Office of the
Privacy Commissioner
of Canada

Privacy

ANNUAL REPORT TO PARLIAMENT

2008-2009

Report on the *Privacy Act*

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. IP50-2009
ISBN 978-1-100-50240-3

Privacy Commissioner of Canada

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

November 2009

The Honourable Noël A. Kinsella, Senator
The Speaker
The Senate of Canada
Ottawa, Ontario K1A 0A4

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, 2008 to March 31, 2009. This tabling is done pursuant to section 38 of the *Privacy Act*.

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.priv.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.priv.gc.ca

November 2009

The Honourable Peter Milliken, M.P.
The Speaker
The House of Commons
Ottawa, Ontario K1A 0A6

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, 2008 to March 31, 2009. This tabling is done pursuant to section 38 of the *Privacy Act*.

Yours sincerely,

Original signed by

Jennifer Stoddart
Privacy Commissioner of Canada

TABLE OF CONTENTS

Message from the Commissioner 1

Key Accomplishments 5

Serving Canadians 5

Supporting Parliament 7

Supporting Federal Government Institutions 9

Advancing Knowledge 13

Positioning Canada as a World Leader in Privacy 15

Privacy by the Numbers 19

The Privacy Landscape 21

Integrating Privacy and Security after 9/11 23

Financial Transactions and Reports Analysis Centre of Canada Audit 26

Passenger Protect Program Audit 31

Privacy in a Connected World 43

Spotlight on Cases 46

Furthering Privacy Rights in Canada – A look at other key OPC activities 59

Audit and Review Work 59

In the Courts 65

Access to Information and Privacy 67

The Year Ahead 69

Appendix 1 73
Definitions of Complaint Types 73
Definitions of Findings and other Dispositions under the *Privacy Act* 74
Appendix 2 76
Investigation Process under the *Privacy Act* 76
Appendix 3 78
Inquiries, Complaints and Investigations under the *Privacy Act*
Inquiries Statistics 78
Complaints Received by Complaint Type 79
Top-10 Institutions by Complaints Received 79
Complaints Received by Institution 80
Complaints Received by Province/Territory 81
Disposition by Complaint Type 82
Disposition of Access and Privacy Complaints Closed 83
Disposition of Time Limits Complaints Closed 83
Disposition of Time Limits Complaints by Institution 84
Disposition of Access and Privacy Complaints by Institution 85
Treatment Times for Complaint Investigations under the *Privacy Act* 87
By Disposition 87
By Complaint Type 87

MESSAGE FROM THE COMMISSIONER

Not too long ago, a person went to a trust company to deposit a government cheque for under $300, and then withdrew the funds again as cash. Unremarkable as the transaction may seem, the trust company flagged it as suspicious and reported it to the powerful federal agency charged with protecting Canadians from money launderers and terrorist financiers.

Unbeknownst to the individual, there is now a lasting record of that trivial little transaction in the data vaults of the Government of Canada.

Without question, the government's efforts to keep us safe from terrorists and other criminals are imperative in this post-9/11 era. And, as a matter of course, a transfer of $300 would trigger no security alarms.

But, as the work of our Office over the past year has shown, the government's drive to secure the public's safety – enabled and abetted for the most part by technology – has led to a seemingly insatiable appetite for personal information about individuals.

The unprecedented scope of government data collection that we are witnessing today heightens the risk of misuses and unauthorized disclosure. The consequences for individuals can be grave.

As such, this report explores two of the most serious threats to privacy today. In two often intertwined themes, we report on the urgent need to integrate privacy protections into state security measures, and on the impact of information and communications technologies on the privacy of individuals.

The security chapter, which focuses largely on our audit work and privacy impact assessment reviews, warns of the dangers of unrestrained data collection. The technology chapter, highlighting our investigation efforts, underscores the new challenges in safeguarding the personal information of Canadians.

Our main message is that privacy rights need not be at odds, either with public security or with the use of information technology. On the contrary: We contend that measures to respect privacy must be integral to these new developments.

Integrating Privacy and Security

Specifically, we report here on our in-depth audit of FINTRAC, the federal government's Financial Transactions and Reports Analysis Centre of Canada, which found that the agency receives personal information beyond its legislative authority.

FINTRAC could oblige as many as 300,000 financial services entities, realtors, accountants, casino operators, precious metals dealers and others to scrutinize and report on the monetary transactions of clients. Failure to report suspicious activity can result in fines of up to $2 million and jail terms of up to five years – two powerful incentives to comply.

Also included in this annual report is our audit of the federal Passenger Protect Program and its cornerstone "no-fly list." Individuals placed on the list, properly known as the "specified persons list," are designated as risks to aviation security and face heightened state scrutiny and grave restrictions on their right to travel. To our surprise, we found that Transport Canada officials were not giving the deputy minister all the information necessary to decide whether a person should be added to or removed from the list.

Privacy in a Connected World

As we discuss in another chapter, it is often technology – that miraculous solution to so many of our problems – that creates new privacy challenges of an unprecedented scope and magnitude.

A hacker using off-the-shelf software, for example, was able to penetrate a computer at Agriculture and Agri-Food Canada, exposing about 60,000 personal data records of farmers using a federal loan guarantee program.

We also found that, for inexplicable reasons, more than 1,200 employees at the Department of Foreign Affairs and International Trade had access to a database containing confidential personal information about a citizen jailed abroad.

On the other hand, many of the 990 public complaints we handled last year revealed that, 26 years after the passage of the *Privacy Act*, too many data breaches can still be traced back to decidedly low-tech origins.

In one case, for instance, a toxic brew of faulty procedures, inadequate staff training and loose lips meant a personal and politically sensitive letter was not secured against unauthorized access, eventually winding up in the hands of a reporter.

Cause for Optimism

Even so, as I look back on the past fiscal year, I am pleased to report on some gratifying progress.

Our work on many fronts is making a difference. Our complaint investigation process helps us identity shortcomings in departments' privacy systems, and to recommend changes to forestall future problems.

We are able to point out important privacy risks through our audits of existing programs and our reviews of Privacy Impact Assessments of proposed new initiatives. For the most part, we find that our recommendations are adopted by the organizations we work with.

While it is inevitable that there will sometimes be differences of opinion about how to approach certain issues, we are heartened by the fact that the vast majority of the federal public servants we work with across the government *do* take privacy issues very seriously.

As Canada's privacy guardian, it is our job to raise red flags when we see problems – and we do occasionally find serious ones. However, we do this mindful of the fact that, for the most part, Canadians should be satisfied with the way the federal government handles their personal information.

New Leadership

This past year also saw the appointment of Chantal Bernier as Assistant Commissioner responsible for the *Privacy Act*. Her wealth of experience at senior levels in the federal public service has greatly strengthened our efforts to promote effective privacy management practices within the Government of Canada.

Having served most recently as Assistant Deputy Minister, Community Safety and Partnerships Branch at Public Safety Canada, Ms. Bernier brings to the Office her in-depth knowledge and understanding of some of the key challenges we face.

We welcomed Ms. Bernier on Dec. 8, 2008, and have benefited greatly from her insight and expertise. In light of the privacy challenges facing Canada in the years ahead, we will continue to count on her leadership.

The Challenges Ahead

With the 2010 Winter Olympic and Paralympic Games just around the corner, for instance, the challenge of integrating privacy into security measures will come to a head in an unprecedented way. We have already engaged security officials in a constructive dialogue to build privacy considerations into their security measures.

Other challenges ahead include a review of the Privacy Impact Assessment of the Canadian Air Transport Security Authority's recommendation to begin using airport scanners that penetrate clothing in order to search for hidden weapons.

We will also be taking a close look at Citizenship and Immigration Canada's plans to roll out initiatives involving the use of biometrics, including biometric-based visas for foreign nationals.

And we will continue to monitor the government's efforts to push forward legislation that would require wireless, Internet and other telecommunications companies to make subscriber data available to authorities, even without a warrant.

Next year's report will reflect back on developments in these emerging areas. But, even now as we pause to submit this year's report to Parliament and the people of Canada, it is instructive to recall the words of the first Privacy Commissioner, John Grace, writing in the inaugural annual report for 1983-1984.

With the digital age still in its infancy and the electronic networking enabled by the Internet still several years away, the report raised prescient concerns about government surveillance and the power of computers to surreptitiously mine and match data on individuals.

"What kind of Privacy Commissioner would remain silent in the face of the threat to a citizen's privacy rights posed by the technique of linking computer files?" the report demanded. "The *Privacy Act* is a testimony that Parliament does not want Canadians to be supervised by computers, specifically by government computers, and does not want government trafficking in personal information."

At a time of often dizzying change, it is comforting to remember that some truths remain immutable.

KEY ACCOMPLISHMENTS

SERVING CANADIANS

Inquiries and Investigations

One of the most important ways in which we serve Canadians is by answering their questions about privacy issues.

Our Inquiries Unit dealt with 1,770 calls and 1,333 pieces of written correspondence related to issues that we could pin directly to the *Privacy Act*. In addition, we handled another 2,488 inquiries on privacy-related matters that could not be linked exclusively to the *Privacy Act* or our private-sector privacy law, the *Personal Information and Electronic Documents Act* (PIPEDA).

Although people's reasons for contacting us were many and varied, certain concerns predominated. For example, many people were looking for help in making formal requests for access to their personal information or to file a complaint with a government institution. Also common were inquiries about perceived breaches of privacy.

We also help Canadians by investigating their complaints about privacy problems. We received 748 formal, written complaints last year, down only slightly from the 759 complaints logged in 2007-2008. The lion's share – 60 percent – came from residents of Quebec or Ontario.

As in previous years, the most common complaints to our Office related to access to personal information, and to the length of time that government departments and agencies were taking to respond to access requests.

Not surprisingly, departments that collect and hold the largest amounts of personal information also attracted the most complaints, including Correctional Service of Canada, Human Resources and Skills Development Canada, the Royal Canadian Mounted Police (RCMP), and the Canada Revenue Agency.

Because of a concerted effort to clear up a growing backlog of investigation cases, we were able to close 990 complaint files last year, up 13 percent from the year before.

There are various outcomes to investigations. For instance, we may find ways to resolve the cases early, or to settle them in the course of the investigation. In some instances, the complainant chooses to discontinue the process. In all, one-third (32 percent) of cases were closed before investigative findings were issued.

Where the investigation continued to completion and findings were ultimately made, we determined that 342, or 35 percent of the 990 cases, had not been well-founded. However, in 327 cases, (33 percent) the complainants' allegations were substantiated with findings of well-founded (24 percent of all cases), resolved (two percent), or well-founded and resolved (seven percent).

More than half (53 percent) of all closed investigations related to complaints from people who had been denied access to the personal information they were seeking.

However, only 70 (13 percent) of those 525 access complaints were determined to be well-founded or well-founded and resolved.

In the end, the majority of complainants accepted that they could not receive the documents they were seeking because of statutory exemptions that had been properly applied. For example, the *Privacy Act* allows the head of a department to refuse to disclose personal information when doing so could be harmful to international affairs or the defence of Canada or where the information was collected during a criminal investigation. As well, the *Privacy Act* does not allow for the release of the personal information of other people without their consent.

The 213 complaints about the time it took for government institutions to respond to requests for personal information were the second most common class of cases we handled. Nearly 80 percent of the time-limit complaints (169 of 213) were determined to be well-founded because complainants typically only come to us after the statutory deadline for their complaint has passed. This suggests that delays in providing citizens with access to their personal information continues to be a challenge.

Please refer to Appendix 1 for detailed statistics related to our inquiries and investigation work.

Cases involving the collection, use, disclosure, retention or disposal of personal information accounted for a combined 229 (23 percent) of the 990 complaints we

investigated. Of those 229, 61, or only 27 percent, were determined to be well-founded, or well-founded and resolved.

Public Awareness Efforts

Our Office does not have an explicit public education mandate under the *Privacy Act* in the same way it does under the *Personal Information Protection and Electronic Documents Act* (PIPEDA). Therefore, the bulk of our communication with Canadians about public-sector privacy issues tends to occur through more formal channels, such as speeches and this report to Parliament.

Still, in 2008-2009, we did publish a new guide entitled *Safeguarding Your Personal Information: An Overview of Privacy Protections in the Federal Government*. The bilingual publication, available in print and on our recently updated website, is a citizens' guide to the *Privacy Act* and the complaints process.

The document also touches on important contributions that our Office makes to the preservation of privacy within the federal public sector by, for example, explaining the Privacy Impact Assessment process.

A separate publication we published last fiscal year, titled *Psst!...A Word in Private?*, describes the work of our Office through our statutory framework and other initiatives.

In addition, we did proactive media relations work such as audio news releases offering recorded comments to radio stations aimed at increasing Canadians' knowledge of personal information handling practices in the federal government. We also had the opportunity to speak with federal public servants at meetings and conferences.

SUPPORTING PARLIAMENT

One of our main duties as an Officer of Parliament is to support the work of Parliamentarians by reviewing proposed legislation, appearing before Parliamentary committees and speaking with MPs and Senators.

Reviewing Draft Legislation

The Senate and House of Commons often called on our Office to engage in the legislative process during 2008-2009.

For instance, we were asked by the Senate to consider the privacy implications of Bill S-2, which would expand search powers within airport security zones. In light of our

work on assessing privacy risks arising from traveller screening and facilities security, we were more than happy to discuss the issue with the Senate Standing Committee on National Security and Defence.

MPs and Senators, meanwhile, asked us to address Bill C-11, the *Human Pathogens and Toxins Act*, which would regulate laboratories in Canada that use domestically acquired human pathogens and toxins. Our recommendations to the House of Commons Standing Committee on Health and the Senate Standing Committee on Social Affairs, Science and Technology focused on safeguards needed to protect personal information.

We also provided comments to Health Canada on Bill C-6, the *Canada Consumer Product Safety Act*, which is aimed at allowing the government to work with industry to identify and assess safety risks, develop standards and share best practices.

Renewing the Privacy Act

Reform of the *Privacy Act* has been a perennial concern for this Office, and continued to be a major thrust of our Parliamentary activities during 2008-2009. We made two appearances on the issue before the House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI).

Enacted in 1983, the legislation came into force when telex machines and typewriters still dominated government offices. Progressive for its time in the manner in which it sought to ensure privacy protection, it is now a statute showing its age.

