 2000 in the E-311 case (*Privacy Commissioner v. Attorney General of Canada*). The Court concluded that the disclosure provision in section 8(2)(b) of the *Privacy Act* enables Parliament to confer on any Minister (through a given statute) wide discretion to disclose information collected by the Minister's department.

The Privacy Commissioner argued that the *Privacy Act* required that the Minister disclose personal information only for the purpose for which it was collected, or for a use consistent with that purpose. However, the Court of Appeal found that section 8(2)(b) of the Act did not impose any such limitation. The Supreme Court "agreed substantially" the following year.

The *Privacy Act* also sets out in subsection 8(2) specific circumstances in which government institutions may disclose personal information without the individual's consent. Among these are disclosures to named investigative bodies, to Public Archives, to MPs to help constituents, to provincial and foreign governments, and for research and statistical purposes.

Some of these disclosures seem too permissive; for example, section 8(2)(f) authorizes disclosures under an agreement or arrangement between the Government of Canada and the government of a province or a foreign state. This provision needs to be much more specific as to the parameters of any such sharing and provide guidance on the kinds of contract provisions that are needed to safeguard privacy.

When Canadians share their information with the Canadian government at home or in consulates abroad, they do so with the expectation that this information will not generally make its way into the hands of foreign states. The current wording of section 8(2)(f) is broad and leaves much discretion to departments. There should be an obligation to thoroughly examine why the information is required by the foreign state, how it will be used, on what authority the request is made, and whether there are adequate safeguards to protect the information, including provisions protecting against secondary release. Pending reform of the *Privacy Act*, the Privacy Commissioner is actively encouraging government institutions to self-impose higher standards.

After more than 20 years overseeing the *Privacy Act's* administration, it is evident to us that the disclosure provisions need review and substantial revision.

Enabling the Privacy Commissioner

Moving from the pure "ombudsman" role

The *Privacy Act* gives the Privacy Commissioner of Canada the powers of an ombudsman, with no inherent powers of enforcement. The Privacy Commissioner can, however, go to Federal Court in certain circumstances. While the ombudsman model has been an effective one in avoiding an adversarial climate to encourage compliance, appeals to fairness and good sense are only as effective as the compliance they engender.

Models in several other jurisdictions, both in Canada and abroad, give the overseer the tools to compel respect for the law. Parliament may wish to review the merits of such powers for the Privacy Commissioner of Canada.

Conducting research and public education

For years, succeeding Privacy Commissioners have argued that the burgeoning threats to Canadians' privacy warrant an informed and effective voice for privacy. The Commissioner's Office needs both the power and the resources to conduct research and prepare reports on privacy issues, educate the public about their privacy rights, and evaluate the privacy implications of proposed legislation.

While Parliament heard the pleas during drafting of *PIPEDA*—and how valuable the tools have proven to be—the Commissioner has not been given the same mandate for public education under to the *Privacy Act*. The Commissioner should be equally empowered to sensitize business, government and the public under both laws.

Strengthening Court Review

Finally, complainants—and the Privacy Commissioner—may only seek a Court review of, and remedies for, denials of access to their personal information. Effectively this means that allegations of improper collection, use and disclosure may not be challenged before the Court, and the subsequent benefit of the Court's guidance on all government institutions is lost. Nor does the *Privacy Act* contemplate remedies for any damages caused by government actions.

Even when the Commissioner agrees that the complaint has merit, the Federal Court decided in March 2005 (in *Murdoch v. Canada (Royal Canadian Mounted Police))* that neither the Court nor the Privacy Commissioner has any powers beyond those set out in the *Privacy Act*.

Individuals, or the Commissioner acting on their behalf, should be able to ask the Court to review government collection, use and disclosure of personal information. As well, the Commissioner, in his or her capacity as complainant, should be allowed to apply to the Court for review of any matter to which the *Privacy Act* applies. And the Court should be empowered to assess damages against offending institutions.

Privacy Management Framework

Building a Privacy Management Framework for the Federal Government

What is a framework?

Generally management frameworks serve as blueprints to help an institution achieve a desired result. They establish goals and policies, and describe the systems, procedures and performance measurements needed to meet those goals. Properly constructed and applied, frameworks can be powerful instruments for showing institutions how best to conduct an activity, and how to marshal and allocate resources to achieve results.

While the concept is not new in management circles, applying it in the privacy context is. A government-wide model privacy management framework should be designed to help departments protect the personal information they control by identifying the inherent privacy risks, and how best to mitigate those risks.

OPC interest in privacy management frameworks

Our Office continually seeks improvements in the federal government's privacy management. We do so assuming that:

- The *Privacy Act*, (despite needed reform), should not inhibit improved privacy management;
- Improvements can be achieved through policy and guidelines; and

- Treasury Board Secretariat (TBS), as the locus for privacy policy, should ensure that federal departments and agencies meet high privacy management standards.

For example, in August 2004 our Office submitted a brief to the government on the implications of the *USA PATRIOT Act*. We suggested the federal government examine the circumstances under which it allows Canadians' personal information to be processed outside of Canada—and thus beyond the protection of the *Privacy Act*.

The Privacy Commissioner subsequently wrote to the President of Treasury Board requesting his support on this matter.

In response, TBS began reviewing the federal government's arrangements for outsourcing personal information. It also began developing model contractual clauses that departments could use to reduce the potential privacy risks to personal information being processed by U.S. companies or U.S. affiliates subject to the *USA PATRIOT Act*. This work is critically important and TBS expects to complete it shortly.

Our Office also suggested TBS review the federal government's data mining and assembly, re-examine the dated (1989) data matching policy, and strengthen the reporting requirements under the *Privacy Act*. These are also underway. We applaud the initiatives, as well as new privacy reporting requirements TBS issued in April 2005.

On the face of it the reporting guidelines indicate a desire for stronger privacy management. After new guidelines have had a chance to work, our Office intends on examining privacy reporting in some depth to determine which annual reports and statistical data are most effective in explaining privacy activity and issues, and supporting sound privacy management.

While each of these initiatives is significant, collectively they highlight the need for a more comprehensive and consistent approach to managing privacy in the federal government. A privacy management framework would help achieve this goal.

What makes a good privacy management framework?

First, TBS and departments—not our Office—are responsible for ensuring that an appropriate privacy management framework is in place. The design and implementation of frameworks need to be driven from within, not imposed externally. An external oversight body such as our Office certainly can, and should,

suggest the key attributes of an effective framework. We can also review and audit after the fact to determine whether a framework is working as intended. However, departmental ownership of the process is critical to its success.

The idea of privacy management frameworks appears to be gaining momentum in the federal government. The Assistant Deputy Minister Privacy Committee (chaired by TBS, the department of Justice and the Privy Council Office) has met periodically to promote a coherent and effective federal approach to privacy which includes developing an overall privacy framework and the sharing of best practices.

Some departments are already at work. For example, Human Resources and Skills Development Canada (HRSDC) presented their privacy management framework to the ADM Privacy Committee in June 2004. The department is a heavy user of personal data since it administers (among others) the Employment Insurance and Canada Student Loan programs. The framework aims to build trust with citizens by giving them more information about departmental programs and how they use and disclose individuals' personal information.

HRDSC defines the four pillars of their privacy management framework as:

- **strategic planning and governance**—conducting research and analysis to better understand citizens expectations on privacy, and defining the core privacy principles for their operations;

- **risk management**—establishing a review and approval protocol for privacy impact assessments, setting standards for personal information-sharing agreements and carrying out privacy reviews of research databases;

- **cultural change**—providing training for all managers, staff and contractors on personal information management, including specialized training on the requirements of specific programs; and

- **assuring compliance**—developing internal audit standards for managing personal information.

HRSDC found that adopting a privacy management framework provided the department a renewed impetus for improving their personal information management. The framework established a common platform both for defining better privacy practices, and helping it take the initiative in identifying and resolving issues. We applaud the department's leadership and commitment to fair information practices.

With a little help from Privacy Impact Assessments

Conducting privacy impact assessments (PIAs) provides another impetus for developing sound privacy management frameworks. Since May 2002, Treasury Board policy requires federal departments and agencies to conduct PIAs for all new programs or services that raise potential privacy issues. The assessments are designed to forecast potential privacy problems and identify options to mitigate risks before beginning a project.

The PIA policy is not only a key component of any good privacy management strategy; the policy itself promotes adopting a structure that is essentially a privacy management framework. The PIA policy guidelines, for example, require department heads to define the roles of their personnel in adhering to the requirements. Department heads must also assume responsibility for overseeing implementation–accountabilities that lie at the core of a privacy management framework. The policy also serves as an instrument for both promoting awareness of sound privacy practices, and measuring a department's compliance with privacy best practices.

The Treasury Board would be responsible for promulgating a model privacy management framework. A flexible approach should be taken in designing and applying a model. We recommend it possess the following attributes:

- Communicates effectively the importance of personal information management and the commitment to building privacy into program management;
- Sets clear objectives and standards on personal information gathering, quality, use, security, transmission, access, disclosure, retention and disposal;
- Clarifies the roles and responsibilities, and provides a basis for determining the resources and skills needed for achieving sound privacy management;
- Relies on sound risk management approaches, particularly through privacy impact assessments and/or threat risk assessments;
- Uses effective controls to support compliance and best practices—integrating best available privacy-enhancing technology, resolving disputes effectively, and identifying and correcting system weakness or privacy incidents; and
- Promotes accountability and continuous improvement through such means as reporting, audit and evaluation, education, and performance appraisals.

Since the concept is new, inevitably there will be some fine tuning—driven by experience and experimentation. In fact we are in the midst of a major audit that will allow us to test, refine and validate our approach. Once completed, we expect the audit will further substantiate the value of a privacy management framework.

Privacy is, in many respects, a risk management issue. Privacy management frameworks are of vital importance in helping federal institutions manage that risk. Accordingly, we recommend that the TBS develop a model framework to guide privacy management in federal departments and agencies.

We have discussed our recommendation for a model framework with TBS management. The President of the Treasury Board is committed to exploring the concept of a government-wide privacy management framework. We understand that TBS has begun examining both the scope and process for a project that should build on existing management frameworks. The project will require dedicated resources, cooperation among stakeholders (including our Office), effective communication with departments, and appropriate compliance mechanisms.