We were pleased that the ETHI Committee built on our representations by calling in other experts from across government and outside. Then, shortly after the end of this reporting period, the Committee agreed in a report that a complete overhaul of the *Privacy Act* is warranted to better protect the privacy rights of Canadians in their dealings with the federal government.

In *The* Privacy Act*: First Steps Towards Renewal,* tabled June 12, 2009, the Committee expressed unequivocal support for half of the 12 "quick fix" changes that our Office has advocated to address some of the most pressing shortcomings of the Act, while calling for further discussion on several more.

As this report went to press, our Office was urging Parliament to build on the all-party consensus expressed in the report and to address several outstanding concerns.

Other Parliamentary Committee Appearances

Apart from our work on *Privacy Act* reform, the Commissioner in 2008 appeared before the ETHI Committee on Main Estimates, the annual review of our Office's budget by Parliament, and before the House of Commons Standing Committee on Health on the privacy implications of post-market tracking of adverse drug effects.

In the first three months of 2009, the Office appeared before the House of Commons Standing Committee on Public Safety and National Security, as MPs undertook the statutory five-year review of the *DNA Identification Act*. We took advantage of this important opportunity to elaborate on our long-standing concerns over the privacy implications of genetic information and biobanks.

We also appeared before the Senate Standing Committee on National Security and Defence to discuss amendments to the *Customs Act* that would broaden the search powers of security personnel at airports.

Other Interactions with Parliamentarians

An important part of our Office's policy work is providing advice to Parliamentarians outside the formal committee structure. The privacy concerns of individual Canadians are often expressed in letters to their local Members of Parliament, and the Commissioner's views are frequently sought on specific constituent issues.

In phone calls, letters or meetings, our Office aims to provide all Parliamentarians and their support staff with useful guidance or referrals on privacy issues.

In 2008-2009, for example, our Parliamentary Affairs desk dealt with a wide range of issues, including transborder data flows and the privacy impacts of outsourcing, concerns about surreptitious recording of political meetings, the ability of the general public to request access to their own credit reports and scores, and the then-new Do Not Call List, which allows consumers to opt out of receiving telemarketing calls.

We have commissioned research on the issue of the use of voters' personal information by political parties. We look forward to discussing this issue with Parliamentarians after the report is completed in late 2009.

SUPPORTING FEDERAL GOVERNMENT INSTITUTIONS

Beyond the Parliamentary precinct, our Office works with federal departments and agencies to ensure adherence to the spirit and the letter of the *Privacy Act* within the Government of Canada.

And, because an ounce of prevention always outweighs a pound of cure, much of our efforts are geared toward the front end – ensuring through outreach, consultation and collaboration that privacy implications are taken into account from the very start of the policy-development process.

This approach has the benefit of strengthening the protection of personal information across systems as they are built, and ideally forestalls unnecessary privacy risks.

Policy Development and Privacy Consultations

Some federal organizations, such as the RCMP, the Canada Border Services Agency and Citizenship and Immigration Canada, have an important security, intelligence or enforcement role and, as a consequence, collect substantial amounts of personal information.

Our Office's approach is to engage with such institutions to help them consider the privacy implications of programs before they are launched. An effective tool for this purpose is the Privacy Impact Assessment (PIA) process, created by the Treasury Board Secretariat in 2002 to enhance privacy and data security across the federal bureaucracy.

In 2008-2009 our Office worked with several federal organizations under the PIA process to ensure that their new programs incorporate appropriate measures to collect, use, disclose and dispose of personal information, in conformity with the *Privacy Act*.

Two prominent examples related to the inter-jurisdictional security measures being planned for the 2010 Vancouver Olympics, and plans by Canadian border and immigration authorities to expand their collection of biometric personal information on visitors seeking visas to enter the country. Both are large-scale endeavours involving many departments, local officials and international players.

In the past year, our Office has also reviewed with interest some important new guidance being issued by the Treasury Board Secretariat, including:

- An updated Policy on Privacy Protection,
- Expanded obligations on all departments to report privacy-related performance statistics, and
- New rules for effective Personal Information Sharing Agreements governing the exchange of data between government departments or with other jurisdictions within Canada or international partners.

Olympic and Paralympic Games

In February and March 2010, Canada will host the Winter Olympic and Paralympic Games in Vancouver and Whistler, British Columbia. Our Office has been closely monitoring security arrangements for the Games, and has been weighing their impact on privacy.

As the first major international event to take place in Canada since the 9/11 terrorist attacks on the United States, security will be imperative at these Games. At the same time, it is important for Canadian officials involved in security planning to remember that they play a key role in upholding civil liberties, including the right to privacy.

In February 2009, our Office sponsored a workshop on privacy and security at the Games, held in Victoria as part of the 10th Annual Reboot Privacy and Security Conference. Experts from academia, civil society, the private sector and government participated in the workshop, organized by the University of Victoria. Speakers addressed the extent to which security officials have considered privacy protections, as well as the legacy effect of security and surveillance installations to be erected around the Games.

Over the winter, Assistant Commissioner Chantal Bernier and other senior officials met with the Vancouver Olympics Integrated Security Unit, which brings together police, military and other security forces that are working together to secure the Games.

Our Office also continues to collaborate on this file with the Office of the Information and Privacy Commissioner for British Columbia. As this is an issue of shared jurisdiction, the two offices worked together to develop guiding principles and recommendations intended to help security officials plan and carry out their duties in a way that does not unduly infringe on the privacy rights of individuals.

We have created a section on our website devoted to the Olympics and privacy issues.

Federal Administrative Tribunals

In last year's *Privacy Act* annual report, we highlighted the privacy issues confronting Canadians when federal administrative and quasi-judicial tribunals publish on the Internet decisions that contain highly sensitive personal information.

These bodies consider issues such as the denial of pension and employment insurance benefits; compliance with employment and other professional standards; allegations of regulatory violations, and irregularities in federal public service hiring processes.

Our Office continues to receive complaints from people concerned that participating in a tribunal proceeding could violate their privacy when the tribunal decision is posted online.

Decisions of administrative and quasi-judicial bodies often contain personal details that not many people would be comfortable sharing widely: salaries, physical and mental health problems, detailed descriptions of disputes with employers and alleged wrongdoing in the workplace. Other information of questionable relevance is also often included in decisions of these bodies, such as the names of participants' children, home addresses, places and dates of birth, and descriptions of criminal convictions for which a pardon has been granted.

Many complainants told us they were distressed to discover – often with no prior notice – that personal information about them was available on the Internet for neighbours, colleagues and prospective employers to see.

A long-ago transgression or temporary lapse in judgment could continue to haunt an individual for many years. Even if no past transgression was involved, the nature of the personal information that was being disclosed could be deeply embarrassing.

In our opinion, exposing so much personal information to the entire world poses enormous privacy risks. Often, moreover, there is no apparent need for, or benefit from, the widespread public disclosure of the identities of individuals who participate in tribunal proceedings.

At the federal level, we have met with officials from the Treasury Board Secretariat to reiterate our urgent call for centralized and specialized policy guidance for federal tribunals regarding the electronic disclosure of personal information in their decisions.

Our Office, along with our provincial and territorial counterparts and the Office of the Information Commissioner of Canada, are consulting with administrative tribunals on the development of broad guidelines to address the natural tension between maintaining the transparency of administrative justice, while also protecting the privacy of individuals.

We hope that Treasury Board will eventually adopt these guidelines.

ADVANCING KNOWLEDGE

In order to further our understanding about emerging privacy challenges, our Office created strategic working groups focused on each of our four identified priorities.

The priorities, which we first put forward in 2007, focus on the privacy challenges inherent in national security initiatives, information technologies, genetic technologies, and the protection of identity.

With members drawn from our Office's operational branches, the working groups:

- Identify current issues, trends and challenges within their specific priority area;
- Help develop the Office's position; and
- Provide advice and work to influence public policy.

This section describes the groups' efforts to further understanding of the privacy issues affecting the Office's four priority areas, especially with respect to the public sector.

National Security Working Group

The National Security Working Group acts as the Office's eyes and ears on security-related matters. The group monitors developments in the field, and invites experts to brief members on emerging trends.

For example, an official with Justice Canada's Human Rights Law Section described his ongoing analysis of information-sharing agreements among national security agencies in Canada. Two officials from Public Safety Canada elaborated on the work of the Canada Cyber-Security Directorate.

The working group also supports the Commissioner's appearances before Parliament on national security-related issues, and undertakes research on the oversight mechanisms supporting Canada's national security programs.

In order to strengthen the Office's relationships with other oversight bodies, representatives of the working group were also invited to join the Review Agencies Forum, which brings together the Office of the Communications Security Establishment Commissioner, the Security Intelligence Review Committee, the Office of the Inspector General of the Canadian Security Intelligence Service, and

the Commission for Public Complaints against the RCMP. The Forum provides an opportunity for review analysts to compare best practices and discuss issues of mutual interest and concern.

Information Technology and Privacy Working Group

The Information Technology and Privacy Working Group monitors and researches developments that could have an impact on privacy in the rapidly changing field of information technology.

As part of this work, the group holds briefing sessions to gather information about how new technologies work and what their implications on privacy may be. In 2008-2009, for example, we had briefings from industry on a new online authentication service and a biometrics solution.

The group also organized a workshop on the privacy implications of geospatial technologies.

Genetic Privacy Working Group

The Genetic Privacy Working Group explores the privacy issues raised by frontier genetic technologies.

The group invited several external experts to a staff workshop aimed at increasing our understanding of the issues, and setting our work and research agenda for the next two years.

The workshop focused on four issues: The banking of biological tissue for research purposes (biobanking); the use of genetic information by law enforcement agencies; direct-to-consumer genetic testing (e.g. paternity tests), and the use of genetic information by insurance companies.

The working group was active on the legislative front, participating in the mandatory Parliamentary review of the *DNA Identification Act* and appearing before both the House of Commons Committee on Public Safety and National Security, and the Senate Legal and Constitutional Affairs Committee.

In particular, the group expressed concerns about expanding the national DNA database by taking DNA from more offenders for a broader range of offences, allowing "familial searches," and increasing international information sharing.

Identity Integrity Working Group

The Identity Integrity Working Group seeks to understand and anticipate the challenges to personal identity as government and private sector organizations begin to integrate their information management, client service, network security and knowledge management systems.

Members of the working group are currently tracking the development of a federated identity management system for the Government of Canada, as well as actively engaging federal and provincial agencies in the development of standards for a system of pan-Canadian electronic health records.

As social media tools like Facebook and Twitter become popular in the private sector, they are also being considered by government organizations. Members of the working group are participating in the pilot testing of an internal social network for federal public servants, and have provided guidance for use of social networks by employees and managers of the public service.

The working group is also providing direction to independent research into how political parties in Canada and abroad collect and use personal information.

POSITIONING CANADA AS A WORLD LEADER IN PRIVACY

We live in a global economy in which personal information is continually in motion. The flow of information across national borders benefits organizations and individuals by lowering costs, increasing efficiency and improving client convenience. Countries with common interests, particularly in commerce and security, are also increasingly likely to share information about their citizens.

However, as personal information moves across borders, the privacy risks increase. This creates new challenges for our Office that, in many cases, are similar to those faced by other jurisdictions.

Indeed, it is apparent that, when Canadians' personal information flows across international borders, we have to work with international counterparts to make the protection of personal information as seamless as possible. We also need to work co-operatively to develop enforcement mechanisms that provide people with recourse, regardless of where their information is being processed.

Participants at the 29th International Conference of Data Protection and Privacy Commissioners, hosted by our Office in Montreal in September 2007, agreed to continue working together to strengthen data protection worldwide. They also agreed to

work with standards bodies such as the International Organization for Standardization (ISO) to develop effective and universally accepted international privacy standards.

Our Office was also instrumental in creating the Association of Francophone Data Protection Authorities and we are now members of the Asia Pacific Privacy Authorities (APPA). We also meet regularly with national and sub-national data protection authorities from countries that, like Canada, are federal states, in order to discuss the challenges of data protection when power is shared between orders of government.

Here is a snapshot of our ongoing efforts during 2008-2009:

Organisation for Economic Co-operation and Development

The Organisation for Economic Co-operation and Development's (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, adopted in 1980, were instrumental in the development of privacy legislation worldwide. Indeed, the guidelines form the basis of both the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*. The OECD continues to promote international co-operation in efforts to enhance protections for personal information.

In 2008-2009, our Office participated in a workshop, co-hosted by the OECD, which explored accountability in privacy governance. We also provided input into the OECD's work on identity management and to the OECD Ministerial Meeting on the Future of the Internet Economy.

Asia-Pacific Economic Co-operation

Our Office contributed to efforts by the Asia-Pacific Economic Co-operation (APEC) to explore ways to implement the APEC Privacy Framework, adopted in 2004. In particular, we worked with other commissioners and enforcement authorities on co-operative information sharing and complaints investigations.

We also helped build capacity within economies in the region that do not have their own privacy legislation through seminars on how PIPEDA functions, particularly with respect to cross-border transfers of personal information.

The Asia Pacific Privacy Authorities

The Asia Pacific Privacy Authorities (APPA) is an important regional forum for the exchange of ideas about privacy regulation, new technologies, and the management of privacy inquiries and complaints. APPA meets twice yearly and organizes an annual

Privacy Awareness Week throughout the Pacific region to promote awareness of privacy rights and responsibilities.

Francophonie

Following a meeting in Monaco in 2006, representatives of data-protection authorities in 14 French-speaking nations agreed, in recognition of their common challenges, to share knowledge and experience in a structured forum. And so, with the support of the *Organisation internationale de la francophonie* (OIF), they decided to form an Association of Francophone Personal Data Protection Authorities, which held its inaugural meeting in Montreal in 2007.

Chaired by Jacques Saint-Laurent, president of Quebec's *Commission d'accès à l'information*, the association's prime objective is to build co-operative programs driven by training activities, information-sharing practices, and studies that call for the pooling of expertise and experience.

In 2008, the association continued to follow up on an action plan developed at the Montreal meeting. In addition to devising a longer-term strategic plan, the association last year established a working group involving representatives of the association and the OIF. It also shared among members various documents on video surveillance, biometrics and the protection of children's rights with respect to personal information; set up a practical internship practice; published a newsletter, and engaged in outreach.

A study of the privacy mechanisms prevailing in the three francophone jurisdictions of Canada – Quebec, New Brunswick and across the federal government – was published in 2009, along with an audio-visual companion piece. Entitled *Protection of Personal Information – Beyond the Blueprint*, the project involved privacy authorities in the three jurisdictions. Spearheaded by former *Commission d'accès à l'information du Québec* president Paul-André Comeau, the study showcased lessons learned from these "Canadian models."

The association also promotes the sharing of best practices among francophone data-protection authorities. At the 2008 conference of the Association of Francophone Personal Data Protection Authorities, for example, our Office described how discussion papers are commonly used in Canada to promote reflection on privacy issues within communities. We also spoke of our use of contests to raise awareness among young people.

International Standards Development

Our Office has been an active participant in efforts by the International Organization for Standardization (ISO) to develop and maintain standards and guidelines addressing security aspects of identity management, biometrics, and the protection of personal information.

ISO's key projects in 2008-2009 included work towards a framework for identity management, a privacy framework, as well as identifying requirements for additional future standards and guidelines related, for example, to specific privacy-enhancing technologies.

The identity management framework is intended to describe fundamental concepts of identity management and to establish appropriate principles, processes and technology components for managing identities.

A senior member of our Office chairs the Canadian Advisory Committee feeding into this international work and also heads the Canadian delegation to the ISO working group responsible for identity management and privacy technologies. In addition, he is the liaison officer responsible for presenting the views of the International Conference of Data Protection Commissioners to this ISO working group.

During 2008-2009, the identity management and privacy framework projects continued to progress towards publication of international standards. We were pleased to see agreement on basic terminology and certain concepts.

PRIVACY BY THE NUMBERS – 2008-2009

Inquiries and Complaint Investigations		
Total inquiries received		12,179
Inquiries linked to the *Privacy Act*	3,103	
Inquiries linked to PIPEDA	6,588	
Inquiries that could not be linked exclusively to the *Privacy Act* or PIPEDA	2,488	
Complaints received		748
Complaints closed		990

Audit and PIA Reviews	
Public Sector Audits:	
Underway from previous year:	4*
Newly launched:	3
Privacy Impact Assessment submissions:	
Received	64
Reviewed	31

Legal, Policy and Parliamentary Affairs	
Public-sector policies or initiatives reviewed	70
Policy guidance documents issued	4
Draft bills and legislation reviewed for privacy implications	9
Parliamentary committee appearances made	9
Other interactions held with Parliamentarians or staff	103

Other OPC Activities	
Formal visits from external stakeholders received	63
Speeches and presentations delivered	100
News releases and fact sheets issued	29
Media interviews granted	294
Stakeholder outreach events attended	11
Publications distributed	13,200
Hits to Office website logged	1.71 million
Hits to Office blog logged	291,500
Access to Information Act requests received	28
Access to Information Act requests closed	23
Privacy Act requests received	10
Privacy Act requests closed	10

* 2 completed; 2 remained in progress at year-end

PRIVACY LANDSCAPE

The following sections of this annual report highlight the two main threats to our privacy: security concerns and developments in information technology.

Governments around the world have determined – sometimes erroneously, in our opinion – that collecting, analyzing and storing more and more personal information is the key to ensuring the security of their citizens.

Meanwhile, information technologies are ever-more powerful and allow for mountains of personal data to be collected, manipulated and shared in ways that were unimaginable not so long ago.

Much of our work in recent years has centred on these two areas. During that time, we have sought to be clear that privacy rights need not be at odds at with either public security or the use of information technology. On the contrary: measures to respect privacy must be integral to both of these new developments.

We expect these issues to continue to dominate in the years to come.

INTEGRATING PRIVACY AND SECURITY AFTER 9/11

Major audits of security programs raise concerns about the over-collection of personal information; IT risks

Much of our work in recent years has focused on the privacy risks inherent in post-9/11 security programs that involve the collection and use of personal information.

In 2008-2009, we closely examined two key tools in Canada's efforts to combat terrorism – the so-called "no-fly list" and an independent agency mandated to analyze financial transactions and identify suspected money laundering and terrorist financing. These audits highlighted several privacy concerns.

We also worked with government departments and agencies to try to mitigate the privacy risks related to, for example, airport scanners that penetrate the clothing of travellers to reveal concealed objects; the use of biometrics in visas for foreign nationals, and enhanced driver's licences.

It is hard to imagine a single day in recent history that has had a bigger impact on privacy than September 11th, 2001.

In the wake of the horrific terrorist attacks that stunned the world that day, governments everywhere have rolled out scores of new security programs involving the collection, analysis and storage of personal information.

This trend has created significant new risks for the privacy rights of Canadians.

The impact of the reaction to 9/11 is felt in many of life's ordinary activities – going to the airport or sending money to an overseas relative.

Travelling by air now involves having your name checked for a possible match against lists of people designated as too dangerous to fly. Searches are more thorough and more frequent.

Your routine interactions with a broad range of businesses such as banks and casinos, and professionals such as accountants and life insurance brokers, may now involve the collection of extra personal information that must be reported to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). This information is sent without your consent.

A number of companies and professionals are also now required to make judgments about whether your behaviour is suspicious – and then report their suspicions to FINTRAC.

Surveillance cameras increasingly monitor your movements in public spaces.

In Vancouver, officials are preparing an Olympic Winter Games security operation unprecedented in Canadian history – one that will entail dramatically increased surveillance and scrutiny of residents and visitors.

Meanwhile, plans are in the works for foreign nationals coming to Canada to be issued visas that contain their biometric information.

Our personal information is constantly in demand as our government scrambles for ways to protect us from future terrorist attacks.

Life has changed since September 11th, 2001.

Integrating privacy and security

The debate around the plethora of new security programs has often centered on questions such as: How much privacy are we willing to give up for security? Does privacy even matter when lives are at stake?

Security officials and privacy advocates alike talk about striking an appropriate balance between security and privacy.

However, debates about privacy versus security too often take as a given the notion that giving up some privacy will automatically make us safer. At the Office of the Privacy Commissioner of Canada, we don't believe that to be the case. Indeed, our work with federal government departments and agencies often involves challenging this assumption.

Many times we are not convinced that collecting mountains of personal data will make anyone any safer. While we can appreciate the underlying aim of many security programs, we often question the approach, efficacy, efficiency or proportionality of certain initiatives.

There will be times when some of our privacy rights must be set aside in order to protect public safety. However, Canadians should only be asked to make this sacrifice when it is clear that doing so will actually lead to a safer society, and that no other less privacy-intrusive options are available. Even then, it is critical to integrate privacy protections.

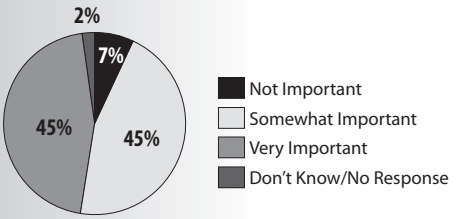
Canadians value privacy

A poll we commissioned in early 2009 found that Canadians feel personal privacy is an important consideration as governments provide law enforcement and intelligence agencies with enhanced powers. Nine in 10 said it was important that privacy considerations factor into decisions about enhanced security powers for law enforcement agencies.

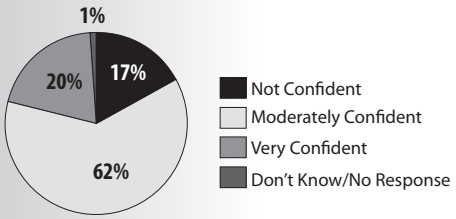
At the same time, a majority of Canadians expressed only moderate confidence that new security measures at borders and airports are actually keeping them safer. A clear two-thirds majority also said they were only moderately confident that Canadian law enforcement and security agencies adhere to privacy laws that restrict the collection, storage, and sharing of personal information.

Privacy issues related to security initiatives continued to be a major focus for our Office in 2008-2009. The following is a look at some of the major security-related work we undertook over the year – through our audits, our reviews of privacy impact assessments, and other consultations with Parliament and government departments and agencies.

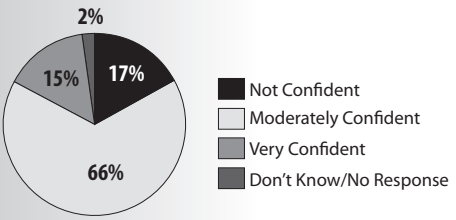
"How important should a person's privacy be considered as governments provide law enforcement and intelligence agencies with enhanced powers?"



"How confident are you that new security measures (at borders and airports, for example) result in increased safety and security?"



"As you may be aware, law enforcement and security agencies in Canada are subject to privacy laws that place restrictions on the collection, storage and sharing of personal information. How confident are you that law enforcement and security agencies in Canada adhere to these privacy laws?"



2009 OPC survey of 2,028 Canadians conducted by EKOS Research Associates Inc.

Audits

FINTRAC

The Financial Transactions and Reports Analysis Centre of Canada – better known to Canadians as FINTRAC – is an independent agency with a mandate to collect and analyze financial transactions and to disseminate intelligence concerning suspected money laundering and terrorist financing. Created in 2001, the agency operates at arm's length from law enforcement.

Under amendments passed in 2006, the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* requires our Office to review FINTRAC every two years and report the results to Parliament. This audit requirement was included along with legislative changes that expanded the types of transactions that must be reported to FINTRAC; increased the number of entities required to collect information about clients and report to FINTRAC; and established an administrative monetary penalty regime for non-compliance with the Act.

What We Found

Our first audit of FINTRAC found that, overall, the agency has a robust and comprehensive approach to securing the personal information of Canadians. However, privacy involves more than protecting data; it also means ensuring that the amount of personal information that is collected is kept to an absolute minimum.

Our audit found that FINTRAC is acquiring and retaining more personal information than what the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* allows.

Entities Reporting Personal Information to FINTRAC

- Financial entities of all types (banks, credit unions, *caisses populaires*)
- Life insurance companies, brokers or agents
- Securities dealers, portfolio managers, provincially authorized investment counsellors
- Foreign exchange dealers
- Money services businesses
- Crown agents accepting deposit liabilities and/or selling money orders
- Accountants/accounting firms, real estate brokers/sales representatives involved in activities such as receiving or paying funds on behalf of a client
- Casinos (except some temporary charity casinos)
- British Columbia notaries public (including notary corporations) and dealers in precious metals and stones
- Real estate developers

This is not an insignificant issue for Canadians. The legislation requires potentially up to 300,000 entities (see examples on the previous page) to scrutinize and report vast amounts of personal information related to the financial transactions of clients. Such reports are submitted without the consent of those clients.

Given the clear risks to privacy, Canadians must be assured that their personal information is being appropriately managed within well-established controls.

The requirement to safeguard information assets, while common to all government departments, is heightened for organizations such as FINTRAC.

As part of our audit, we examined policies, practices and procedures, guidelines, analytical tools, security assessments, training materials and information-sharing agreements. We reviewed a sample of the reports FINTRAC receives, as well as information it discloses to law enforcement agencies and other federal departments and agencies.

Privacy Protections

We also assessed the checks and controls the agency has in place to safeguard privacy, how it assigns privacy responsibilities, manages privacy risks, and ensures compliance with its obligations under the *Privacy Act*.

While the Centre has put in place elements of checks and controls, there are gaps that need to be addressed. Specifically, governance and accountability for privacy are not clearly defined, FINTRAC's privacy risk management process is not formalized, and there is a lack of privacy-specific training for staff.

Strengthening the framework will help ensure FINTRAC meets its obligations under the *Privacy Act* and better protects the personal information of Canadians.

Down the road, this stronger framework could help the organization avoid the types of privacy problems uncovered during the audit.

Some of the most serious deficiencies identified in the audit relate to the acquisition and retention of personal information. Current controls – including front-end screening and ongoing monitoring of reports – are not sufficient.

As explained below, the result is that FINTRAC is acquiring personal information beyond its legislative authority.

The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* requires certain businesses and professions to submit reports to FINTRAC on large cash transactions or electronic funds transfers of $10,000 or more. Any suspicious transactions related to money laundering or terrorist financing – regardless of the amount of money involved – must also be reported.

Excessive Reporting

In the sample of reports we looked at, we found a number of large cash transaction reports, electronic funds transfer reports and cross-border currency reports (on funds taken into or out of Canada) that fell below the $10,000 threshold. We also found instances where a casino reported transactions involving the disbursement of $10,000 or more – even though the requirement for casinos to report the transactions to FINTRAC had not yet taken effect at the time our audit was conducted.

We also found problems related to reports made on the basis of unsubstantiated suspicion. The legal threshold of "reasonable grounds to suspect" is not defined in the legislation. FINTRAC policy describes it as a level of suspicion above "mere suspicion" and below "reasonable belief".

We found that, although suspicious transaction reports are reviewed and prioritized, they are not assessed for reasonable suspicion of money laundering or terrorist financing.

Of the files sampled, we identified several that did not clearly demonstrate reasonable grounds to suspect money laundering or terrorist financing. For example:

- A reporting entity filed several reports in which it stated it was "taking a conservative approach in reporting this … because there are no grounds for suspecting that this transaction is related to the commission of a money laundering offence, but there is a lack of evidence to prove that the transaction is legitimate."

- An individual deposited cash under the $10,000 reporting threshold in a financial institution. The report indicated that, although the account activity appeared normal, the transaction was reported to ensure that the individual complied with all tax requirements. There was no indication that the transaction related to suspected money laundering or terrorist financing.

- An individual deposited a government cheque for an amount less than $300 and then withdrew the entire amount. The financial institution filed a Suspicious Transaction Report, but did not indicate why the transaction was deemed suspicious.

These examples would suggest that some reporting entities may be unclear on their reporting obligations, or default to reporting if any doubt exists, rendering privacy a secondary consideration.

We also examined a sample of voluntary information records.

The Centre receives voluntary information concerning suspicions of money laundering and terrorist financing from a wide range of sources – the public, police, the Canadian Security Intelligence Service (CSIS) and foreign financial intelligence units.

Upon receipt, FINTRAC assesses these reports to determine whether they fall within its mandate. Reports unrelated to the Centre's mandate are retained but not made available for analysis.

Despite this screening, we found voluntary information records in FINTRAC's database where no suspicion of money laundering or terrorist financing was evident. For example:

- FINTRAC received a report from a retailer that had implemented its own anti-money laundering program, whereby all cash and debit transactions in excess of $10,000 were reported. None of the reports we examined contained any indication that money laundering was suspected.