We welcome the initiative.

Complaints

Introduction

The *Privacy Act* has been in force since 1983, protecting individuals' personal information held by federal government departments and agencies. The Act governs those institutions' collection, use, disclosure, retention and disposal of the personal information they hold to administer government programs. Individuals also have the right to request access to and correction of their government-held personal information. The Act also sets out the duties, responsibilities and mandate of the Privacy Commissioner of Canada.

The Commissioner receives and investigates complaints from individuals who believe their *Privacy Act* rights have been violated. The Commissioner may initiate a complaint and investigate any situation where she has reasonable grounds to believe the Act has been violated.

The Privacy Commissioner of Canada 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. It is an offence under the Act to obstruct an investigation.

The Act does not grant the Commissioner order-making powers. Nevertheless, the Commissioner can and does recommend necessary changes to the information-handling practices of government institutions. The Commissioner may audit any federal department or agency at any time, and may recommend changes to any practices that are not in compliance with the *Privacy Act*.

The Commissioner is required to submit an Annual Report to Parliament, detailing the activities of the Office in the previous fiscal year. This report covers the period from April 1, 2004 to March 31, 2005 for the *Privacy Act*.

Investigations and Inquiries

Complaints Received

The Office received 1,577 complaints under the *Privacy Act* in 2004-05, down from 4,206 in 2003-04. While this is a significant decrease, the 2003-04 volume was an all-time high due to specific circumstances: almost 500 aboriginal Canadians filed complaints against a Health Canada consent form; and correctional officers, staff and inmates filed more than 2000 complaints against Correctional Service Canada. This year's volume is a return to a more normal year.

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 file 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.

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

Privacy:

- **Collection.** Personal information collected that 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[1]): 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, 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 Limit.** 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.

COMPLAINTS RECEIVED BY COMPLAINT TYPE

Received between April 1, 2004 and March 31, 2005

This table shows the number of complaints received by Complaint Type.

Complaint Type	Total	Percentage
Access	604	38%
Correction-Notation	29	2%
Language	2	0%
Collection	92	6%
Retention and Disposal	17	1%
Use and Disclosure	250	16%
Time Limits	489	31%
Extension Notice	90	6%
Correction-Time Limits	4	0%
Total	**1,577**	**100%**

TOP TEN DEPARTMENTS BY COMPLAINTS RECEIVED

Year ending March 31, 2005

This table represents the departments that received the greatest number of complaints in the reporting period.

It should be noted that this does not necessarily mean that these departments are exercising poor compliance with the *Privacy Act*. Rather, some of these departments because of their mandate hold a substantial amount of personal information about individuals and are therefore more likely to receive numerous requests for access to that information. A large amount of personal information increases the likelihood of complaints about the department's collection, use and disclosure, retention and disposal of personal information, and the manner in which it provides access to that information.

Institution	Total	Access	Time	Privacy
Correctional Service of Canada	395	162	84	149
Immigration and Refugee Board	222	96	126	0
Canada Revenue Agency	183	69	64	50
Royal Canadian Mounted Police	155	58	67	30
Citizenship and Immigration Canada	118	39	72	7
National Defence	72	25	34	13
Canada Post Corporation	60	32	1	27
Canadian Security Intelligence Service	49	46	2	1
National Research Council Canada	47	0	46	1
Justice Canada	32	14	17	1
Others	244	94	70	80
Total	**1,577**	**635**	**583**	**359**

COMPLAINTS RECEIVED BY RESPONDENT

Received between April 1, 2004 and March 31, 2005

This table shows the actual number of all of the complaints lodged against the various departments and agencies that were received in the reporting period.

Institution	Total
Agriculture and Agri-Food Canada	2
Atlantic Canada Opportunities Agency	1
Bank of Canada	1
Canada Border Services Agency	26
Canada Customs and Revenue Agency	6
Canada Post Corporation	60
Canada Revenue Agency	183
Canada School for Public Service	1
Canadian Firearms Centre	1
Canadian Food Inspection Agency	2
Canadian Human Rights Commission	3
Canadian Nuclear Safety Commission	1
Canadian Security Intelligence Service	49
Citizenship and Immigration Canada	118
Commission for Public Complaints Against the RCMP	3
Correctional Investigator Canada	2
Correctional Service Canada *	395
Elections Canada	1
Environment Canada	4
Farm Credit Canada	1
Financial Transactions and Reports Analysis Centre of Canada	1
Fisheries and Oceans	8
Foreign Affairs and International Trade Canada	24
Health Canada	27
Human Resources and Skills Development Canada	41
Immigration and Refugee Board **	222
Indian and Northern Affairs Canada	4
Industry Canada	3
Justice Canada, Department of	32
Military Police Complaints Commission	1
National Archives of Canada	3
National Capital Commission	5
National Defence	72
National Gallery of Canada	2
National Parole Board	10
National Research Council Canada	47

* CSC - A large portion of these complaints were submitted by Correctional Officers in the course of their labour relations negotiations with their employer.

** IRB - A significant portion of these complaints were submitted by one individual in the course of dealing with the IRB.

COMPLAINTS RECEIVED BY RESPONDENT (cont.)

Received between April 1, 2004 and March 31, 2005

This table shows the actual number of all of the complaints lodged against the various departments and agencies that were received in the reporting period.

Natural Resources Canada	8
Natural Sciences and Engineering Research Council of Canada	1
Office of the Chief Electoral Officer	11
Privy Council Office	1
Public Service Commission Canada	6
Public Service Human Resources Management Agency of Canada	1
Public Service Staff Relations Board	1
Public Works and Government Services Canada	3
Royal Canadian Mounted Police ***	155
Social Development Canada	18
Statistics Canada	1
Transport Canada	1
Veterans Affairs Canada	5
Western Economic Diversification Canada, Department of	3
Total	**1,577**

*** RCMP - A great number of these complaints are time related complaints since the RCMP was not able to respond to requests within the legislated time frames imposed by the *Act*.

Complaints Completed

We closed 2,407 complaints under the *Privacy Act*, over 800 more than our Office received in the year. However, almost 1,000 of those complaints were from one group of individuals–correctional officers requesting copies of their employee personnel files. Since many were similar, they required less work than would 1,000 unique complaints (once one complaint is concluded, the documentation serves as a model for many others). Nevertheless, the investigators accomplished a formidable task in closing so many cases, particularly since there were fewer staff than in previous years and investigators were diverted on a rotational basis to help the Inquiries Unit.

Despite closing more *Privacy Act* complaints than it received, the Office is carrying a significant number of ongoing cases—1,277 at fiscal year end. Resource levels were not sufficient to keep up with demand. Year end saw the final stages of a major Business Process Review of the Investigations and Inquiries Branch which was undertaken to streamline processes wherever possible, help establish appropriate resource levels, and solve our ever-growing aging caseloads.

Normally we would expect to close approximately 1,185 complaints with the allocated staff. With an annual intake in excess of 1,500, we are losing ground; the caseload is aging and by fiscal year-end 577 complaints remained unassigned due to lack of staff. We have limited open caseloads to 35 per investigator at a time. Some of the unassigned cases are now nearly a year old. Even older complaints being actively investigated take more time as the delay becomes a factor in finding documents and dealing with fading memories. The Branch's established standard of investigators completing 75 cases each year means that it would take approximately eight investigators one year to clear the unassigned cases alone.

Definitions of Findings 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*.

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.

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". This is a new type of disposition which the Office began using in April 2004.

COMPLAINT FINDINGS BY COMPLAINT TYPE

Closed between April 1, 2004 and March 31, 2005

This table clearly shows the total number of the various findings issued by the Office by complaint type in the reporting period.

	Discontinued	Early Resolution	Not well-founded	Resolved	Settled during investigation	Well-founded	Well-founded-Resolved	Total	Percentage
Access	44	22	1,170*	18	120	21	21	**1,416**	**59%**
Correction-Notation	1	0	5	0	3	0	0	**9**	**0%**
Language	1	0	0	1	0	0	0	**2**	**0%**
Collection	3	11	32	2	12	6	0	**66**	**3%**
Retention & Disposal	0	2	7	0	2	2	1	**14**	**1%**
Use & Disclosure	29	43	143	1	63	138	1	**418**	**17%**
Time Limits	15	9	42	0	5	361**	0	**432**	**18%**
Extension Notice	1	0	14	0	0	23	0	**38**	**2%**
Correction-Time Limits	1	0	0	0	0	11	0	**12**	**0%**
Total (# and %)	**95 (4%)**	**87 (4%)**	**1,413 (59%)**	**22 (1%)**	**205 (8%)**	**562 (23%)**	**23 (1%)**	**2,407**	**100%**

* As mentioned previously a large portion of the complaints determined to be not well-founded were submitted by the Correctional Officers in CSC who invoked the access provisions of the Act and its subsequent complaints mechanism in the course of their on-going labour dispute with CSC. In these cases CSC had decided to provide the Correctional Officers with their personal information by using a particular method of access to which the Correctional Officers objected. Our subsequent investigation of these complaints determined that CSC had the authority to choose the method of access and that it was compliant with the *Privacy Act* in doing so.

** A large number of time limit complaints were lodged against some departments that are facing significant resourcing problems. While we can sympathize, the *Privacy Act* simply does not provide this Office with any flexibility about refusing to investigate these complaints. Departments and agencies are required to respond to each and every privacy request and our role is to see that departments properly apply the *Privacy Act*. Having said this we are aware that some institutions are addressing their resourcing issues and commend them for dealing with their problem. We look forward to seeing the impact that these new resources will have on the number of complaints and will report on this issue in the next annual report.

COMPLETED COMPLAINTS BY ORIGIN

Closed between April 1, 2004 and March 31, 2005

This table shows the province of origin of the complaints investigated in the reporting period. It is to be noted that some complaints were received from some persons living outside of Canada.

Province/Territory	Total
Quebec	1,090*
Ontario	641*
British Columbia	274
NCR (ON)	106
Alberta	81
New Brunswick	59
Saskatchewan	40
NCR (QC)	39
Manitoba	34
Nova Scotia	17
Prince Edward Island	6
International	6
Newfoundland and Labrador	5
Northwest Territories	3
Nunavut	3
Yukon Territory	3
Total	**2,407**

* A significant portion of both these figures is attributable to the complaints lodged by the Correctional Officers in CSC.