- An individual converted some foreign currency at a money service business. When asked to provide information to meet legislated record-keeping requirements, the individual asked if this information would be shared with federal government agencies. The clerk explained the information would only be retained by the business, and was needed to comply with federal regulations. The client left without completing the transaction. The report includes the comment: "I don't believe (the individual) was laundering money but was concerned about immigration or taxation for some reason."

- An individual deposited at a financial institution a cheque from a law firm. The financial institution was satisfied that the individual provided legitimate reasons for the source of funds, but decided to notify FINTRAC anyway because of the individual's ethnic origin and the fact the individual had recently taken a pleasure trip to a particular country.

We also identified instances where extraneous information such as social insurance numbers and health card numbers was submitted and retained by the Centre.

Our Recommendations

We recommended that FINTRAC work with reporting entities to ensure the Centre does not acquire personal information that it has no legislative authority to receive and that it does not need or use.

Toward that end, the Centre should enhance its front-end screening of reports, and develop stronger ongoing monitoring and review to ensure that its information holdings are both relevant and not excessive.

We also recommended that FINTRAC permanently delete from its holdings all information that it did not have the statutory authority to receive.

Given that we looked at only a sample of reports, we did not determine the extent to which FINTRAC's information holdings contain information that the agency was not authorized to obtain.

Further Issues

The audit also highlighted other areas where FINTRAC could strengthen privacy protections for Canadians.

For example, we recommended that the agency work with its intelligence partners to ensure, to the extent possible, that terrorist affiliations are confirmed prior to retaining this data and making it available for analytical purposes.

Although FINTRAC attempts to verify individuals' affiliations with terrorist groups, it is difficult to do so because of a lack of vital information, such as dates of birth.

Where identity cannot be confirmed, FINTRAC does not pursue further analysis, but does retain the information in its database. The practice, by default, is to retain reports, irrespective of knowledge, belief or suspicion of terrorist affiliation.

We also made recommendations to strengthen checks and controls to safeguard privacy. We urged FINTRAC to:

- Appoint a senior executive as Chief Privacy Officer to provide strategic leadership and to co-ordinate and oversee privacy-related activities;

- Ensure that all initiatives and programs requiring privacy impact analyses are identified, reported and tracked;

- Finalize and implement privacy incident guidelines to comply with breach reporting expectations established by the Treasury Board Secretariat; and

- Expand its security awareness initiatives to ensure all employees who handle personal information or have privacy responsibilities receive specific training on core privacy principles and requirements surrounding privacy impact analysis.

FINTRAC's Response

In response to our recommendations, FINTRAC has agreed to make numerous changes, including the creation of a new Chief Privacy Officer position and development of privacy incident guidelines. FINTRAC also agreed to update its privacy awareness training to include more privacy-specific information for employees.

While FINTRAC said it has taken steps to limit the receipt of personal information that should not have been sent to the Centre, it noted that the destruction of extraneous information already in the FINTRAC database presents a technical challenge. The Centre is developing a strategy to move forward with a destruction plan.

The Centre will establish a set of written criteria to help its officials determine when the threshold for disclosures to the Canada Border Services Agency and the Communications Security Establishment of Canada has been met. It will also enter into a dialogue with its intelligence partners to explore ways to mitigate the risk of retaining information about individuals initially suspected of a terrorist affiliation, once it has been confirmed that no such affiliation exists.

FINTRAC also recognized the importance of observing the principle of data minimization during the execution of its compliance mandate. The Centre will reinforce the importance of respecting this principle when training staff and when reviewing and updating its policies and procedures.

PASSENGER PROTECT PROGRAM

Aviation security has always been a government priority, but when passenger airliners were turned into terrorist weapons on September 11th, 2001, security measures were heightened around the world.

Canada was no exception. The federal government created several national security programs that were designed to protect Canadians, but that also wound up affecting their privacy.

One of those was the Passenger Protect Program, better known to Canadians as the "no-fly list". This passenger screening tool, implemented in June 2007, aims to prevent people named on a "specified persons list" from boarding domestic or international flights leaving or bound for Canadian airports.

The program has sparked privacy concerns, in part because it is secretive, using personal information without the knowledge of the individuals concerned.

Moreover, the repercussions for a person named on the list being denied boarding on an aircraft can be profound in terms of privacy and other human rights, such as freedom of association and expression and the right to mobility.

Our Office audited the Passenger Protect Program to determine whether Transport Canada has adequate controls and safeguards for the personal information collected and used by the program.

We did not examine the effectiveness of the program or the reliability of information used to determine whether particular individuals should have been added to the specified persons list. Those issues fall outside our mandate.

Moreover, we did not examine the personal information handling practices of airlines, although we did examine Transport Canada's oversight role in this regard.

How it Works

The Passenger Protect Program operates out of Transport Canada headquarters in Ottawa. Senior officials from Transport Canada, CSIS and the RCMP form the Specified Persons List Advisory Group, which meets regularly to review the existing list and recommend to the Deputy Minister of Transport Canada any names that should be added to or removed from the list.

Airlines must verify all passenger names against the specified persons list at check-in. If a match is confirmed, the airline must immediately notify Transport Canada's Intelligence Operations and Support Centre by telephone.

Transport Canada carries out its own verification to confirm whether a passenger identified by an airline is actually a person on the list. A Transport Canada officer makes the decision to deny or allow boarding.

Individuals barred from boarding under the Passenger Protect Program may apply to Transport Canada for reconsideration. The onus is on them to provide grounds for reconsideration.

Transport Canada's Office of Reconsideration engages contract security advisers to review such applications and to recommend to the Deputy Minister whether a person under consideration should be on the list.

Individuals may also apply to the Federal Court of Canada for a judicial review of Transport Canada's decision. At the time of the audit, only one such application has been filed.

Overview of What We Found

In general, we found that Transport Canada collects and uses personal information within the Passenger Protect Program in accordance with the *Privacy Act* and the *Aeronautics Act*. The department has operating procedures and agreements in place to ensure that it collects only the personal information it needs to administer the program.

In particular, Transport Canada discloses personal information selectively to officials who actually need it, and takes steps to restrict the disclosure of personal information only to that which is essential to operate the program.

The audit did, however, raise some concerns:

- The Deputy Minister at Transport Canada, who is responsible for the names being added to or removed from the specified persons list, was not provided with complete information to make informed decisions. The Deputy Minister was provided with a recommendation to sign, with little to no supporting evidence to explain why someone should be placed on or removed from the list.

- The information technology application used to disclose to air carriers information on the specified persons list has not undergone a formal certification and accreditation process as required by government security policy. The purpose of this process is to reduce the chances of undetected information technology security weaknesses that may leave sensitive personal information at risk.

- Transport Canada has not verified that airlines are complying with requirements of federal identity screening regulations related to the handling and safeguarding of specified persons list information. There is a further risk that this information could be inappropriately disclosed, due to a small number of air carriers that rely on paper copies of the list.

- There were no requirements that air carriers report to Transport Canada security breaches involving personal information.

Information used in Decision-Making

Transport Canada's Deputy Minister has the delegated authority to determine who is included on the specified persons list. The audit did not identify problems with the accuracy of program information. However, the information provided to the Deputy Minister was not sufficient to support informed decision-making.

In particular, the Specified Persons List Advisory Group does not provide the Deputy Minister with critical information supporting the reasons for recommending changes to the list. For example, the Deputy Minister does not receive a copy of the records, meeting notes and full reasons supporting recommendations.

Providing an incomplete record to the Deputy Minister raises the possibility that an incorrect change will be made to the specified persons list. This could have serious implications for individuals wrongly placed on the list, or for the travelling public if a potentially dangerous person is left off it.

Safeguards

Transport Canada generally has put in place physical measures, training programs and staff security clearances to safeguard personal information within the Passenger Protect Program.

However, Transport Canada did not demonstrate that the Specified Persons List information technology application used to disclose list information to air carriers had been certified and accredited to meet government security standards. An information technology system that has not been certified and accredited increases the likelihood of undetected security weaknesses, which could render sensitive personal information vulnerable.

During the course of our audit, we found an example of a system control that was not operating as intended. This undetected error prevented authorized officials at Transport Canada from accessing data on the system. We were concerned about the possibility that this vulnerability could have resulted in access rights being given to people without the authority to update the specified persons list.

The program error that we identified during our audit may have been prevented if a formal certification and accreditation process had been in place. The department has since corrected this issue.

We also found that Transport Canada has not taken steps to ensure that airlines are properly handling and safeguarding the personal information included on the specified

persons list. Given this lack of oversight, the department cannot provide assurances that this sensitive personal information could not be used or disclosed inappropriately.

We also found that two smaller airlines did not have an automated means to match passenger information with the specified persons list. These airlines print copies of the list for airport check-in counter staff. If the list were to go astray, there could be serious implications for the people named on the list and the reputation of the Passenger Protect Program.

Despite the potential consequences of a breach, there are currently no requirements for airlines to report privacy breaches to Transport Canada.

Transport Canada's Response

Transport Canada has responded positively to our recommendations relating to the Passenger Protect Program. The department has already made changes to comply with recommendations dealing with information provided to the Deputy Minister and oversight of airlines handling specified persons list information.

The department has committed to improve its practices to better protect Canadians' sensitive personal information.

Transport Canada did not demonstrate that it has a documented certification and accreditation process, as defined in the government security policies. The department has committed to review its existing processes and will adjust them based on best practices and guidelines.

Previous Passenger Protect Work

In 2005 and 2006, we reviewed Privacy Impact Assessments about the Passenger Protect Program from Transport Canada and Public Safety and Emergency Preparedness Canada (now Public Safety Canada) on behalf of CSIS and the RCMP.

We made several recommendations at the time to eliminate and mitigate some of the most serious privacy impacts. Transport Canada, CSIS and the RCMP implemented many of the recommendations soon after. Some of those changes included:

- Creation of identity screening regulations to create enforceable standards for air carriers' handling and protection of personal information;

- Increased age for passenger screening (from 12 years to 18 years);

- Development of memoranda of understanding with air carriers and the RCMP that include provisions for the protection of personal information;
- Establishment of retention schedules for Passenger Protect information; and
- Implementation of standard operating procedures for the Office of Reconsideration and Transport Canada intelligence duty officers.

Canada Border Services Agency Audit Follow-up

In 2008-2009, we followed up with the Canada Border Services Agency (CBSA) to review the status of our recommendations arising from an audit we conducted in 2006.

That audit focused on trans-border exchanges of personal information between the CBSA and agencies in the United States. The audit report included 19 recommendations such as:

- Strengthening the agency's privacy management framework, including information-sharing agreements with the U.S.;
- Developing security standards with U.S. partners;
- Evaluating shared lookout and high-risk traveller initiatives with the U.S;
- Developing policies and practices for the recording and tracking of external disclosures of personal information;
- Strengthening internal access rights procedures for IT systems;
- Defining security roles and a security management framework to safeguard personal information; and
- Improving public reporting of cross-border data flows to ensure greater transparency about these activities for Canadians and Parliament.

During our follow-up review, we were pleased that the agency indicated that it has fully implemented or made progress on all 19 recommendations.

For example, information-sharing agreements with the U.S. are to be reviewed to ensure that their objectives are being met and privacy gaps are identified and addressed. Based on this review, the CBSA will negotiate with the U.S. where agreements are deemed deficient.

The agency's intelligence program has implemented a policy under which the sharing of all personal information with partners must be documented. This obligation is underscored with specific training for employees.

As well, the agency's implementation of a privacy management framework and its associated policies, guidelines and training is targeted for mid-2010.

The CBSA's follow-up activities in response to our audit recommendations will strengthen privacy protections for people crossing Canada's borders.

PIA Review

Privacy Impact Assessments (PIAs) are designed to help federal institutions determine the effects of programs and services on privacy.

The Office does not approve PIAs or endorse projects. Instead, we make recommendations on how projects can be improved to better protect Canadians' privacy.

Generally if a department conducts a PIA before implementation and acts to mitigate identified privacy risks, it is supposed to ensure that, at the end of the process, the majority of privacy risks have been satisfactorily addressed – to the ultimate benefit of Canadians.

Here are descriptions of key security-related PIAs we reviewed over the year:

Whole Body Imaging Scan Trial at Canadian Airports

In 2008, the Canadian Air Transport Security Authority (CATSA) launched a trial at the international airport at Kelowna, B.C., involving the voluntary use of scanners that penetrate clothing to generate a detailed image of the body. This allows airport security officers to detect potentially dangerous objects hidden beneath clothing.

Our Office reviewed a Preliminary Privacy Impact Assessment submitted by CATSA for the trial. The agency accepted our recommendations that during the trial:

- Participation would be on an anonymous basis and purely voluntary;
- The image generated was not correlated with the name of the passenger or any other identifying information;
- The screening officer reviewing the images would be in a separate room and unable to see the passenger;

- The screening officer with the passenger would not be able to see the image;
- Images would be deleted from the system once the screening was complete.

In 2008-2009, staff from our Office visited the Kelowna airport to verify that the safeguards were actually being followed.

At the conclusion of the trial in January 2009, CATSA submitted a final report to Transport Canada, with a copy to our Office. CATSA has recommended that the scanners be used in Canadian airports but, at the time of drafting this report, we have no information on the configurations being considered or whether they would be used for primary or secondary screening of passengers.

CATSA agreed to do a full PIA before any further deployment of the technology. We received this PIA and we were reviewing it at the time of writing this report. Transport Canada had not made public its decision on whether to introduce this scanning technology in Canadian airports.

Privacy advocates and data protection authorities are generally concerned about the invasiveness of this technology, so we will continue to follow this issue closely.

In the event that Transport Canada proceeds with a national roll-out, our Office will also work with CATSA to ensure that privacy-protective measures are implemented.

Enhanced Driver's Licence and Enhanced Identity Card Program

Under the U.S. government's Western Hemisphere Travel Initiative (WHTI), all travellers – including American and Canadian citizens – must now present a passport or other secure citizenship document when travelling to or through the United States.

In response to this new entry requirement, the Canadian government proposed the Enhanced Driver's Licence (EDL) and Enhanced Identity Card (EIC) for Canadians to use as an alternative to a passport when entering the U.S.

The EDL and EIC program is unique in that it falls under both provincial and federal jurisdiction.

Our Office's role in reviewing the privacy implications relates to the involvement of the Canada Border Services Agency (CBSA) as program intermediary, and Citizenship and Immigration Canada in its role of helping provinces examine documentary evidence of Canadian citizenship.

To date, the provinces of British Columbia, Ontario, Quebec and Manitoba have implemented EDL and/or EIC programs.

We have worked closely with our provincial privacy counterparts to ensure that privacy risks associated with the program as a whole are addressed.

One of our main concerns relates to the creation of another set of border-crossing credentials when the Canadian passport already exists. It is unclear why an alternative is necessary.

We also have questions about the use of vicinity Radio Frequency Identification (RFID) chips in the EDL and EIC cards. The chips can reportedly be read from distances of up to 30 metres, raising the risk of unauthorized interception of personal information. Appropriate safeguards for the CBSA database itself will also be critical, given the extent of personal information it holds.

Another major issue involves the potential use to be made of EDL holders' personal information once it is captured and stored in U.S. databases, particularly in light of U.S. laws such as the *USA PATRIOT Act*.

In our 2007-2008 annual report, we reported that we were working with the Information and Privacy Commissioner for British Columbia during the review of an EDL pilot project in that province.

The Canadian government and U.S. Department of Homeland Security agreed that, when the B.C. program was fully rolled out in June 2009, the database of EDL holder information would be stored in a separate and secure database maintained by the CBSA and housed in Canada.

Personal information will only be electronically transmitted to U.S. border officials when the EDL holder crosses the border into the United States.

We will continue to monitor the EDL and EIC program as it expands to other provinces and territories, or as changes are made.

ePassports

Passport Canada is preparing to issue electronic passports starting in 2011. The electronic passport, or ePassport, will contain an embedded chip carrying the personal information now found on the passport's data page, as well as the digitized facial image of the passport holder.

Our review of Passport Canada's PIA on the ePassport led us to question whether the personal information on the chip is adequately protected against unauthorized interception such as skimming and eavesdropping – risks identified by the International Civil Aviation Organization (ICAO). We have already seen instances of ePassport hacking in the United Kingdom.

We also broached the issue of risks related to inclusion of biometrics such as fingerprints or iris scans in the Canadian ePassport. Passport Canada has informed us that there is currently no intention to do this.

Another significant concern for our Office is the potential to build databases aimed at speeding border control processes and tracking travellers across national boundaries. We are also concerned about the potential for function creep and for such activities to be conducted without the public's knowledge.

Citizenship and Immigration Canada Biometrics Initiatives

Citizenship and Immigration Canada plans to implement initiatives involving the use of biometrics.

One, planned for 2011, involves collecting biometrics to support the process of issuing visas to foreign nationals entering Canada. The goal is to prevent criminals from entering Canada, while making the processing of legitimate applicants more efficient.

The program builds on a 2006 biometrics field trial that involved the introduction of fingerprint and facial recognition technologies to the processing of temporary resident visa applicants and refugee claimants. The technologies helped officials uncover cases of identity fraud.

We have expressed to Citizenship and Immigration Canada our concern that the use of biometrics data tends to be privacy intrusive.We have asked the department to provide more information about the need for biometrics data sharing.

Biometric information is highly sensitive information about a person's physical characteristics that is truly unique to each of us. The ability provided by the use of biometrics to uniquely identify someone is both one of the main reasons it is gaining in popularity and one of the main risks posed to privacy. The broad use of a unique identifier such as someone's biometric data increases the risk of identity theft and can have a greater impact on the individual in the event identity theft occurs.

There may be serious consequences for individuals if biometrics are used improperly, which is why it is so important that legal safeguards are introduced at the same rate as

advances in biometrics technology occur and that sufficient protections are designed to ensure that biometrics are not used in a privacy-invasive fashion.

Anti-Money Laundering/Anti-Terrorist Financing Regime

The Anti-Money Laundering and Anti-Terrorist Financing regime, formed in 2000, was formerly known as the National Initiative to Combat Money Laundering. It involves the Department of Finance, Department of Justice, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), the Canada Border Services Agency (CBSA), the Canada Revenue Agency, the RCMP, Public Safety Canada, and the Canadian Security Intelligence Service.

We have received PIAs from FINTRAC, CBSA and the RCMP related to each organization's respective role in administering specific portions of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*.

However, this is an example of a large-scale program where a strategic PIA, examining the cumulative privacy effects of every piece of the regime, would have been appropriate.

We have met with officials from the Department of Finance, in its role as lead organization, to address overarching privacy risks associated with the regime and to discuss our recommended mitigating measures.

National Integrated Interagency Information (N-III) System

The need for a broad PIA was also clear when we began looking at the National Integrated Interagency Information (N-III) initiative, an electronic records-sharing program linking national, provincial and municipal police forces, with the capacity to expand access and sharing capabilities to federal government departments.

The initiative involves the RCMP, Public Safety Canada and other federal departments and agencies.

In our 2007-2008 annual report, we noted that we had asked Public Safety Canada for a comprehensive PIA covering all elements of the system, but had yet to receive one.

Public Safety Canada did send us an overarching PIA on one component of the N-III system – the Integrated Query Tool – in February 2009. Although the PIA took several years to complete, the submission lacked information in key areas, preventing our Office from providing meaningful observations and recommendations. We sent the PIA back for revision and the department has provided timely elaboration in line with our recommendations.

Up to 25 departments and agencies stand to use the Integrated Query Tool, and each will be obliged to conduct its own PIA, as an addendum to the broad PIA prepared by Public Safety.

To date, however, we have received PIAs only from CBSA and FINTRAC.

PRIVACY IN A CONNECTED WORLD

From high-tech hitches to human error: Responding to complaints and privacy breaches

In 2008-2009, we received 3,103 calls and letters from Canadians concerned about a wide range of public-sector privacy issues. In all, we dealt with 990 formal complaints under the Privacy Act, *up from 880 the previous year.*

Most stemmed from problems people experienced in gaining access to their personal information, or perceived breaches of their privacy by federal departments or agencies. Not surprisingly, departments such as Correctional Service of Canada and Human Resources and Skills Development Canada, which handle large amounts of personal information, attracted the most complaints.

Canadians were also justifiably concerned when they feared their personal information was improperly disclosed. In many cases, our investigators were able to trace data breaches back to thefts or losses, faulty or inadequate procedures, or simple human error.

For all their benefits, information technologies also kept our investigators busy. While complaints about hacked computers, stolen laptops and missing disks are disturbing enough now, it is clear that future trends in computing will only magnify and intensify the risks.

In the years ahead, safeguarding the personal information of Canadians promises to become a mounting challenge for the Government of Canada.

In March 2009, after a year of sustained detective work, computer experts at the University of Toronto stunned the world with revelations about GhostNet, a sinister infiltration of high-value computer systems in more than 100 countries around the globe, from the offices of the Dalai Lama to embassies, defence establishments, media organizations and trade missions.

There is no evidence that the Government of Canada's computers were compromised, or that the personal information of Canadians stored or processed in those data systems was jeopardized. On the other hand, nothing is for certain, since no one has ever completely lifted the veil on GhostNet.

Still, the experience underscored the magnitude and persistence of the threat facing a government that relies heavily on information technologies to serve its citizens. Indeed,

the Canadian Security Intelligence Service reported in April that threats to Canada's information systems and critical infrastructure posed by hackers, terrorists and foreign states continue to rank among the service's key priorities.

Without question, the personal information of Canadians would be compromised in an attack by cyber-terrorists or spies. When the uses of information technology are benevolent, however, the risks to privacy are less clear-cut. Even so, in the absence of failsafe protections, vigilance will be the watchword.

Already, the government has embraced the next generation of computing. Often referred to as Web 2.0, this interactive world of user-generated online content and interpersonal engagement encompasses such phenomena as wikis, blogs and social networks. Public servants are already encouraged to communicate, network and share information through online tools such as departmental blogs and the GCPedia, launched in October 2008.

The Canadian public, meanwhile, is demanding access to ever more services over the Internet. Just as they buy books, shoes and furniture online, citizens expect to be able to pay their taxes, change their addresses and obtain government benefits at the click of a mouse. And, except when it cancelled its online passport application service, the government has been happy to oblige.

Audit of Government's Wireless Communications Underway

In work substantially completed during the reporting period, we examined how a sample of six government organizations that handle significant amounts of personal information managed their communications over wireless networks and devices such as cellphones and BlackBerry smartphones. We will report on this audit in our 2009-2010 annual report.

For now, it appears that the government has been able to meet its computing needs in-house. But, around the world, the trend is toward the outsourcing of data processing and storage to large private "cloud computing" providers, such as Google and Amazon. For Canadians, the trend raises challenging questions: Where in the world will the data be stored, and whose privacy laws would apply? Who would have access, and how would the data be defended against hackers, fire or other disasters?

Common Risks

As technical experts ponder these issues, the majority of risks that preoccupy our Office's complaints and privacy breach investigators are of a relatively lower-tech nature. Indeed, it is astounding how often, even in 2009, personal information is compromised by risks as old as the earliest computer punch card.

The following section describes cases of a technological nature that we closed in 2008-2009. They included a computer attack by an amateur hacker that threatened 60,000 personal data records, a case in which no one questioned why hundreds of people had untraceable access to certain government databases, and the disturbingly frequent theft of laptop computers and their sometimes sensitive contents.

Subsequent sections are devoted to other common risks we noted in 2008-2009, including inadequate or faulty data-management procedures, and basic human error. A final section describes efforts by our Office to reduce the backlog of complaint files.

Key Statistics

Most Common Complaint Types Closed

Difficulties gaining access to personal information	525
Concerns that an institution took too long to respond to a request for access to personal information	213
Concerns about an institution's use or disclosure of personal information	183
Other	69
Total	**990**

Top-10 Institutions by Complaints Received *

1	Correctional Service of Canada	249
2	Human Resources and Skills Development Canada†	129
3	Royal Canadian Mounted Police	67
4	Canada Revenue Agency	51
5	Canada Border Services Agency	31
6	Citizen and Immigration Canada	27
7	National Defence	25
8	Canadian Security Intelligence Service	23
9	Canada Post Corporation	22
10	Justice Canada	14

** The mandates of some of these institutions require them to hold a substantial amount of personal information about individuals. As a result, they tend to receive the most requests for that information, and are proportionately more likely to draw complaints.*

† Includes Service Canada and Social Development Canada

SPOTLIGHT ON CASES

Risk: Information Technology

1. ***Personal information leaked from DFAIT database***

In the spring of 2008, the media reported on the leak of personal information of a Canadian citizen being held in a foreign jail, prompting the government to apologize in Parliament for this violation of the *Privacy Act*.

Our investigation confirmed that the information in question had been held in the official consular record that is housed in the computer system of the Department of Foreign Affairs and International Trade (DFAIT).

Disturbingly, a total of 1,231 DFAIT employees had access to the files on this computer system, and the investigation could not determine which of them might have leaked the information to the media. There was no audit trail capability to show who accessed which records, or any mechanism to restrict access to particular files.

The complaint was determined to be well-founded.

As a result of our investigation, DFAIT agreed to:

- prepare better guidance on the sharing of personal information between departmental and ministerial officials, along with better documentation of requests for information and responses to those requests, and
- explore changes to its computer system to enable audit trails and restrict access to files.

2. ***Amateur hacks into Agriculture and Agri-Food Canada computers***

In September 2008, an Agriculture and Agri-Food Canada (AAFC) IT system administrator discovered that an external party had hacked into two Linux servers and installed modified e-mailing software. The evidence trail pointed to a "script kiddie" – an amateur who uses readily available malicious software to attack computer systems and networks, usually for kicks.

Though unsophisticated, the breach nevertheless threatened approximately 60,000 personal data records of agricultural producers who were recipients of the Advance Payments Program (APP), a federal loan guarantee program administered by third parties.

The exposed data included personal information such as names, addresses, phone numbers, loan amounts and repayments. While it was technically feasible to copy the data, AAFC found no evidence that this occurred.

As a result of this incident, AAFC took immediate action to assess the extent of the intrusion and to minimize further compromises to its systems. The department reviewed all firewall and e-mail logs for the two weeks before and after the intrusion, and removed any data from the APP secure copy server that was not required for immediate business needs.

The institution also continued to explore ways to reduce risk and to detect and mitigate incidents in a more timely fashion.

3. ***No proof Human Rights Commission accessed woman's Internet connection***

A woman complained that the Canadian Human Rights Commission (CHRC) improperly collected and used her personal information. She alleged that, in the course of an investigation, the CHRC accessed her wireless Internet connection to log on and post messages to a white supremacist website.

In response to a subpoena issued during the course of a Canadian Human Rights Tribunal public hearing, an Internet Service Provider disclosed the name, address and phone number of the Internet subscriber it associated with an Internet Protocol (IP) address that had allegedly been accessed by the CHRC during its investigation. The named subscriber was the complainant.

This Office has previously concluded that an IP address can be considered personal information if it can be associated with an identifiable individual.

However, our investigation found no evidence that the CHRC ever collected, used or disclosed any personal information about the complainant – or, indeed, even knew of her prior to the allegations made at the tribunal hearing. Technological experts suggested that the association of the complainant's IP address to the CHRC was simply a mismatch by a third party, which could have occurred in a variety of ways not involving the CHRC.

We concluded that the complaint was not well-founded. However, we cautioned Canadians to properly secure their Internet connections to avoid unauthorized access to their personal information.

4. *Software glitch at border services agency triggers data breach*

In response to an *Access to Information Act* (ATIA) request, the Canada Border Services Agency (CBSA) in March 2007 released a 52-page document that included one page containing personal information belonging to other individuals.

Due to a software problem, the personal information appeared on the computer printout, even though it had been severed in the electronic version. The individual who had requested the information returned the page.

A similar software problem had been reported in our 2007-2008 Annual Report, and CBSA was aware of the Treasury Board Secretariat's security policy alerts, issued in October 2007, with respect to vulnerabilities in the electronic release of information under ATIA and the *Privacy Act*. The agency had been working with the software vendor to try to address its information technology problems.

CBSA pledged to continue to work with the software vendor and review procedures to ensure that information severed pursuant to the ATIA or the *Privacy Act* is permanently removed. The agency also undertook to implement a manual quality assurance process of all information to be released under the two laws.

5. *Theft of laptops exposes personal information*

In 2008-2009, several federal departments and agencies reported the theft of laptop computers and flash drives containing the personal information of Canadians.