COMPLETED COMPLAINTS AND RESULTS BY RESPONDENT

Closed between April 1, 2004 and March 31, 2005

This table shows the number of completed complaints by respondent and by finding.

Respondent	Discontinued	Early Resolution	Not well founded	Resolved	Settled during investigation	Well-founded	Well-founded Resolved	Total
Agriculture & Agri-food Canada	0	0	2	0	1	0	0	**3**
Auditor General of Canada, Office of the	0	0	1	0	0	0	0	**1**
Business Development Bank of Canada	0	0	0	0	1	0	0	**1**
Canada Border Services Agency	0	7	0	0	0	2	0	**9**
Canada Customs & Revenue Agency	28	2	56	3	28	16	3	**136**
Canada Mortgage & Housing Corporation	0	0	0	0	0	0	1	**1**
Canada Post Corporation	5	9	29	0	12	37	3	**95**
Canada Revenue Agency	2	11	41	3	2	26	0	**85**
Canadian Firearms Centre	1	1	0	0	0	0	0	**2**
Canadian Food Inspection Agency	0	1	0	0	1	1	0	**3**
Canadian Heritage	0	0	1	0	0	0	0	**1**
Canadian Human Rights Commission	0	0	0	1	0	1	0	**2**
Canadian Museum of Civilization	0	1	0	0	0	0	0	**1**
Canadian Security Intelligence Service	1	0	16	0	9	1	0	**27**
Canadian Space Agency	0	0	1	0	0	0	0	**1**
Canadian Tourism Commission	0	0	0	0	0	3	1	**4**
Citizenship & Immigration Canada	6	7	26	0	22	52	2	**115**
Commission for Public Complaints Against the RCMP	0	0	1	0	0	2	0	**3**
Correctional Investigator Canada	0	0	2	0	0	1	1	**4**
Correctional Service Canada	12	20	1,112 *	5	54	305	2	**1,510**
EDULINX Canada Corporation	0	1	0	0	0	0	0	**1**
Environment Canada	0	0	1	0	0	0	0	**1**
Finance Canada, Department of	0	0	0	0	0	0	1	**1**
Financial Transactions & Reports Analysis Centre of Canada	0	0	1	0	0	1	0	**2**
Fisheries & Oceans	0	0	4	0	0	0	1	**5**
Foreign Affairs & International Trade Canada	0	1	5	0	3	9	0	**18**
Health Canada	1	0	2	1	2	6	1	**13**

* This figure clearly shows that CSC had appropriately responded to the large number of access requests it had received from its Correctional Officers and that it was compliant with the requirements of the Act.

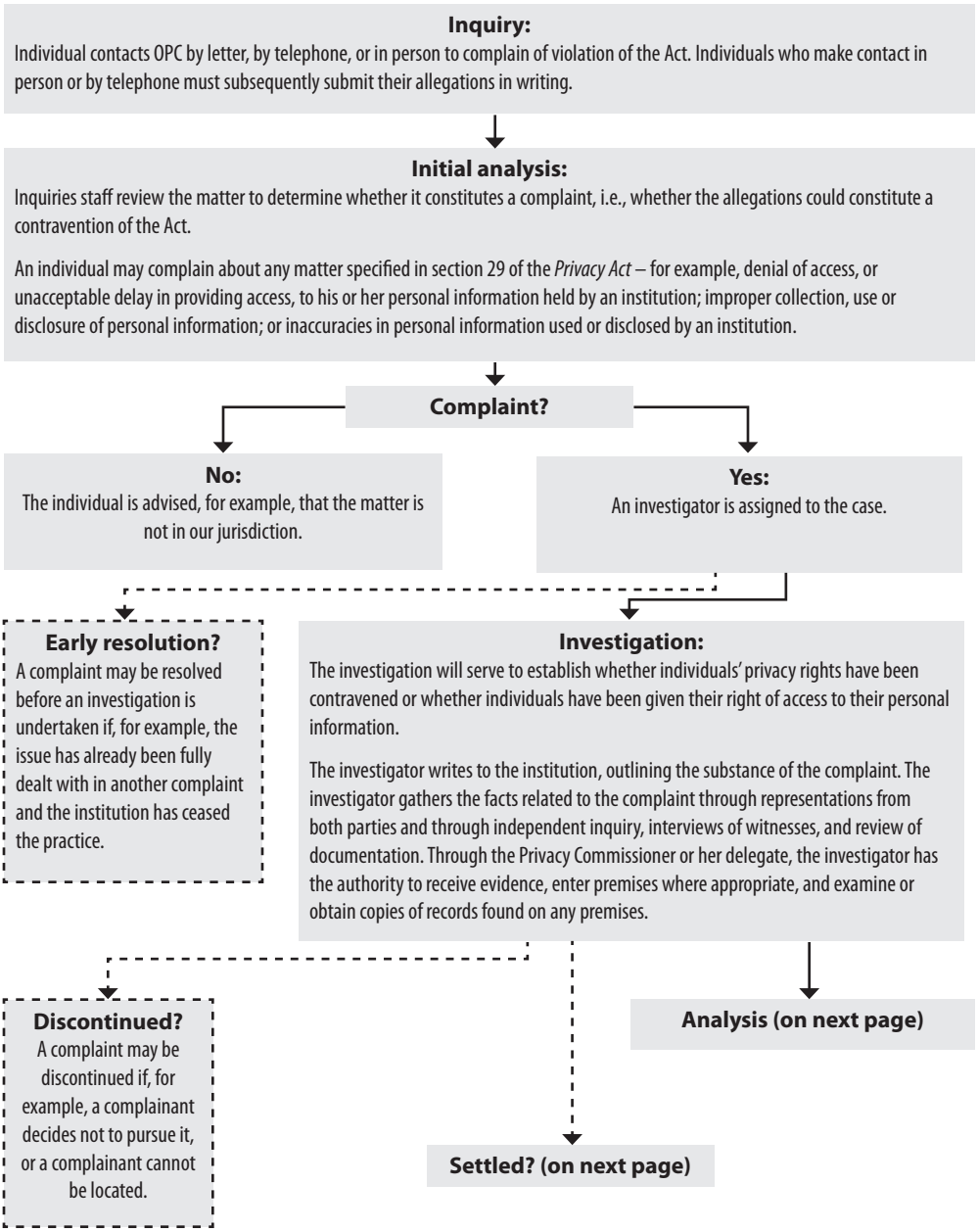
COMPLETED COMPLAINTS AND RESULTS BY RESPONDENT (cont.)

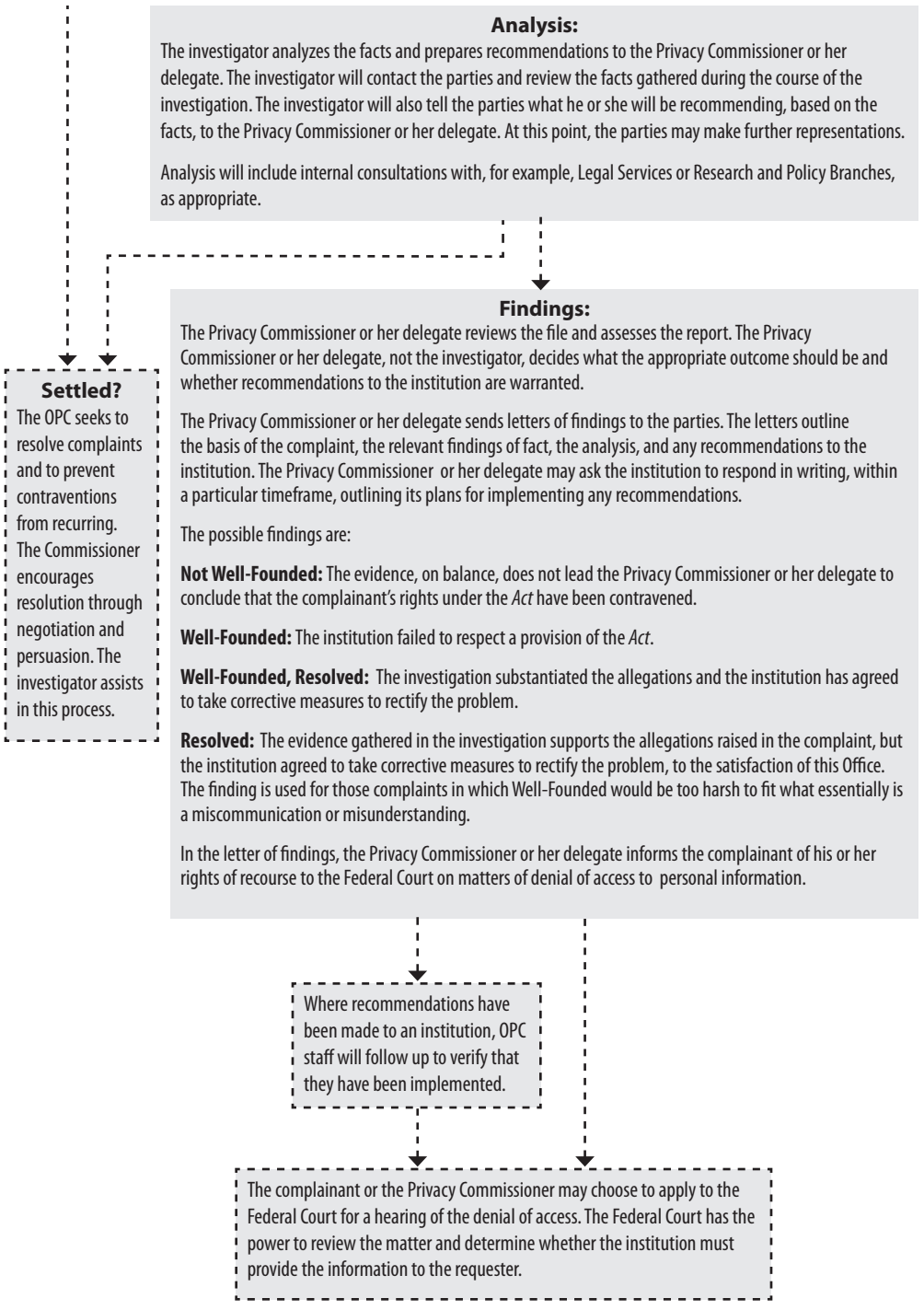
Closed between April 1, 2004 and March 31, 2005

This table shows the number of completed complaints by respondent and by finding.