In one instance, a laptop was stolen from the Canadian Canola Growers Association, which administers a federal loan guarantee program for Agriculture and Agri-Food Canada (AAFC). The computer contained information on 31,160 applicants, including some businesses. Although the laptop was password protected and had a biometrics feature designed to limit access, it would have been possible to read the data by removing the hard drive and installing it on another computer.

As a result of that incident and our representations, AAFC developed and implemented:

- a new agreement for services provided by third parties;
- a comprehensive data-sharing agreement for third parties delivering AAFC programs, clarifying all roles and responsibilities under the *Privacy Act*;
- a privacy breach policy.

In another case, a break-in at a Service Canada building in Victoria where Canada Pension Plan and Old Age Security benefits are processed resulted in the theft of six laptop computers. Fortunately, only one contained client information, and it was encrypted.

Computers were also stolen from the residences of government employees. Some contained no personal information, but others held data on refugee and Employment Insurance claimants.

In any such incidents, our Office advises institutions to remind all employees of the importance of protecting the personal information of Canadians. If a laptop must be taken home, for instance, it should not be left in the car or other places where it can easily be stolen. Data, moreover, should be protected by encryption.

In the event of a breach, institutions have an obligation to notify all affected individuals. They should be counselled on protecting themselves against identity theft, and advised of their right to file a complaint under the *Privacy Act*.

Risk: Faulty Data-Management Procedures

1. *CIC challenged over indirect information-gathering procedures*

A Canadian citizen complained about the way Citizenship and Immigration Canada (CIC) collected the personal tax information it required from him in order to process a temporary-resident visa application submitted by his parents in Colombia.

The complainant stated that CIC's visa control office at the Canadian Embassy in Bogota required that Colombian applicants for a visitor's visa furnish specific supporting documentation, such as tax statements from relatives living in Canada.

The complainant did not dispute CIC's authority to collect information that established his financial solvency. However, he felt he should be able to provide the information directly to CIC, rather than by way of a third party, even if this was a family member.

The *Privacy Act*, in fact, backs him up. It states in Section 5 that the government must, wherever possible, collect personal information directly from the individual to whom it relates, unless the individual authorizes otherwise or disclosure is permitted under other provisions of the law.

This issue has come to our attention in previous complaints, dating back to 1998. Those complaints were determined to have been well-founded. However, our Office's recommendations had been ignored.

CIC has agreed to review its current procedures concerning the application process for Colombia and all 110 of the other countries where a temporary residence visa is required to enter Canada. Where necessary, CIC will amend its documentation to indicate that applicants may choose whether they will supply the supporting documents on behalf of their Canadian hosts, or whether the hosts will forward the documentation directly to the department.

2. ***VIA updates procedures after passenger finds manifest in recycling bin***

A traveller complained after he discovered a VIA Rail passenger manifest in a recycling bin at Toronto's Union Station. The passenger turned over to a manager the manifest, which identified travellers' names, reference numbers and other travel information. After hearing nothing back from the rail company, he complained to our Office.

Our investigation showed that the information printed on the document could allow unauthorized access to personal information, such as the addresses and phone numbers of people on the list. Credit card information would not, however, be compromised.

VIA made immediate changes to its procedures for handling passenger manifests and other documents containing the personal information of passengers. For instance, it directed all employees to shred such documents before recycling them.

Manifests now also carry a bilingual banner, reminding staff that the documents are confidential and must be returned to a VIA Rail office for destruction.

3. ***Sensitive letter leaked to media not treated as confidential***

In one case that came to our attention, a highly sensitive letter from a cabinet minister to a senior official had been properly designated as "Protected B – sensitive personal information," but was not handled in accordance with the Government Security Policy.

It remains unclear what happened next, but in the absence of adequate confidentiality safeguards, the letter was eventually leaked to a newspaper and republished widely across Canada.

An RCMP investigation and an internal review by the department, which is not being identified here in order to protect the identity of the subject of the letter, could not confirm the identity or the motive of the leaker.

In the wake of this incident, the department gave its records-management staff more training. The case underscores how important it is for public servants to understand their obligations under both the *Privacy Act* and the Government Security Policy.

4. ***Prisoner finds sensitive papers in garbage***

An inmate at the Saskatchewan Penitentiary turned over to an assistant warden a document he found in a garbage bin inside the prison. The document contained the names, prisoner numbers and work and other program assignments for 184 inmates. Seven of the inmates were identified as participating in sex offender programs.

Following this incident, penitentiary officials searched for other discarded documents but found none.

All inmates affected by the breach were informed of the incident and their right to complain to the Privacy Commissioner.

Prison officials directed an end to the practice of printing and distributing these types of reports.

5. ***Mail discarded after container mistaken for garbage bin***

Agriculture and Agri-Food Canada (AAFC) notified us of a privacy breach in Saskatchewan after a plastic container holding incoming mail was mistaken for a garbage bin and emptied into the trash. By the time the loss was discovered, the refuse had already been hauled to the Regina dump and the papers could not be recovered.

It is believed that 44 files containing applications to a crop protection program were among the discarded papers. The lost files included signed declarations and other personal information from clients.

AAFC was eventually able to contact 42 of the producers whose applications were thought to have been lost, in order to advise them of the incident. Our investigation turned up no indication that the papers were ever found or misused, but the potential for both remains.

As a result of this incident, mail is now processed on tables in the mailroom and stored for data entry in coloured and clearly marked plastic containers.

6. Personal data vanishes with government briefcases

It is not uncommon for our Office to be alerted to incidents in which a public servant's briefcase containing the personal information of Canadians is lost, temporarily misplaced or stolen.

Such situations may be very serious for Canadians whose personal information is compromised in the process. The losses, moreover, would be largely preventable if documents are simply left in secure premises.

More than a quarter-century since the passage of the *Privacy Act*, such breaches continue to underscore the need for vigilance in the handling of personal information by government employees.

In one notable case, a Justice Canada official on a business trip to Kingston, Ont. lost a briefcase containing the personal information of 145 taxpayers, including their social insurance numbers and some details of their investments in a tax shelter. The briefcase was not locked or secured and was never recovered by police.

The department informed the Canada Revenue Agency, which advised every affected individual in writing. Justice Canada also promised to train its employees about properly securing personal information.

In another case, the Canadian Institutes of Health Research (CIHR) advised our Office that documents containing personal information of about 63 medical professionals and students was lost from a briefcase carried aboard a domestic airline flight. The documents were never found but they are thought to have been discarded by cabin-cleaning crews.

CIHR informed the affected individuals of the incident and their right to file a complaint with our Office. The organization also pledged to review its policies, train staff and coach external experts who review grant applications, in the hopes of preventing similar breaches in future.

In a third incident, a briefcase containing paper documents was stolen from a car. It contained sensitive human resources information such as draft performance reviews of executives at Agriculture and Agri-Food Canada.

The affected individuals were notified and employees were furnished with secure briefcases equipped with combination or key locks.

7. *Thieves target important papers mailed by Canadians*

In last year's annual report, our Office reported on a comprehensive audit of the personal information-handling practices of Passport Canada, part of the Department of Foreign Affairs and International Trade (DFAIT).

The audit turned up privacy and security problems in passport operations that added up to a significant risk to Canadians applying for this vital identity document. Indeed, we found weaknesses at every step of the application process – the way in which personal information was collected and stored, how it could be accessed, and how it was ultimately disposed of.

Passport Canada and DFAIT agreed to most of our audit's 15 specific recommendations for strengthening the privacy management framework governing their passport operations.

Then, as the current reporting period drew to an end, issues with Passport Canada's online application process necessitated a shutdown of the service. A brief note on the agency's website stated: "Passport On-line is stepping aside for a new generation of interactive forms. The new forms . . . are more secure and easier to use."

During 2008-2009, however, the only three passport-related breaches that came to our attention were beyond the agency's control because they involved the theft of application packages from the postal systems in Alberta and British Columbia. An RCMP investigation led to an arrest and criminal charges against an individual.

Passport Canada advised the affected applicants of the theft. The agency also told them how to protect against identity theft, reapply for new birth certificates, and obtain reimbursement for lost fees and costs associated with the incidents.

The agency also continues to warn Canadians on its application forms: "The original documents that you enclose with your application are valuable. To ensure that these documents are not lost or misplaced, it is preferable to use a courier or mail service that allows you to trace your mail."

Mail theft victimized other departments and their clients as well last year. In one notable case, an RCMP investigation into an identity theft ring based at a Surrey, B.C. residence turned up extensive amounts of equipment and paraphernalia related to credit card fraud, along with 3,000 pieces of stolen mail – including 31 completed census questionnaires.

The individuals charged in this matter were not employees of Canada Post or Statistics Canada, which carries out the census. It is believed the census forms were obtained by tipping mailboxes or breaking into cars or homes.

The forms were returned to Statistics Canada, which wrote to each of the 31 affected households to explain the situation and provide an RCMP contact. Our Office reminded the agency that it should also have advised individuals of their right to file a complaint under the *Privacy Act*.

Risk: Human Error

Even with the best of intentions and seemingly solid procedures, the privacy rights of Canadians continue to be bedevilled by moments of sloppiness or inattention on the part of government employees. On 14 occasions, for instance, Public Works and Government Services Canada mailed exam results for public service staffing competitions to the wrong people.

But nowhere is the problem of human error more common than in the handling of information requested under the *Access to Information* or *Privacy Acts*, collectively referred to as ATIP requests.

Here are some of the cases that came to our attention in 2008-2009:

- The Department of National Defence (DND) sent a journalist a report that contained the names of 24 people who had made ATIP requests, including a summary of the nature of their requests. The names of people requesting information under freedom-of-information laws is considered personal information and may not be disclosed. After the reporter agreed to DND's request to return the document, officials accidentally sent the same report back to him a second time.

- Due to a printing glitch, duplicate pages attached to an information package sent by Environment Canada in response to an ATIP inquiry contained personal information of 41 other people.

- In response to an ATIP request, the RCMP inadvertently sent the recruiting information of one individual to another person with the same name.

- The names of a Public Works and Government Services Canada employee accused of fraud and his supervisor were inadvertently disclosed in response to an ATIP request.

No one will ever stamp out human error but, in the event of such accidental disclosures, certain rules apply.

Notably, the affected parties should be advised of the breach and their right to file a complaint with our Office. Depending on the circumstances, they may also benefit from information on how to remedy, or at least mitigate, the fallout from the breach.

In the wake of such breaches, departments have also implemented various strategies, most centred on training employees to become more vigilant about the importance of safeguarding personal information.

Changes to Investigations and Inquiries

The complaints our Office receives are becoming increasingly complex and require extensive investigation. Over time, our complaints-handling processes became overwhelmed and treatment times were getting longer.

On average in 2008-2009 it was taking nearly 20 months for a case to be closed, whether that meant it was discontinued, resolved, settled or became the subject of reported findings. That was up by 35 percent from the previous year, and left us with an unacceptable backlog of files.

To tackle this challenge, we opted for a proactive, multi-pronged approach that included outreach to selected departments and agencies and a wholesale re-engineering of our case-management processes.

By the end of the year, we were making gratifying progress and our backlog of complaints cases older than one year had decreased from 575 to 333, or 42 percent.

Proactive Approach

In addressing our workload issues, it was apparent that a big part of the solution would be to solve problems before they turned into complaints. Toward that end, our Office has been more actively engaged in outreach.

We met with the access to information and privacy (ATIP) co-ordinators of selected departments to help them fulfill their obligations under the *Privacy Act*. Along with the Office of the Information Commissioner, we hosted an ATIP Breakfast to promote networking among ATIP professionals and to explore ways for our two Offices to support them.

We were also reaching out to Canadians with a new online complaint form that has simplified the filing process, while giving us more complete and standardized information from which to launch our investigations.

And we have strengthened our ties with provincial and territorial privacy offices because we recognize we have much to learn from each other. In February 2009, for instance, we hosted our annual investigators conference in Ottawa, bringing together Information and Privacy investigators from across Canada. The two-day conference allowed investigators and inquiries officers to make new contacts, share experiences and exchange best practices.

In the shadow of our growing case backlog, we recognized the urgent need to re-engineer our internal processes in order to cope with the workload.

The initiative, which was designed in 2008 but is being rolled out over 2009, has several components. These include putting more hands on the job, a concerted effort to eliminate the backlog of unfinished business, and some new complaint-handling processes, backed by an improved computerized case-management system. These initiatives are described below.

More Human Resources

A new and experienced Director General joined the Investigations and Inquiries Branch in August 2008 and provided continued leadership for the re-engineering process.

A shortage of investigators has been a significant challenge for our Office. Numerous experienced *Privacy Act* investigators retired or otherwise left the Branch in recent years and they have been difficult to replace. Many organizations are vying for a small pool of access and privacy professionals, making recruitment and retention difficult. The use of outside resources can fill this gap.

The Backlog Blitz

Over the past year, we changed the definition of when a file is in backlog to more accurately reflect how long a complainant was actually waiting for service. Previously, we considered a file to be backlogged if there was not an investigator free to deal with it.

Under our new definition, a file is considered to be in backlog if more than a year has passed since the date of receipt. As a result of this change in definition, we restated the size of the backlog in April, from 370 unassigned files to 575 files that were more than one year old.

The new number, though higher, more accurately reflects levels of service to Canadians.

With a comprehensive re-engineering process already underway as described below, we also launched in June a 16-part "backlog blitz" to try to shrink the numbers in an orderly fashion.

For example, we grouped cases by federal department or complaint subject, and dealt with them together. We introduced a streamlined process for obtaining legal advice or review. And we committed to dealing with cases in the backlog before tackling any new ones.

Even as new cases continued to arrive at a rate of about 62 per month, we had, by the end of the fiscal year, managed to cut the backlog down by 42 percent, to 333 cases. We are on track to eliminate it by March 2010.

Re-engineered Processes

We have long recognized that we needed to retool our processes in order to keep on top of the thousands of complaints and inquiries we expect to continue to receive in the years ahead.

Toward that end, we are re-engineering our inquiries and complaint-handling processes in order to make them more streamlined and efficient. The retooled processes are being implemented in phases, and we expect them to be fully operational by fall 2009.

The new processes are supported by a computerized case-management system, which was implemented for our inquiries work in 2008 and will be rolled out for investigations in 2009.

A vital first step in the re-engineered process is to find a quick solution wherever possible. People who contact us with an inquiry or a complaint, for example, are encouraged to speak first with the institution, in order to explore ways to resolve their concerns.

Where direct talk doesn't resolve the issue and a complaint is made to our Office, we want to ensure it is handled efficiently and in a manner satisfactory to all. Our new online complaint form is designed to ensure that all the key information is provided, which in turn allows us to assess the complaint more efficiently.

Under our re-engineered procedures, a complaint is channelled first to our newly created position of Complaints Registrar. On the basis of the nature, complexity or urgency of the issue, the registrar will decide how the complaint will be handled.

Although some cases may be assigned directly to an investigator, the registrar will, wherever possible, try to send complaints for early resolution. Early Resolution Officers use negotiation, conciliation and other expert techniques to try to help the parties resolve their issues expeditiously. Cases that cannot be resolved in that way, however, may also be forwarded to an investigator.

FURTHERING PRIVACY RIGHTS IN CANADA

AUDIT AND REVIEW WORK

While much of our Office's work on audits and reviews of Privacy Impact Assessments (PIAs) in 2008-2009 focused on national security programs (see page 23), we also highlighted privacy issues inherent in other areas.

Auditing to Ensure Strong Protection of Personal Data

Privacy Management Frameworks of Selected Federal Institutions

In February 2009, our Office tabled a special report to Parliament that detailed the findings of an audit examining the privacy management frameworks of four federal institutions – Elections Canada, Passport Canada, the Canada Revenue Agency and Service Canada.

The purpose of the audit was to assess whether these agencies treat personal information in a manner that safeguards the privacy of Canadians. At the same time, the Auditor General's Office audited the same federal institutions to determine whether they work together to efficiently manage identity information and that they collect only information relevant to program needs.

We found shortcomings in two agencies' efforts to safeguard the personal information of Canadians.

Elections Canada

At Elections Canada, we concluded that gaps in the way the personal information of Canada's 23 million registered voters is governed could expose Canadians to serious consequences such as identity theft.

The audit found:

- Some voter lists simply vanished during elections and by-elections;
- Elections Canada collects too much personal information on voters, including on teenagers too young to vote, and
- Canadians are not fully informed about how their personal information will be used.

We identified concerns about the potential loss or misuse of information collected by Elections Canada and made available to political candidates, party staff and the tens of thousands of temporary poll workers hired at elections.

A key concern relates to the voter lists that are drawn up from the National Register of Electors and include not only names and addresses, but also birthdates. There is evidence that these lists go missing. As well, lists distributed to political parties and candidates can be endlessly photocopied and circulated.

We recommended Elections Canada develop policies to better track such electoral documentation, and that returning officers and poll workers be better trained to safeguard voter information.

Elections Canada committed to pursuing a range of risk-mitigating measures for the protection of elector information, including improved employee awareness mechanisms and stronger management oversight.

The *Privacy Act* does not apply to political candidates and parties. We recommended Elections Canada ensure that strengthened guidelines on the handling of voter information be conveyed to political party workers.

We were also concerned that Elections Canada was collecting information not required for the maintenance of its National Register of Electors. For example, although provincial licensing authorities routinely pass along driver names and addresses, their lists also included information such as whether a driver has had a licence suspension. Moreover, Elections Canada was collecting and using some personal information related to drivers too young to vote.

The *Privacy Act* requires federal institutions to collect only personal information related directly to their mandates.

The audit also raised concerns around meaningful consent. Taxpayers can check off a box at the end of their returns authorizing the Canada Revenue Agency to share with Elections Canada their name, address, date of birth and citizenship. However, tax filers aren't told how their information will be used. In particular, they are not advised that much of it will be provided to political candidates and parties, to be used for fundraising and marketing.

Passport Canada

Our Office had previously completed a separate audit of Canada's passport operations and published our findings in December 2008. (See the OPC's 2007-2008 Annual

Report to Parliament for details.) Last February, our observations with respect to Passport Canada's privacy management framework were republished as part of the four-agency audit conducted concurrently with the Office of the Auditor General of Canada.

In our 2008 examination of how Passport Canada and the Department of Foreign Affairs and International Trade handled passport applications, we identified a variety of shortcomings in procedures and controls that could pose significant privacy and security risks for Canadians applying for passports.

For instance, we found inadequate privacy training for passport employees – an issue of concern across government institutions. The audit recommended a number of changes to strengthen governance structures, policies and operations.

Further Findings

While the audits of the four agencies revealed some problems, it also identified strengths in the federal government's personal information management practices.

For instance, the audit of **Service Canada**, which manages the personal records of everyone who has applied for a Social Insurance Number (SIN), found sound policies to safeguard privacy, but noted they are not always followed in practice.

The **Canada Revenue Agency** has comprehensive controls, built up over many years throughout the organization, to safeguard the security of taxpayers' personal information, the audit found. However, the agency did not consider the privacy implications before automatically collecting the SIN information for between six and eight million children.

Departmental Annual Privacy Reports to Parliament

We also looked at federal departments' compliance with Treasury Board Secretariat requirements for the tabling of Annual Privacy Reports to Parliament.

These reports are intended to describe how each department carries out its obligations under the *Privacy Act*. They typically tally the number of requests received by the department under the *Act*, the exemptions invoked, the complaints received and a summary of the key issues. The reports are also intended to hold federal organizations accountable for the management of the personal information of Canadians through such activities as data matching, data sharing and privacy impact assessments.

We looked at the extent to which federal institutions were complying with Treasury Board Secretariat's reporting requirements for Annual Privacy Reports to Parliament.

In assessing compliance, we focused on the 2006-2007 Annual Privacy Reports for 25 federal organizations that handle a great deal of personal information, as well as another eight randomly selected organizations.

All but four of the 170 organizations required to table an Annual Privacy Report for 2006-2007 did so. Most of the 33 federal institutions that we examined complied with most, if not all, of Treasury Board Secretariat's mandatory reporting requirements.

However, many reports failed to provide anything beyond a very basic level of information. They did not provide a clear picture of either an organization's privacy practices, or its approach to managing the risks associated with personal information. Only three of the reports we reviewed described some of the privacy-protection measures in place, as well as how and why they were implemented.

Only 16 of the 33 organizations we surveyed made their annual reports available online. And, even when annual reports were posted, they were often difficult to find or out of date.

PIA Review: Assessing the Privacy Impacts of Government Programs

A Privacy Impact Assessment (PIA) is a tool to ensure that privacy is considered throughout the design or redesign of programs or services. It is used to identify and mitigate privacy risks.

The Treasury Board *Privacy Impact Assessment Policy* came into effect in 2002. Since then, our Office has reviewed some 385 PIAs, examining the collection, use, disclosure, retention and disposal of personal information by federal departments and agencies.

Our work with various government institutions in 2008-2009 continued to raise concerns that assessments are not always being undertaken in a timely manner.

Some programs – for example the Do Not Call List at the Canadian Radio-television and Telecommunications Commission (CRTC) – were launched *prior* to completing a PIA. As a result, our Office could not verify that privacy considerations had been taken into account during the design and implementation stages of the program.

In a 2006 audit, we raised serious concerns about the potential threats to privacy when PIAs are not completed prior to program implementation. Based on the PIAs reviewed since then, we have not found a significant improvement in departments' tendencies to proactively complete PIAs.

One positive trend in recent years has been for departments to invite members of our Office to take part in early consultation meetings to discuss privacy concerns associated with programs or policies. While this allows our office to identify potentially privacy-invasive programs prior to their implementation and to work with departments to identify risks from the outset, it does not replace the need for PIAs.

Due to staffing shortages, we accrued a backlog of PIA files waiting for review.

In an attempt to decrease this backlog, we have implemented a triage process where PIA files are now prioritized. This has allowed us to fast-track reviews of programs or initiatives that pose the greatest risk to Canadians' privacy.

Our Office does not approve PIAs or endorse projects - we make recommendations on how projects can be improved to better protect Canadians' privacy.

Under the government's PIA policy, federal departments are under no obligation to respond to, or implement, our recommendations. However, we have found that, much of the time, departments are receptive to our recommendations for improving privacy protections and the PIA process often has a very positive impact.

We've noted that an increasing number of departments are showing a higher level of engagement and cooperation during the PIA process. Although not all departments respond to the Office's advice formally through letters, many recommendations are given and received at all stages of PIA development through on-going consultation with departmental officials.

During 2008-2009, our Office received a total of 64 PIAs, which represents a slight increase from the 60 received in the previous reporting period, and completed 31 reviews. We received written responses to 62 PIA review letters (issued in either the current or previous fiscal year) – almost double the 32 responses received during the previous reporting period.

One of the PIA files we worked on involved Canada's new Do Not Call List. The list was established to help protect the privacy of Canadians who object to being called by telemarketers and our Office has been a strong supporter of this goal.

The list has also proven to be extremely popular with Canadians – so popular, in fact, that the program's website couldn't handle the rush of people trying to sign up on the day registration opened. As of the summer of 2009, nearly seven million telephone numbers had been registered.

However, as has been widely reported, some Canadians who placed their names on the list say they actually began receiving more unsolicited calls. The CRTC is conducting its own investigations into public complaints it has received.

Our Office has had a number of discussions with the CRTC about the list. The commission provided our Office with two PIAs related to the Do Not Call List on December 19, 2008. One focused on the operator of the list, Bell Canada, and the other on the CRTC's complaint procedures.

However, these PIAs were submitted three months *after* the list became operational.

When our Office reviewed the two PIAs, we identified a number of concerns. For example, the CRTC acknowledged a lack of formal processes, procedures, and documentation required to manage the personal information in the Do Not Call List program.

As well, we were not able to fully assess security risks as we did not receive a copy of the CRTC's threat and risk assessment.

We have requested a response to our initial concerns from the CRTC. At the time of writing this report, the CRTC had asked for an extension to the previously agreed-upon timeline for responding to our requests.

In our opinion, moreover, the CRTC might have been able to identify, evaluate and mitigate the majority of privacy risks associated with the program before the launch if it had conducted a PIA in the planning stages of the program.

We will continue to monitor this program and will attempt to work with the CRTC to ensure that privacy is a key consideration in the program going forward.

IN THE COURTS

Section 41 of the *Privacy Act* permits the Federal Court to review only a government institution's refusal to grant access to personal information requested under the Act. Review applications may not be made for a government institution's wrongful collection, use or disclosure of personal information.

In numerous representations to Parliament, our Office has recommended that the federal government broaden the grounds under which an application may be made for a court review under section 41.

In the meantime, as a result of the limited grounds on which an application may be made under the *Privacy Act*, we have, over the years, seen few applications proceeding to court. In 2008-2009, only a few cases of interest were before the Federal Court. They are described below.

In keeping with the spirit of our mandate, we do not publish the plaintiff's name in order to protect the privacy of complainants. The court docket numbers and the names of the respondent institutions, however, are provided.

Actions Against the OPC

X v. Privacy Commissioner of Canada
Federal Court File No. T-349-09

The application for judicial review sought to challenge the Privacy Commissioner's response to a complaint previously filed with our Office by the applicant. The complaint alleged an improper disclosure of personal information by the Public Service Staffing Tribunal in 2007.

The applicant filed a judicial review application seeking an order requiring our Office to exercise its jurisdiction and complete its investigation into the applicant's complaint.

Having nearly completed our investigation at the time the application for judicial review was filed, we subsequently provided the complainant with a final report of findings pertaining to his complaint. Accordingly, the applicant filed a Notice of Discontinuance in June 2009.

Interventions by the Privacy Commissioner

In the following cases, the Privacy Commissioner intervened in judicial review proceedings in which the applicants challenged decisions of the Public Service Commission to publish their personal information.

Both proceedings raise issues related to the application of the "open court principle" to decisions of administrative tribunals, as well as the interpretation of various provisions permitting government institutions to disclose the personal information of individuals without consent. (See page 11 for more information on this issue.)

In both instances, the applicants sought similar relief, which included, among other things, a declaration that the proposed disclosure of personal information contravenes the *Privacy Act*, and a writ of prohibition barring the Public Service Commission from disclosing the applicants' personal information.

Monsieur A. and Madame B. v. Attorney General of Canada
and Mr. X v. Attorney General of Canada
Federal Court File Nos. T-1256-08 and T-1257-08

Mr. X had been investigated by the Public Service Commission and found guilty of fraud in various public service hiring processes. In August 2008, Mr. X and certain relatives (Monsieur A. and Madame B.) filed separate Notices of Application, each initiating a judicial review of the Commission's decision to disclose sensitive personal information concerning Mr. X and his family in its annual report to Parliament. The Court agreed to consolidate the applications and hear them together.

Mr. X also sought and obtained leave from the court to proceed with the matter using a pseudonym and a broad confidentiality order permitting him to file confidential affidavit material.

By Order dated February 20, 2009, the Privacy Commissioner was granted intervener status to participate in the application and assist the Court to determine the legal issues with respect to privacy. However, the parties reached a settlement and the applications were discontinued on August 24, 2009.

X v. Public Service Commission
Federal Court File No. T-1659-08

The applicant was investigated by the Public Service Commission for allegedly engaging in improper political activities while employed as a federal public servant. The applicant filed an application for judicial review of the Commission's decision to disclose sensitive personal information about the applicant on the Internet.

The Privacy Commissioner was granted intervener status to participate in the application and assist the Court to determine the legal issues with respect to privacy. Following a period of inactivity, the matter is proceeding in accordance with a court-ordered timetable pursuant to which the Privacy Commissioner must file its written arguments on February 22, 2010.

ACCESS TO INFORMATION AND PRIVACY

This fiscal year marked only the second year in which our Office has been subject to both the *Access to Information Act* and the *Privacy Act*.

In addition to one request for records under the *Access to Information Act* that had been carried forward from the previous year, our Office received 28 new request for such records in 2008-2009. This was two fewer than the year before.

Another 48 access requests that we received in 2008-2009 were seeking records under the control of other federal institutions and were therefore redirected.

We completed 23 requests by the end of the fiscal year and six requests were carried forward.

We did not receive any complaints under the *Access to Information Act* during the fiscal year. However, the Information Commissioner's Office issued findings with respect to two complaints that had been carried forward from the previous fiscal year. One was concluded as "not substantiated" and the other was "resolved".

We also received 10 requests under the *Privacy Act* for personal information contained in documents under our control. We closed all 10 requests in the fiscal year.

THE YEAR AHEAD

The risks for privacy – and therefore the challenges for our Office – will undoubtedly continue to evolve in the year ahead.