Respondent	Discontinued	Early Resolution	Not well founded	Resolved	Settled during investigation	Well-founded	Well-founded Resolved	Total
Human Resources & Skills Development Canada	12	9	26	1	8	6	3	**65**
Immigration & Refugee Board	0	0	4	0	6	2	0	**12**
Indian & Northern Affairs Canada	0	1	0	0	5	0	0	**6**
Industry Canada	0	0	1	1	1	0	0	**3**
Justice Canada, Department of	1	2	3	1	3	7	0	**17**
National Archives of Canada	0	0	2	0	0	0	0	**2**
National Capital Commission	0	1	0	0	0	0	0	**1**
National Defence	5	4	10	4	15	33	0	**71**
National Gallery of Canada	0	0	0	0	1	0	0	**1**
National Parole Board	1	0	15	0	1	1	0	**18**
National Research Council Canada	0	0	0	0	1	0	0	**1**
Ombudsman National Defence & Canadian Forces	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	0	0	0	1	0	**1**
Public Service Commission Canada	0	1	3	0	0	0	0	**4**
Public Works & Government Services Canada	0	0	2	0	4	0	1	**7**
Royal Canadian Mint	0	0	1	0	0	0	0	**1**
Royal Canadian Mounted Police	15	5	33	1	19	43	1	**117**
Social Development Canada	0	0	1	0	3	2	0	**6**
Solicitor General Canada	0	0	0	0	0	2	0	**2**
Statistics Canada	1	1	2	0	0	0	0	**4**
Status of Women Canada	0	0	2	0	0	0	0	**2**
Transport Canada	0	1	4	1	2	2	1	**11**
Veterans Affairs Canada	1	1	3	0	0	0	0	**5**
Western Economic Diversification Canada, Department of	3	0	0	0	0	0	0	**3**
Total	**95**	**87**	**1,413**	**22**	**205**	**562**	**23**	**2,407**

Investigation Process under the *Privacy Act*





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

COMPLAINT INVESTIGATIONS TREATMENT TIMES - *PRIVACY ACT*

This table represents the average number of months it has taken to complete a complaint investigation by disposition, from the date the complaint is received to when a finding is made.

By Disposition

For the period between April 1, 2004 and March 31, 2005.

Disposition	Average Treatment Time in Months
Early Resolution	2.2
Well-Founded	6.1
Not Well-Founded	6.1
Discontinued	6.7
Settled in the Course of Investigation	10.1
Well-Founded, Resolved	11.5
Resolved	12.0
Overall Average	**6.4**

By Complaint Type

For the period between April 1, 2004 and March 31, 2005.

This table represents the average number of months it has taken to complete a complaint investigation by complaint type, from the date the complaint is received to when a finding is made.

Complaint Type	Average Treatment Time in Months
Correction/Notation Time Limit	4.1
Extension Notice	4.4
Time Limits	5.6
Access	6.3
Use and Disclosure	7.2
Collection	9.4
Retention and Disposal	10.0
Correction/Notation	10.7
Overall Average	**6.4**

Upon reviewing this table, one can see that the less complex complaints (Time Limits and Extension Notice) were completed in a shorter period of time than the more complex ones. This is reasonable since the more complex complaints usually require more on-site interviews, more in-depth research and analysis and, often times, lengthier negotiations with an institution regarding proposed corrective measures when there has been a breach of the Act.

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 cases described below have been selected for their educational value. They demonstrate the importance of correctly handling personal information and what can go wrong if this does not occur. It is hoped that they will encourage government institutions and agencies to be ever vigilant in handling personal information in accordance with the Act and to engage in ongoing staff education in that regard. At the same time, members of the general public may be prompted to ask questions about how their personal information is being handled by federal institutions and know that they can complain to this Office should something go wrong.

Outside psychologist's notes still "under control of" RCMP

An RCMP member, under investigation for allegedly uttering threats and unlawful use of a firearm, complained that the force denied her access to information gathered during its investigation. She did not receive a copy of a videotaped interview or the notes and psychometric data from interviews with a psychologist.

The privacy investigator determined that some of the information she sought in the videotaped interview with an RCMP investigator contained information about other people—an exemption under the *Privacy Act*. The force was able to remove these segments and provide her with the remaining information.

More problematic were the psychologist's records. The RCMP did not have copies of the material since the services were provided, not by a staff member, but by an outside professional on a fee for service basis. Pressed by the investigator, RCMP staff obtained some of the information but the psychologist refused to provide the psychometric data and what he termed his "personal notes" unless served with a court order. He argued that disclosing the material would breach his profession's ethical standards.

The RCMP's attempts at persuasion yielded nothing until the OPC wrote formally to the former Commissioner advising him that since the RCMP had hired the psychologist to assess the member, all the information prepared or created for the assessment was "under the control of" the RCMP for *Privacy Act* purposes. The psychologist eventually provided his notes, as well as the psychometric data which the RCMP sent to the complainant's doctor for explanation and interpretation.

Our Office concluded that the complainant eventually received the appropriate information but her complaint was well-founded. We reminded the RCMP that personal information collected on its behalf by outside experts is still under its control and thus subject to individuals' access. Contracts should make this clear.

Tax information disclosure narrower than it appears

A man complained that he was being forced to provide his province's drug insurance program with his income tax information before receiving the benefits.

This is a provincial drug insurance program providing financial assistance to residents who need help paying for prescription drugs. The program's level of assistance is tied to the family's net income—the less you earn, the more help you receive. Not surprisingly, the program verifies applicants' income by seeking their consent for the Canada Revenue Agency (CRA) to release their income information to the insurance program.

However, the consent form is very broad and appears to allow the program to see virtually all an individual's tax return. The privacy investigator followed up with CRA's Federal and Provincial Affairs Division. Staff explained that the breadth of the consent was dictated by the wording contained in the Memorandum of Understanding (MOU) with Ministry of Health. The key words in the consent form are "relevant to and solely for the purpose of determining, verifying and administering my level of benefit…"

To determine just what information meets those criteria, the privacy investigator examined the MOU and confirmed that CRA provides only three income amounts to the program: lines 236—Net Income; 303—Married Amount, and 5105—Net Income of Spouse as Reported Under GST Credit.

The complainant was satisfied with the investigator's findings and appreciative of the Office's efforts to determine how the program worked. He did not need any further action and the complaint was considered settled in the course of investigation.

Offender given caregiver's personal information

A woman complained that Correctional Service Canada (CSC) gave extensive personal information about her to an offender for whom she was caring.

The woman provides palliative care in her home to the elderly and those with special needs. CSC assessed the complainant to determine whether the home would be an appropriate facility in which to place offenders with special needs. CSC visited her home, conducted a full interview, prepared a Private Home Placement Report and approved the facility. The individual subsequently agreed to take in an offender whom the National Parole Board (NPB) had granted day parole. The offender needed placement in a facility capable of handling his extensive physical and mental conditions while also meeting the conditions of his parole. CSC considered him an unrepentant child molester and at danger of re-offending.

Once the offender was approved to move into the woman's care, he wrote to her saying that he had seen "your report from NPB" and that he understood her problems. The day after he moved into her home, he produced his address book in which he had written the names and telephone numbers of two of the woman's references to CSC. He also produced an entire copy of the Private Home Placement Report – a document the woman had never seen. The report included information about the woman's family members including information about her childhood, her marital history and current status, and educational and employment history.

The complainant was shaken by the offender's revelations and got in touch with local CSC parole officials. They agreed to her removing the report from the offender's room and blacking out her references' names and telephone numbers from his address book.

The investigation revealed that CSC officials originally intended releasing the offender to another facility but had to change plans. They then had to seek the NPB's approval to change the release destination. The offender's particular situation and his required level of care prompted Parole Board members to ask for more information about the private home placement. CSC provided the Placement Report to the Parole Board; it was then given to the board members who subsequently approved the change of

destination. The investigator was satisfied that the offender had not disclosed the information to anyone else.

At issue was whether CSC contravened the *Privacy Act* by giving the report to the offender. The *Corrections and Conditional Release Act* (*CCRA*) requires the Parole Board to share with the offender the information it uses to reach a decision about him or her. However, the information can be in the form of a summary or the "gist" of the information. The CCRA also allows the Parole Board to withhold "as much information as strictly necessary" (Section 144(4)) if the disclosure could jeopardize someone's safety, the security of a correctional institution, or the conduct of a lawful investigation.

It was evident from the investigation that only the Parole Board members who were deciding on the application had actually read the Placement Report. No-one else at the NPB had read the full report and so none knew the extent of the personal details it contained. The NPB contended that CSC was responsible for ensuring that information was lawfully shared with the offender. NPB officials were also adamant that the law's requirements would have been fully met had CSC given the offender only the "'gist" of the report. Unfortunately no one at CSC had read the report before giving it to the offender so they too were unaware of its contents.

The OPC found the case extremely disturbing, given the offender's history, the nature of the information in the report, and the fact that he was residing in her home. We understood that NPB and CSC officials were under time constraints to place the offender as quickly as possible and there was no malicious motive for the disclosure. Nevertheless, we found it disconcerting that the woman's personal information was disclosed simply because no one took the time to read the report. The disclosure should never have happened. The *Privacy Act* has been in force since 1983 and federal government employees are constantly reminded of their obligations to protect personal information.

Our Office concluded that CSC had seriously contravened the woman's confidentiality rights and that the complaint was well-founded. Unfortunately the *Privacy Act* provides no remedies or grounds for court review in the case of an improper disclosure of personal information.

The case has led to an agreement that CSC will no longer provide Placement Reports to the NPB.

Expired passports insufficient identification—for a passport

A man trying to renew his passport to attend a conference in Sweden questioned:

- Why he had to provide additional identifying information;
- Why an expired passport was not sufficient identification even though it was provided by a competent federal authority; and
- In what circumstances the Passport Office could refuse a document issued by a competent federal authority.

The complainant was opposed to providing a health card, firearms permit or driver's licence as proof of identity, arguing that Canadians are under no legal obligation to hold any of these documents and requiring any of them was both a violation of the Charter and the *Privacy Act*. The man also objected to providing his employer's address or that of any educational institution he attended in the past two years since either requirement would effectively preclude retired or unemployed persons from obtaining a passport.

Finally the man claimed that the Passport Office's demand for at least two references from people other than family members made it difficult for those, like himself, whose ill health or physical disability limits their contacts. He also argued that family members should not be automatically excluded as references.

The privacy investigator met Passport Office staff to review the requirements. The power to issue a passport comes from exercising Royal Prerogative not a particular law. The Passport Office (a Special Operating Agency of the Department of Foreign Affairs and International Trade), collects the passport information under the authority of an Order in Council *Canadian Passport Order* which gives the Minister the power to prescribe which forms will be used before issuing the passport. A third page was added to the application following September 11, 2001 to satisfy the department's concerns that the process was secure. The third page asks for addresses during the preceding two years, as well as for references.

Since a passport establishes the identity and citizenship of the bearer abroad, its validity is heavily dependent on the accuracy of the applicant's statements. Confirming the information with references who have known the applicant for at least two years helps substantiate its accuracy. However, applicants who cannot provide such references can complete form *PPT 132-Declaration in lieu of guarantor* and may also be able to name a family member in some circumstances.

The Passport Office confirmed that it cannot accept either an expired passport or Canadian birth certificate as supplementary identification because both were issued under less rigorous rules and can be forged. The office now demands the additional information to support the accuracy of the applicant's statements, and help avoid circulation of false passports. Applicants can use expired passports as proof of Canadian citizenship but not as a secondary piece of identification.

Our Office concluded that the Passport Office has the legal authority to collect the additional information to confirm the applicant's identity. The intent is not to impose draconian restrictions on applicants but to give the Passport Office confidence in the identity of the bearer and to help maintain the security of Canadian passports.

The complaint was considered not well-founded.

On-line security of taxpayers' information

A Chartered Accountant challenged the security of the Canada Revenue Agency (CRA)'s on-line system. She complained that the existing system could improperly disclose taxpayers' information. Individual taxpayers do not have to ask for on-line access—it is available by default. She argued that CRA has put the onus on taxpayers to protect their information. Instead it should require taxpayers wanting on-line service to register, and should then enhance the security requirements.

In October 2003 CRA introduced a program allowing taxpayers to access their 2001 and 2002 tax information via the "My Account" section of CRA's Web site at www.cra-arc.gc.ca. To gain access, taxpayers have to supply their Social Insurance Number, date of birth, amount of income reported on line 150, and their eight-digit access code from their Notice of Assessment. Taxpayers can block on-line access to their information by getting in touch with CRA's e-help desk at the toll free number provided.

CRA also protects the information with encryption technology and security procedures. Taxpayers wanting to use the service must first install a secure browser which requires the taxpayer to use a personally assigned password.

The accountant also pointed out that with the exception of the date of birth, all the information required for on-line access is printed on the Notice of Assessment. Since taxpayers are frequently asked to provide the notices as proof of income by lenders,

credit card providers, financial advisors and other institutions, anyone with a copy could access the taxpayer's file. The complainant had no evidence of any unauthorized access.

The OPC concluded that CRA's security measures are sufficient to protect taxpayers' information in the system and the complaint was not well-founded. Also the *Income Tax Act* requires CRA to provide taxpayers with a Notice of Assessment. Once taxpayers receive the notice, the onus is on them to protect the information.

Creating Travel Profiles for Public Servants

A government employee complained about the amount of personal information that Public Works and Government Services Canada (PWGSC) collects in the Traveller Profile form.

The federal government has completely reorganized its method of arranging employees' travel. It created a Government Travel Modernization Office which subsequently awarded a contract to Accenture to deliver all government travel services. Accenture then subcontracted credit cards and travel services to American Express.

Government employees must now make all travel arrangements through Travel AcXess Voyage. But they must first complete a Traveller Profile in order to obtain the required Travel Identification Number before making any travel arrangements. The profile is sent to the credit card company, which then issues the number.

The information required included employees' group and subgroup, level, travellers' home telephone numbers and home addresses, emergency contact names, and dates of birth. The investigator reviewed the form and met PWGSC staff to determine why employees had to provide each of the details. The investigator also reviewed a PWGSC document explaining why the information was required. Eventually, the department agreed to the investigator's request to remove the date of birth and make optional the requests for emergency contacts and home telephone numbers.

The complainant reviewed the revised Traveller Profile form and was pleased with the deletion of the date of birth, and the now-optional requests for other details. He was also happy with the department's explanation of how the information is safeguarded and agreed that the case could be considered settled during the investigation.

Buying gallery ticket not an invitation to ongoing marketing

An art lover who purchased a ticket to the National Gallery's Klimt exhibit was disconcerted when called on to support the Gallery's ongoing programs. Shortly after buying the Klimt ticket, the complainant received a call from the National Gallery Foundation asking whether she had enjoyed the exhibit. She ended the call.

Some time later, when a foundation volunteer called again to solicit her support, the woman asked how they knew about her visit and why she was on the call list. Since the volunteer did not know, she asked the gallery directly. They revealed that they routinely disclose ticket buyers' information to the foundation for fund raising.

The woman complained to the Privacy Commissioner that the disclosure was improper. The investigator confirmed that the gallery builds a database from ticket sales for membership drives and to promote upcoming exhibits. The gallery removed her name from the database and apologized for the calls. It will also seek express consent in future before adding ticket purchasers' names to the foundation's database.

The woman was satisfied with the resolution of her complaint, which the Office considers settled in the course of investigation.

E-mail system confounds sender, discloses safety worries

A Statistics Canada employee complained that his supervisor's e-mail branding him violent and a threat to others' safety was an improper use and disclosure of his personal information. The e-mails between the supervisor and a human resources officer were available to all staff on the agency's internal network for five weeks.

The complainant had filed a harassment complaint against his supervisor. The e-mails discussed the supervisor's concern that the employee could become violent if given copies of her and other employees' witness statements about the harassment complaint.

Statistics Canada investigated the complaint as a possible breach of both its internal security and privacy policies. The agency's e-mail system allows users to designate their e-mails as normal, personal, private or confidential; however, the Document

Management Centre (DMC), which administers and maintains the electronic communication systems, does not routinely capture the designation.

The disputed e-mail was sent through the DMC using the Agency Messaging Options which offers a "Complete Send" or, if senders select the "Options" function, two other possibilities. Senders can select an "Accessibility Option" which allows them to determine the message's level of security and distribution, or the "Access Restriction Option" which allows a "read only access". Senders can also tell the DMC what level of access they want. However, they will only be aware of these choices if they select the Options function at the outset.

The supervisor had attempted to classify her message by flagging it "Private" or "Confidential" through Microsoft Outlook. She had not understood that she also needed to flag it as "Protected" for the DMC. The DMC procedures require its classifiers to check the header information, analyze the contents, check the security level and verify with the sender if the security is unclear. The message is then sent to appropriate recipients.

Two factors contributed to the inappropriate disclosure; the supervisor's misunderstanding of the system's method of controlling access—disclosure was not intentional, and the DMC's failure to properly classify the message before putting it on the system.

Following the complaint investigation, Statistics Canada issued agency-wide instructions on assigning security levels to e-mails. The agency is also considering having DMC personnel staff review any Outlook e-mail that is flagged with security designations before putting them in the database. Longer term, StatsCan will review the DMC's workings and protocols on personal information and report progress to the Office.

The Office concluded that the complaint was well-founded but, given the work underway on the e-mail system, the Office need take no further action.

Incidents under the *Privacy Act*

Over and above individual complaints, incident investigations are conducted into matters of improper collection, use or disclosure of personal information that come to the attention of our Office from various sources including the media and directly from departments themselves. They often highlight a systemic issue, or an

unrecognized privacy breach that needs to be fixed as soon as possible. Last year, the Office completed 27 investigations into mismanagement of personal information. Of these, five incidents concerned individuals receiving someone else's information. All were determined to be isolated incidents and prompted renewed vigilance among government employees.

Two cases of interest are described below.

Gardener Finds Income Tax Information

Several incidents involved stolen information. For example, early in 2004 a Vancouver Parks Board gardener found a bag containing income tax information under the False Creek Bridge. The bag contained 12 bundles of taxation remittance slips from two financial institutions. The slips contained the name, address, payment amounts and account numbers of various individuals and businesses. Only two of the bundles had been opened but all the documents were wet and had been exposed to the elements for some time. This information had been processed directly by a private clearing house on contract to the two financial institutions. The bag is believed to have been stolen in transit from the financial institutions to the Canada Revenue Agency.

At the time of the theft, the agency determined that the stolen bag contained 1,600 remittance vouchers. While the majority of the vouchers concerned businesses, 390 were from individuals. Since the clearing house did not plan to contact any of the affected individuals, the Agency on its own initiative notified the clients of the theft so that they could take steps against identity theft. Our Office confirmed that clients had indeed been notified at the time of the theft so that they could take appropriate steps against identity theft. All information was apparently recovered and no individual privacy complaints were received relating to this theft. The Privacy Commissioner commends the Agency for its initiative in protecting the privacy of its clients, even though it was not responsible for this particular privacy breach.

Photos of CSC Employees Appear in CBC Story

A Correctional Officer of the Correctional Service Canada (CSC) reported that on November 16, 2004 he had seen a photograph of himself and some of his colleagues on a CBC Web site in a story entitled "*Ombudsman Looking into Abuse at Prison Unit*".

The CSC's Web site has a "Photofile" containing various photographs of penitentiaries, CSC office buildings, and correctional officers at work. The photos are intended to provide the media with photographs to illustrate news articles. Also on the CSC site and therefore publicly available is a CSC employee publication entitled *Let's Talk* which often contains photographs of employees at work.

In this case, the CBC was preparing a story on allegations that correctional officers were abusing inmates in the segregation unit at Kingston Penitentiary. The CBC obtained a group photograph of several correctional officers from the CSC site, which it used to illustrate its story about abuse in the segregation unit. Although the individuals had nothing to do with the unit, by using the photo in this context, the CBC left the impression that they did.

The CSC contacted the CBC which removed the offending photographs from its site. The CSC also removed the disputed photos from its "Photofile". It then examined each remaining photograph to ensure that the individuals signed proper waivers before it displayed the photos on the site. However, CSC recognized that the waivers would have to be updated to ensure that employees knew that once their photographs were on the Web site, they could be reproduced and used for purposes other than simple articles about CSC. The department conducted extensive internal discussions with management and legal services on employee consent. CSC also temporarily withdrew *Let's Talk* from the site until all the issues were resolved.

The "Photofile" is now on the CSC site but it no longer contains any photographs of individuals. *Let's Talk* has also returned to the CSC site but the photographs only depict people who have signed express consent/waiver forms.

Public Interest Disclosures under the *Privacy Act*

Paragraph 8(2)(m) of the *Privacy Act* gives heads of government institutions the discretion to disclose personal information without the individual's consent when the disclosure benefits the individual or when a compelling public interest outweighs

the invasion of the individual's privacy. The head of the institution is required (under subsection 8(5)), to notify the Privacy Commissioner of such disclosures, preferably in advance (unless some urgency dictates otherwise). The Office reviews the disclosures and, if deemed necessary, the Privacy Commissioner notifies the individual to whom the information relates. During the review process, the Office also advises institutions when it believes more personal information than is necessary to address the public interest is proposed for release. In this way, we minimize the intrusion into the individual's life.

Last year we reviewed 76 such notices, a large number of them in two categories. The first concerns disclosing the circumstances of death to family members. We received 24 notices of this type, the majority of which came from the CSC and National Defence.

The second significant volume – 21 – came from the RCMP and the CSC concerning individuals who were either unlawfully at large or being released from custody at the end of their sentences. All are considered at high risk to re-offend and therefore a danger to the community.

Another 11 notices dealt with disclosures to Parliamentary Committees, Boards of Inquiry or other public entities on matters such as the sponsorship program, possible misconduct by public servants, or the circumstances surrounding accidental deaths.

Also of interest were four notices from Health Canada concerning health risks to the public from individuals with communicable diseases, two notices to the Children's Aid Society concerning possible child abuse, and four notices of security threats.

Inquiries

The Inquiries Unit responds to requests for information from the public about the application of the *Privacy Act* as well as *PIPEDA*. In this reporting year the unit responded to almost 3,000 inquiries solely dealing with matters pertaining to the *Privacy Act* and responded to some 17,000 requests for information under *PIPEDA*. In the course of the year, staff shortages in the Inquiries Unit coupled with the ongoing heavy volume of work have presented challenges. As a result it was necessary to reassess the way we respond to public inquiries. We no longer accept or respond to inquiries or complaints by e-mail. We introduced an automated telephone system to answer the public's most frequently asked questions such as those about identity theft, telemarketing and, of course, the social insurance number. And we continue adding

information to our Web site to answer the most frequently asked questions. We also temporarily assigned some investigators to help the unit. Lastly, we now invite individuals to telephone during office hours since we can often determine a caller's needs faster and better in person than in a series of e-mails and letters.

INQUIRIES STATISTICS

(April 1, 2004 to March 31, 2005)

The following table represents the total number of *Privacy Act* inquiries responded by the Inquiries Unit.

Telephone inquiries	2,391
Written inquiries (letter, e-mail, fax)	585
Total inquiries received	2,976

Inquiries Response Times

Eighty per cent of inquiries were received by telephone. The majority of these were responded to immediately; the remainder which may have required research were responded to within one to two weeks.

Written inquiries accounted for 20 per cent of the workload and, on average, were responded to within three months. Providing written responses to inquiries may be time consuming and labour intensive. Over the year, the Inquiries Unit accrued a backlog of written inquiries which exacerbated the average monthly turn around times. In the next fiscal year, we plan to implement new measures and to obtain additional resources to respond more quickly to the public's queries.

Audit and Review

Strengthening the Audit Function

The *Privacy Act* empowers the Privacy Commissioner (in subsection 37[1]) to investigate some 150 government institutions' compliance with sections 4 to 8 of the Act. These sections set out federal government obligations when collecting, retaining, disposing of, and protecting personal information. The Act also authorizes the Commissioner to audit certain databanks that are exempt from individual access.

In March 2005 the Office re-named its compliance review branch Audit and Review. This signals an important change. The Office has not used its audit powers to their full potential in assessing the quality of privacy management, or addressing the risks inherent in current federal operations. In the past year we began rebuilding and re-enforcing the audit and review functions. We intend to make greater use of audits and they will become an important tool in carrying out our mandate pursuant to the *Privacy Act* and *PIPEDA*.

Our Office's goal is "to conduct independent and objective audit and review of personal information management systems for the purpose of promoting compliance with applicable legislation, policies and standards and improving privacy practices and accountability".

It will take time to build sufficient audit capacity, as well as meet departments' demand for timely reviews of privacy impact assessments as Treasury Board policy requires. In preparation, we have taken the following steps:

- Completed an external review of audit methods and practices;

- Set a branch goal and articulated team values;
- Began developing a longer term audit strategy and plan in view of privacy risks and issues;
- Built a business case to increase audit and review resources;
- Raised awareness with Parliamentary Committees on the potential of privacy auditing; and
- Improved audit practices as part of the audit of the CBSA (see below).

Auditing Cross-Border Flow of Personal Information

As mentioned earlier in this report, improving border security became a top priority for Canada and the United States following the events of September 11, 2001. A number of national security measures were instituted under the December 2001 Manley/Ridge Smart Border Declaration and 30-Point Action Plan.

Since then the government has allocated approximately $10B for national security programs and initiatives. Over $1.7B of that amount was given to the CBSA to implement measures aimed at strengthening land, marine, airport, and border crossing infrastructures; increasing the agency's human resource base; and improving its detection tools.

Canada and the U.S. also committed to enhancing border enforcement by exploring options for exchanging information and making better use of technology. The CBSA and the United States Department of Homeland Security (DHS) have worked on several initiatives that deploy technology and resources to better manage risk at the Canada-U.S. border. The initiatives include joint enforcement, joint-screening facilities, coordinated intelligence, and integrated databases to allow sharing of intelligence.

However, the Canadian public is concerned about the flow of personal information to the U.S. Media reports have indicated that Canadians are not willing to trade their privacy for measures which do not clearly enhance their security. This has been supported by an EKOS Research Associated survey commissioned by our Office, which indicates that 75 per cent of Canadians surveyed believe Canadian government agencies transfer citizens' personal information to foreign governments in order to protect national security, and with that 85 per cent of those surveyed reporting a moderate or high level of concern about such transfers.

Privacy and human rights advocates and Canadian politicians have all raised concerns about the implications of transferring personal data across international borders.

Among the concerns are data mining, racial profiling, direct access to databases by American authorities, secondary uses of information, matching data with private sector information, and the potential of the *USA PATRIOT Act* overriding Canadians' privacy rights.

Given this context, in July 2004 our Office notified the President of the CBSA that it intended to audit the Agency's management of the trans-border flows of personal information under its control.

The objective of the audit is "to assess the extent to which the CBSA is adequately controlling and protecting the flow of Canadians' personal information to foreign governments or institutions thereof". The audit will focus on exchanges of information between Canada and the U.S. A key element will be to map (to the extent practicable) the information about Canadians that the CBSA transmits to the U.S. and for what purpose.

We believe that national security objectives and sound personal information management practices are mutually dependent. Rigorous controls over the gathering and use of personal information will limit such privacy risks as improper uses or disclosures, and also support a robust national security objective. Relevant, timely and accurate information sharing is the life-blood of enforcement and intelligence operations. However, sharing must take place with the highest standards of privacy and security protection to prevent losing credibility with the public, Parliamentarians and foreign partners.

The general criteria guiding the audit are that collection, use and disclosure of personal information must be limited to that which is necessary and permissible by law. They should also be circumscribed by multiple layers of privacy and security protections during the life-cycle of the information so as to prevent and mitigate risks to personal privacy and program objectives.

The CBSA's customs and immigration enforcement programs require it to collect, use and disclose considerable sensitive personal information. The information might include financial, family history, health, and travel information; personal identifiers such as the social insurance number, immigration and passport numbers; and biometrics digital photographs, fingerprints and iris scans.

Due to the CBSA's size and complexity, our Office has spent most of its limited audit resources on determining which of the agency's many programs and information

management activities have the greatest impact on individuals' privacy. The Office will focus its audit on these areas.

To better understand the CBSA's business, the audit team has reviewed open source information, descriptions of CBSA programs and activities, internal policies on managing personal information, applicable training materials, information flow-charts, information sharing agreements, privacy impact assessments and IT system descriptions. The team interviewed selected personnel at headquarters and several regional operational units. We observed customs officers at the primary inspection line and secondary examination areas. The team was also briefed on the electronic systems used at land borders and airport terminals to assess whether a traveller or passenger poses a risk.

This phase of the audit was completed early in the 2005 fiscal year. Examination is began in May 2005 and an audit report completed by January 2006.

Other Audit and Review Activity

HRSDC databank reviews

Since 2001, our Office has reviewed about 60 data linkage proposals by Human Resources Development Canada (now Human Resources and Skills Development Canada–HRSDC and Social Development Canada–SDC). These reviews are mandatory under a *Governance Protocol* that came into force in 2000 following significant concerns about HRDC's Longitudinal Labour Force File (since dismantled). The protocol governs all future research involving data linkage.

The quality of data linking proposals submitted to our Office has increased significantly–to the point that we rarely find it necessary to give advice to HRSDC. The department has developed the internal capacity to identify and respond to privacy risks associated with data linkages for research and program evaluation. The *Governance Protocol* is a model we encourage other departments and agencies to adopt.

Accordingly, in March 2005 our Office wrote to both departments recommending that their review of data linkage proposals be made optional and at the departments' discretion. The departments adopted the recommendation and will make the necessary amendment to the *Governance Protocol*. We proposed the change on the understanding that the departments would maintain the integrity of structures and procedures. We also expect SDC and HRSDC to minimize any potential disruption on the internal review caused by the separation of their responsibilities. Finally, we

encourage personnel from both departments to share their knowledge and experience with colleagues from other departments and agencies. This should reinforce their capacity to assess the privacy impact of any form of data matching or linkage.

Given HRSDC and SDC's large and complex systems which contain extensive personal information, we expect to conduct a future audit to determine whether their privacy management frameworks are sustained and continue working effectively.

Data Matching

Under the Treasury Board Secretariat (TBS) of Canada's *Policy on Data Matching*, federal departments and agencies are required to notify the Office of any data matching proposal. The purpose is to afford the Office an opportunity to review and comment on such proposals.

Given the small number reported to us, our concern is not so much the data matching proposals that take place, but the risk of data matching that is unreported and/or not subject to assessment. Information obtained from TBS indicates that there is confusion among departments as to the meaning of data matching that may contribute to under reporting of such activity. TBS is now addressing the confusion. We share the concern and favour a clear and comprehensive definition that would capture the activity in various forms whether called data matching, linking or mining.

At the moment, it is not clear if the federal government has a handle on the extent of actual "data matching" of personal information, including activity carried out by third parties engaged under contract with the federal government, and whether they are in keeping with legislation, policy and good personal information management practices. We will continuing monitoring developments and consider the possibility of carrying out a future audit in this subject matter area.

Follow-up review of the Canadian Firearms Program

The Office first reviewed the Canadian Firearms Program in 2001. Since then, we have monitored developments (see pp. 49-50 of Annual Report 2003-04). As the result of ongoing negotiations to improve practices, last year we received a positive response from the-now Department of Public Safety and Emergency Preparedness Canada indicating that they had taken steps to address our concerns. These include better written agreements with contractors to protect personal information, limiting access to municipal and provincial police information retrieval systems to a need to know basis, reiterating that it will not disclose personal information to employers, and improving consent forms.

However, given the passage of four years, the controversy surrounding the program, and the many ensuing changes, including recent amendments to the *Firearms Act*, it is time to refresh our knowledge of the program in order to plan a new audit.

Privacy Impact Assessments

The Treasury Board of Canada requires federal departments and agencies to conduct Privacy Impact Assessments (PIAs) on all new government programs or services that raise privacy issues. Assessments are also required when departments substantially change existing programs and services so as to require new or increased collection, use or disclosure of personal information. Departments must also assess new data matching, contracting-out or other changes that may have privacy implications.

The Treasury Board PIA policy is critical to protecting privacy. And, despite their inconsistent quality and thoroughness, PIAs have improved considerably. The improvement trend continued last year. We are particularly pleased that departments are increasingly including action plans in their PIA submissions. This is an encouraging sign that the PIA policy is having its intended impact; ensuring that government adopts privacy as a core consideration in planning, designing, and implementing programs and services.

Implementing a strategy to meet the PIA policy's requirements is a key component of any departmental privacy management framework. The policy itself promotes adopting a privacy governance structure. For example, the policy guidelines establish the accountabilities that form the core of a privacy management framework. The guidelines expect departmental heads to define the roles of personnel on adhering to the policy's requirements. The departmental heads must also assume responsibility for overseeing implementing the requirements.

We continue encouraging departments to establish a formal administrative structure that will review departmental initiatives to determine whether they require a PIA. The structure or bodies should define responsibility for issuing departmental directives and guidelines on compliance with the policy's objectives, and establishing bodies to manage PIAs. The bodies would review proposals to determine whether assessments are required; oversee and coordinate their conduct, consult with relevant stakeholders, approve recommendations, and monitor implementation of the recommendations.

Departments should also consult Treasury Board Audit Guides, particularly the section in the PIA Audit Guide entitled "Management Control Framework", which outlines appropriate administrative structures to support the policy.

As part of our review of PIAs (as required by Treasury Board Policy) we routinely ask departments to report the actions they will take in response to our recommendations and we will assess compliance with the policy's requirements and objectives in any future audit.

Treasury Board scheduled a comprehensive review of the PIA policy in May 2007, five years after its official launch. However, the Board seized the initiative – conducting an interim review of a small sample of federal departments and programs in June 2004. This early start allows the Board to assess the impact on privacy compliance, and identify any potential improvements. The Board consulted relevant stakeholders (including our Office) during the review. We concur with most of the study's findings and recommendations.

The study concluded that the policy had indeed enhanced privacy compliance significantly in the selected departments. There are, understandably, several areas requiring attention. These include, for example:

- acquiring the expertise needed to conduct PIAs;
- coordinating and integrating the contributions of stakeholders;
- documenting observations with the necessary evidence;
- harmonizing PIAs with other government policies, such as the government's security, data matching, and social insurance number policies; and
- making PIA summaries publicly available.

The study also concluded that our Office's oversight and advisory role is critical to ensuring both the integrity of the assessment process and public confidence in the policy. However, our ability is compromised by a lack of resources. We welcome the study's acknowledgment of the need to provide adequate funding. The matter will form part of an overall business case for permanently funding our Office planned for submission to the Treasury Board later in 2005.

Treasury Board's study also found no single reliable source of information on how many assessments have been conducted. Nor is there a sufficiently complete mechanism in place for ensuring assessments is always conducted on initiatives that would warrant such analysis. Departments need to improve their monitoring and reporting, and their annual reports appear to be the appropriate method.

In April 2005 Treasury Board issued revised reporting guidelines for fiscal year 2004-2005 regarding annual reports on the *Access to Information Act* and the *Privacy Act*. We are pleased to see the guidelines now require departments to report on the number of PIAs and preliminary assessments conducted during a fiscal year.

Given indicated shortcomings, we are considering auditing the functioning of the whole PIA system. We are concerned that assessments are not being done when they should. And we need to determine whether systems and procedures are working to ensure departments follow through on the assessment findings as part of their privacy management program or framework.

In the Courts

Privacy Act Applications

Once 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 were filed in the past fiscal year:

1. Keith Maydak v. Solicitor General of Canada (Federal Court file No. T-972-04)
2. James R. Gairdner v. Jennifer Stoddart et al (Federal Court file No. T-2005-04) Discontinued February 2005

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. The Privacy Commissioner did not appear in court in any of these capacities in the past fiscal year.

The Privacy Commissioner can also become involved in applications where the complainant improperly names the Commissioner as a respondent and tries to seek relief against her that is not available. The following two such cases were decided in the fiscal year:

Gauthier v. Canada (Department of Justice) and Privacy Commissioner of Canada
Federal Court File No. T-653-02

Mr. Gauthier requested that the Department of Justice provide him with access to all personal information about himself. After consultations with a variety of other institutions, the Department provided him with a total of 685 pages of information and advised that some information had been withheld under sections 26 and 27 of the *Privacy Act*. Mr. Gauthier complained to the Privacy Commissioner that the Department was improperly withholding his personal information.

The former Privacy Commissioner reviewed the information which had been withheld and agreed that the section 26 and 27 exceptions had been properly applied and thus that the complaint was not well-founded. Nevertheless, the Commissioner asked Department of Justice to reconsider its exercise of discretion with respect to some of the information, upon which information was released to Mr. Gauthier.

Mr. Gauthier filed an application under s. 41 of the *Privacy Act* in which he asked improperly for, among other things, review of the findings of the Privacy Commissioner with regard to his complaint.

In October 2003, the Interim Privacy Commissioner filed representations regarding the lack of Court jurisdiction to review the findings of the Privacy Commissioner.

A hearing was held on March 31, 2004, at which time Mr. Gauthier conceded that he was not in fact seeking a review of the Privacy Commissioner's findings but only of the decision of the government institution to refuse to provide him with access to all his personal information. In a decision which reviewed the principles of solicitor-client privilege and determined that some of the information should have been released, the Application against the government was allowed in part on May 4, 2004.

Mamidie Keïta and Bernard Michaud v. The Minister of Citizenship and Immigration Canada and the Privacy Commissioner of Canada
Federal Court File No. T-676-03

The complainants had sought personal information in all Citizenship and Immigration Canada offices, especially embassies in Guinea, the Ivory Coast, Ghana and Senegal. Dissatisfied with the response from CIC, they lodged a complaint with the Privacy Commissioner, who investigated and concluded that the complaint was well-founded

at the time it was lodged. However, since CIC provided the complainants with the additional information to which they were entitled in the course of the investigation, the Privacy Commissioner considered the complaint resolved. The Commissioner agreed with CIC that the remaining information withheld from the complainants was third party information which was exempt under section 26 of the *Privacy Act*.

The complainants then filed for a Court review under section 41 of the *Privacy Act*. Since the application improperly named the Privacy Commissioner of Canada as a respondent, the Interim Privacy Commissioner filed a motion in July 2003 requesting that he be struck from the application. The Court dismissed the motion suggesting that the issue was overly complex in this case and best dealt with at trial.

The Application was dismissed on April 28, 2004, with the Court reiterating that the Applicants cannot, by means of a review application against the government institution, also obtain judicial review of the Commissioner's recommendations. The Court also confirmed that the section 26 exemptions were proper and that the Applicants had received all the personal information to which they were entitled.

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 *Privacy Act* Reform.

Brian Murdoch v. 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

Mr. Murdoch 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.

On June 18, 2004, Mr. Murdoch 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 Act has been contravened.

On June 29, 2004, the Privacy Commissioner filed an objection to Mr. Murdoch's request that she provide him a certified copy of all material and relevant documents in her possession. In August 2004 she moved to strike the application. However, the Court denied the motion in September 2004 noting that the merits of the Privacy Commissioner's argument (that she has no authority or jurisdiction to grant the remedies sought) could easily be determined when the Court heard the application.

At a hearing in March 2005 the Court determined that the Privacy Commissioner had fulfilled her obligations under the *Privacy Act* and had correctly advised the applicant that the Act provides no penalty to address the respondent's breach of his privacy. The applicant can obtain no further award in the Court for the improper disclosure.

Mr. Murdoch appealed the Federal Court decision in April 2005.

Public Education and Communications

The Office of the Privacy Commissioner of Canada is mandated specifically under *PIPEDA* to develop and conduct information programs to foster public and organizational understanding and recognition of the rules that govern the collection, use and disclosure of personal information. And although there is no legislative mandate for public education specified under the *Privacy Act*, there is certainly a mandate to ensure departments and agencies are held accountable for their personal information handling practices. There is often a necessity to inform the public, as well as departments and agencies, about the requirements of the Act and related policies, and the impact on the privacy rights of Canadians of current and proposed government activities.

In 2004-2005, the Office undertook a strategic communications planning effort with the expertise of external consultants, and the result was a comprehensive communications and outreach strategy for the coming fiscal years. This strategy will enable the Office to have a more comprehensive, proactive approach to communications planning and delivery; a more truly public education-focused approach to communications surrounding *PIPEDA*; and build a greater level of awareness of the Office and of key privacy issues under both laws.

In addition to developing this strategy the Office undertook the following communications activities in 2004-2005:

Speeches and Special Events

Speaking engagement opportunities have helped our Office raise awareness of privacy issues among diverse audiences and settings, including professional and industry associations, non-profit and advocacy groups and universities. In 2004-2005, the Commissioner, Assistant Commissioners and other senior officials delivered

21 speeches, speaking out about issues with privacy implications, such as security initiatives and health care delivery.

In March 2004, the Office began hosting an in-house Lecture Series (approximately one per month). These information sessions featured experts on a variety of privacy issues and brought together members of the privacy community and staff. In 2004-2005, the Office hosted nine of these information sessions.

Media Relations

Privacy issues continued to be of interest to the media in 2004-2005, with significant coverage in Canada on issues such as privacy and security, about which the Office received media calls and participated in interviews. In addition, through other proactive media relations efforts, such as the dissemination of news releases, the Office had the opportunity to raise awareness of, for example, the launch of its Contributions Program; the Commissioner's views on important legislation, such as the do-not-call list legislation; and the Office's views regarding transborder flows of personal information.

Web Site

We post new and useful information on our Web site on an ongoing basis. Fact sheets, news releases, speeches, case summaries of findings under *PIPEDA*, are posted to keep the site interesting to individuals and institutions. In 2004-2005, the Office redesigned its Web site in order to make it compliant with the Common Look and Feel standards established by Treasury Board. This resulted in an enhancement to the design as well as to the navigation tools on the site, in order to help visitors make better use of the site. The Office also made the site more dynamic with the posting of a downloadable Web-video for businesses on complying with *PIPEDA*. Since 2001-2002, we are pleased to report that visits to the site have more than quadrupled, reaching 904,886 in 2004-2005.

Publications

The Office has produced information materials, including guides for individuals and institutions on *PIPEDA*, as well as a variety of new fact sheets on issues including consent, use of the social insurance number in the private sector, transborder flow of personal information, and how our Office conducts investigations into potential privacy breaches.

In 2004-2005, in addition to preparing new fact sheets, we developed an e-kit for businesses to help them comply with the new law. We also revised the content of

our guides, to ensure they were up-to-date given the final stage of implementation of *PIPEDA* on January 1, 2004. We received requests for these materials on a daily basis. Not only were these materials sent to individuals upon request, they were also distributed at conferences and special events, and accessed in electronic format by visitors to our Web site. In 2004-2005, close to 22,000 of our publications (guides, fact sheets, annual reports, copies of both federal privacy laws) were sent out, in addition to the more than 635,000 publications which were downloaded from our Web site.

Internal Communications

Internal communications activities were also a focus of the Office and played a key role in 2004-2005, increasing transparency between management and staff, especially during its ongoing institutional renewal, but also through day-to-day activities. Internal communications activities in 2004-2005 involved providing staff with information on, for example, human resources issues, upcoming speaking engagements, Parliamentary appearances, senior management and labour management committee meetings, and special events such as all-staff meetings and information sessions. The Office has been developing an Intranet, an internal communications portal to host all internal communications and maximize staff access to information, which will be launched in 2005-2006.

In the upcoming year, the Office will continue to undertake the activities outlined above. We also hope to be in a position to initiate many of the more proactive public education activities outlined in the communications and outreach strategy.

Corporate Services

On the Path to Institutional Renewal

The Commissioner's most immediate priority has been to lead the Office's institutional renewal by strengthening OPC management processes, particularly human resources and financial management – planning, budgeting, reporting and control mechanisms.

Planning and Reporting

A foundation component of the Office's institutional renewal is a strategic planning, reporting and control process. During 2004-05 we completed our first year under this revised process. The strategic plan established at the beginning of the year was our road map for the year. As part of the new process were reporting and review opportunities. We made adjustments to plans and budgets throughout the year. To assist in our reporting and reviews we developed a Performance Measurement Framework and a monthly performance report. We also launched a Business Process Review of the entire institution which will enable the Office to better estimate resource requirements and to draft a business case for permanent funding.

Human Resources

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

We developed a number of Human Resource policies in consultation with central agencies and unions. These policies will guide us as we build on the successes of the past year and 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 new Strategic Human Resource Plan and Staffing Strategy, as well as an Employment Equity Action Plan, will help the OPC achieve its mandate and ensure the recruitment of a highly qualified workforce that is diversified and representative of Canadian society. As part of 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.

Over the course of the past fiscal year 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 values based staffing, language training sessions, performance management and employee appraisals and harassment in the workplace. The development and implementation of a Learning Strategy and Curriculum with the CSPS will enable staff to continue to develop the expertise and competencies required to fulfil their functions, as well as to position staff to take on new responsibilities and accountabilities.

We continued to work collaboratively with Central Agencies such as the Public Service Commission and the Public Service Human Resources Management Agency of Canada on follow-up measures to the recommendations of the Public Service Commission and the 2003 report of the Auditor General of Canada. This included 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 2003-2004 Financial Statements by the Office of the Auditor General of Canada. This is a significant milestone and a very positive indicator that the institution has indeed advanced on the path of institutional renewal. The institution has built on that success by establishing planning and review cycles, by streamlining and improving the financial management policies and practices.

Information Management / Information Technology

Signification advancements have also been made in how we manage our information assets. We completed an audit of our information management systems and we completed a vulnerability assessment of our information technology. We also completed an information technology strategy. This will help us to not only meet our obligations with respect to the management of government information and security policies, but

more importantly it will guide us as we move forward in improving on the management of our information assets. During the year we completed a significant upgrade to our case tracking and reporting system, Integrated Investigations Application (IIA). Finally we also established the framework for an internal Intranet site. This site will allow for effective communicating and sharing on information for employees.

Down the road

Strategic planning is an important annual exercise for the OPC. Our last session in January 2005 provided managers and employees an opportunity to re-examine the OPC's priorities for 2005-2006, and the actions they would take to achieve these priorities.

Corporate Services priorities for 2005-2006 are to:

- Develop and implement a Management Accountability Framework (MAF);
- Implement and maintain a human resource strategy that enables the Office to recruit, retain and develop staff and foster a continuous learning environment;
- Satisfy central agencies' requirements to regain delegated authorities, and enable the Office to take on new delegation to implement the Public Service Modernization Act;
- Develop and implement integrated information management;
- Complete Business Case for Resources for the OPC;
- Review Corporate Services Branch and Human Resources Branch policies and procedures; and
- Continue providing effective integrated financial services to the OPC.

Our Resource Needs

At the beginning of fiscal year 2004-2005, the Office's budget was $11.2 million, the same as the previous year. Included was $6.7 million for the Office's *PIPEDA* activities. Ongoing funding of OPC activities continues to be extremely important.

With privacy rights continually under threat, the Office's operations need to be funded adequately so that it is prepared to address the multitude of emerging privacy issues in the public and private sector.

The Office does not have adequate resources to fully exercise its powers and responsibilities under both Acts. Without adequate permanent funding, the Office cannot:

- Reinforce our audit and review functions to effectively address compliance under both privacy laws or strengthen our capacity to monitor, research and respond to emerging issues of technology and privacy;
- Conduct outreach and public education to influence change so policies and programs are viewed through a privacy lens;
- Continue investigating in a timely manner and resolving the growing number of complaints under both Acts; and
- Continue providing specialized legal and strategic advice and litigation support under both federal privacy laws, as well as strengthening established approaches and procedures to deal with cross-jurisdictional complaints.

To this end, the Office's priority beginning in the last quarter of fiscal year 2004-05 was to completely review all business processes. The review included establishing workload indicators and reviewing the legislative requirements, as well as external and internal factors that have an impact on our operations. This will enable the Office to develop a Business Case and make a formal submission to the Treasury Board Secretariat and to Parliament later in 2005 to stabilize our resource base and seek permanent funding for the Office.

We hope that with adequate permanent funding, the Office can further assure Parliament that it is effectively ensuring respect for Canadians' privacy rights in the public and private sectors.

Financial Information

April 1, 2004 to March 31, 2005

	Expenditure Totals ($)	% of Totals
Privacy Act	3,745,058	32
PIPEDA	6,849,650	58.5
Corporate Services	1,107,296	9.5
Total	11,702,004	100

Note: Although OPC salary budget allows for approximately 100 FTEs (full-time equivalents), there were only 86 FTEs staffed at the Office at the end of March 2005.

Detailed Expenditures[1]	*Privacy Act*	*PIPEDA*	Corporate Services	Total
Salaries	3,330,147	3,039,732	419,120	6,788,999
Employee Benefits Program	190,327	844,575	154,640	1,189,542
Transportation & Communication	41,238	266,129	81,282	388,649
Information	1,907	147,911	5,239	155,057
Professional Services	171,783	1,397,579	210,403	1,779,765
Rentals	2,730	107,874	23,759	134,363
Repairs & Maintenance	4,698	155,805	85,353	245,856
Materials & Supplies	9,304	50,764	21,633	81,701
Acquisition of Machinery & Equipment	384	451,788	98,026	550,198
Other Subsidies & Payments	- 7,460	20,084	7,841	20,465
Transfer Payments	0	367,409	0	367,409
Total	3,745,058	6,849,650	1,107,296	11,702,004

[1] Total expenditure figures are consistent with the Public Accounts of Canada.

Financial Statements

The Management Responsibility letter and the audited financial statements as at March 31, 2005 will be available on our Web site at www.privcom.gc.ca in October 2005.