Security issues continue to be a major concern for governments around the world and here in Canada. We can expect to see the development of new security initiatives that involve the collection and use of our personal information. A major issue in early 2010 will be the massive security operation at the Vancouver Olympics.

We will also continue to closely follow the Canadian Air Transport Security Authority's proposal to begin using scanners that can penetrate clothing as an additional option for secondary screening of airline passengers.

As well, we will be analyzing the privacy implications of legislative proposals to create an expanded surveillance regime (Bills C-46 and C-47). Consultations with law enforcement, national security authorities, telecommunications companies, privacy advocates and academics will help inform our analysis.

We will also be keeping a close eye on how new information technologies affect privacy rights.

We have set five broad priorities for our organization in 2009-2010:

- Continue to improve service delivery through focus and innovation.
- Provide leadership to advance four priority privacy issues (information technology, national security, identity integrity and protection, genetic information).
- Strategically advance global privacy protection for Canadians.
- Support Canadians and institutions to make informed privacy decisions.
- Enhance and sustain the organizational capacity.

Audit and Review

The audit and PIA review issues we have already begun, or plan to work on during 2009-2010 include:

- Complete an audit of wireless communications within the federal government to determine whether select government organizations have effective controls to protect personal information transmitted through wireless devices;

- Complete a three-year audit plan to guide our audit work to areas of greatest importance to Canadians and Parliament. We have always taken a risk-based approach to selecting organizations to audit, while also focusing on our strategic priorities. We intend to extend this process by broadening consultations both within and outside our Office to identify high privacy-risk organizations covered by either the *Privacy Act* or the *Personal Information Protection and Electronic Documents Act*;

- Review a Privacy Impact Assessment from the Canadian Air Transport Security Authority on its proposed use of whole body imaging technology in Canadian airports;

- Review PIAs from Citizenship and Immigration Canada related to a number of biometrics initiatives; and

- Review PIAs from the Canada Revenue Agency relating to its Integrated Revenue Collection project, which involves advanced data-warehousing and data-mining capabilities.

Investigations

The key priority issue for us in the coming year will be the elimination of the backlog of complaint investigations and the implementation of our re-engineered processes, which includes a new case-tracking system with an improved management information component to facilitate decision-making.

We expect that a reorganization within the Office, bringing our audit and review and our inquiries and investigations functions under the same Assistant Commissioner, will put us in a better position to identify and address systemic issues in the protection of privacy in the federal government's operations.

Legislative Developments

In the year to come, we anticipate being asked by Parliamentarians to turn our minds to a wide range of new legislation.

In terms of public sector privacy issues, a major focus will undoubtedly be on two bills introduced in June 2009 that would create an expanded surveillance regime with serious repercussions for privacy rights.

Bill C-46, the *Investigative Powers for the 21st Century Act*, and Bill C-47, the *Technical Assistance for Law Enforcement in the 21st Century Act*, give new powers to law enforcement and require telecommunications companies to comply with national security and law enforcement authorities' demands for subscriber data – even without judicial authorization.

The proposed legislation would give police authorities unprecedented access to Canadians' personal information.

Canadians put a high value on the privacy, confidentiality and security of their personal communications and our courts have also accorded a high expectation of privacy to such communications.

APPENDIX 1

DEFINITIONS OF COMPLAINT TYPES

Complaints received in the OPC are categorized into three main groups – Access, Privacy and Time Limits. Here are more detailed descriptions of each:

Access

Access – All personal information has not been received, either because some documents or information are missing or the institution has applied exemptions to withhold information.

Correction/Notation – The institution has failed to correct personal information or has not placed a notation on the file in the instances where it disagrees with the requested correction.

Language – Personal information was not provided in the official language of choice.

Fee – Fees have been assessed to respond to a *Privacy Act* request; there are presently no fees prescribed for obtaining personal information.

Index – Infosource (a federal government directory that describes each institution and the banks of information – groups of files on the same subject – held by that particular institution) does not adequately describe the personal information holdings of an institution.

Privacy

Collection – Personal information collected is not required for an operating program or activity of the institution; personal information is not collected directly from the individual concerned; or the individual is not advised of the purpose of the collection of personal information.

Retention and Disposal – Personal information is not kept in accordance with retention and disposal schedules (approved by the National Archives and published in Infosource): either destroyed too soon or kept too long.

In addition, personal information used for an administrative purpose must be kept for at least two years after the last administrative action unless the individual consents to its disposal.

Use and Disclosure – Personal information is used or disclosed without the consent of the individual and does not meet one of the permissible uses or disclosures without consent set out in sections 7 and 8 of the *Act*.

Time Limits

Time Limits – The institution did not respond within the statutory limits.

Extension Notice – The institution did not provide an appropriate rationale for an extension of the time limit, applied for the extension after the initial 30 days had been exceeded, or applied a due date more than 60 days from date of receipt.

Correction/Notation - Time Limits – The institution has failed to correct personal information or has not placed a notation on the file within 30 days of receipt of a request for correction.

DEFINITIONS OF FINDINGS AND OTHER DISPOSITIONS UNDER THE *PRIVACY ACT*

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

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

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

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

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

Resolved: After a thorough investigation, the OPC helped negotiate a solution that satisfied 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 OPC helped negotiate a solution that satisfied all parties during the investigation, but did not issue a 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.

APPENDIX 2

INVESTIGATION PROCESS UNDER THE *PRIVACY ACT*

Inquiry:
Individual contacts OPC by letter, by telephone, or in person to complain of violation of the Act. Individuals who make contact in person or by telephone must subsequently submit their allegations in writing.

Initial analysis:
Inquiries staff review the matter to determine whether it constitutes a complaint, i.e., whether the allegations could constitute a contravention of the Act.

An individual may complain about any matter specified in section 29 of the *Privacy Act* – for example, denial of access, or unacceptable delay in providing access to his or her personal information held by an institution; improper collection, use or disclosure of personal information; or inaccuracies in personal information used or disclosed by an institution.

Complaint?

No:
The individual is advised, for example, that the matter is not in our jurisdiction.

Yes:
An investigator is assigned to the case.

Early resolution?
A complaint may be resolved before an investigation is undertaken if, for example, the issue has already been fully dealt with in another complaint and the institution has ceased the practice or the practice does not contravene the *Act*.

Investigation:
The investigation provides the factual basis for the Commissioner to determine whether the individual's rights under the *Privacy Act* have been contravened.

The investigator writes to the institution, outlining the substance of the complaint. The investigator gathers the facts related to the complaint through representations from both parties and through independent inquiry, interviews of witnesses, and review of documentation. Through the Privacy Commissioner or her delegate, the investigator has the authority to receive evidence, enter premises where appropriate, and examine or obtain copies of records found on any premises.

Discontinued?
A complaint may be discontinued if, for example, a complainant decides not to pursue it, or a complainant cannot be located.

Analysis (on next page)

Settled? (on next page)

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

Analysis:

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

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

Settled?

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

Findings:

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

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

The possible findings are:

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

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

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

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

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

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

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

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

APPENDIX 3

INQUIRIES, COMPLAINTS AND INVESTIGATIONS UNDER THE *PRIVACY ACT*

April 1, 2008 to March 31, 2009

INQUIRIES STATISTICS

Inquiries Received	
By telephone:	1,770
Written (letter, e-mail, fax):	1,333
Total:	3,103

Inquiries Closed	
By telephone:	1,771
Written (letter, e-mail, fax):	1,105
Total:	2,876

General* Inquiries Received	
By telephone:	2,204
Written (letter, e-mail, fax):	284
Total:	2,488

General* Inquiries Closed	
By telephone:	2,206
Written (letter, e-mail, fax):	260
Total:	2,466

* These are inquiries about privacy issues that cannot be linked exclusively to either the public-sector *Privacy Act* or the private-sector *Personal Information Protection and Electronic Documents Act*.

COMPLAINTS RECEIVED BY COMPLAINT TYPE

Complaint Type	Number	Percentage
Access	282	38
Time Limits	254	34
Use and Disclosure	171	23
Collection	19	3
Correction-Notation	9	1
Retention and Disposal	6	<1
Correction-Time Limits	4	<1
Extension Notice	2	<1
Language	1	<1
Total	**748**	**100**

As in previous years, the most common complaints to our Office related to access to personal information, and to the length of time that government departments and agencies were taking to respond to access requests. See Appendix 1 for definitions of complaint types.

TOP-10 INSTITUTIONS BY COMPLAINTS RECEIVED

Organization	Total	Access to Personal Information	Time	Privacy
Correctional Service of Canada	249	70	149	30
Human Resources and Skills Development/Social Development Canada/ Service Canada	129	16	19	94
Royal Canadian Mounted Police	67	52	3	12
Canada Revenue Agency	51	28	11	12
Canada Border Services Agency	31	24	4	3
Citizenship and Immigration Canada	27	13	11	3
National Defence	25	9	8	8
Canadian Security Intelligence Service	23	12	11	0
Canada Post Corporation	22	8	13	1
Justice Canada	14	8	3	3
Others	110	42	28	40
Total	**748**	**282**	**260**	**206**

The number of complaints filed against an institution does not necessarily mean it is not compliant with the *Privacy Act*. Because of their mandate, some institutions hold a substantial amount of personal information. As such, they are more likely to receive numerous requests for access to that information which may, in turn, lead to complaints.

See Appendix 1 for definitions of complaint types.

COMPLAINTS RECEIVED BY INSTITUTION

Correctional Service of Canada	249
Human Resources and Skills Development Canada/Social Development Canada/Service Canada	129
Royal Canadian Mounted Police	67
Canada Revenue Agency	51
Canada Border Services Agency	31
Citizenship and Immigration Canada	27
National Defence	25
Canadian Security Intelligence Service	23
Canada Post Corporation	22
Justice Canada	14
Foreign Affairs and International Trade Canada	11
National Parole Board	10
Transport Canada	9
Indian and Northern Affairs Canada	7
Health Canada	6
Agriculture and Agri-Food Canada	4
Environment Canada	4
Office of the Information Commissioner of Canada	4
Privy Council Office	4
Public Service Commission Canada	4
Veterans Affairs Canada	4
Canadian Food Inspection Agency	3
Commission for Public Complaints Against the RCMP	3
Immigration and Refugee Board	3
Industry Canada	3
Public Safety Canada	3
Canadian Broadcasting Corporation	2
Canadian Human Rights Commission	2
Fisheries and Oceans	2
Natural Resources Canada	2
Public Works and Government Services Canada	2
Treasury Board of Canada Secretariat	2
Canadian Air Transport Security Authority	1
Canadian International Trade Tribunal	1
Finance Canada	1
Financial Transactions and Reports Analysis Centre of Canada	1
Inspector General of the Canadian Security Intelligence Service, Office of the	1
Marine Atlantic Inc.	1
National Research Council of Canada	1
Office of the Commissioner of Review Tribunals	1
Public Prosecution Service of Canada	1
Public Sector Integrity Canada	1
Public Service Labour Relations Board	1
Public Service Staffing Tribunal	1
Ridley Terminals Inc.	1
Social Sciences and Humanities Research Council of Canada	1
Statistics Canada	1
VIA Rail Canada	1
Total	**748**

COMPLAINTS RECEIVED BY PROVINCE/TERRITORY

Province/Territory	Total	Percentage
Ontario	178	24
Quebec	175	23
British Columbia	98	13
National Capital Region	98	13
Saskatchewan	67	9
Alberta	50	7
New Brunswick	26	3
Manitoba	23	3
Nova Scotia	12	2
International *	12	2
Newfoundland	5	1
Prince Edward Island	3	-
Nunavut	1	-
Total	**748**	**100**

* The right of access to personal information applies to Canadian citizens, permanent residents, inmates of a Canadian penitentiary and any other individual "present in Canada". These individuals have the corresponding right to complain to our Office concerning denial of access. Canadians living abroad have the same rights of access and complaint as those living in Canada, and some chose to exercise those rights in 2008-2009. The privacy protections contained in Sections 4 to 8 of the *Privacy Act*, related to the collection, use, disclosure, etc. of personal information, apply to all individuals about whom the government collects personal information, regardless of citizenship or country of residence. Any individual may complain to our Office about these issues.

DISPOSITION BY COMPLAINT TYPE

	Discontinued	Early Resolution	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Well-founded-Resolved	Total
Access	121	6	257	17	54	11	59	525
Time Limits	8	11	17	0	8	169	0	213
Use and Disclosure	38	20	47	1	19	45	13	183
Collection	10	5	13	0	8	2	0	38
Correction-Notation	6	0	5	0	3	0	0	14
Retention and Disposal	4	0	3	0	0	1	0	8
Correction- Time limits	0	0	0	0	0	5	0	5
Extension Notice	0	0	0	0	0	3	0	3
Language	0	0	0	1	0	0	0	1
Total	**187**	**42**	**342**	**19**	**92**	**236**	**72**	**990**

By their nature, time-limit complaints tend to be well-founded because most complainants only come to us after the statutory deadline for their complaint has passed.

Sixty percent of complaints about access to personal information were resolved early, settled in the course of investigation, or determined to be not well-founded. This indicates that the majority of complainants accepted that they could not receive the documents they were seeking because statutory exemptions had been properly applied.

Cases involving the collection, use and disclosure, or retention and disposal of personal information accounted for 23 percent of all complaints we investigated. Of those, only 27 percent were determined to be well-founded, or well-founded and resolved.

DISPOSITION OF ACCESS AND PRIVACY COMPLAINTS CLOSED

	Discontinued	Early Resolution	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Well-founded-Resolved	Total
Access	121	6	257	17	54	11	59	525
Use and Disclosure	38	20	47	1	19	45	13	183
Collection	10	5	13	0	8	2	0	38
Correction-Notation	6	0	5	0	3	0	0	14
Retention and Disposal	4	0	3	0	0	1	0	8
Language	0	0	0	1	0	0	0	1
Total	**179**	**31**	**325**	**19**	**84**	**59**	**72**	**769**

As in past years, significantly more of the complaints in the Access and Privacy categories were determined to have been not well-founded than well-founded.

In addition, 15 percent of these types of complaints were concluded through alternate resolution mechanisms – by resolving them early or settling them in the course of an investigation.

DISPOSITION OF TIME LIMITS COMPLAINTS CLOSED

	Discontinued	Early Resolution	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Well-founded-Resolved	Total
Time Limits	8	11	17	0	8	169	0	213
Correction-Time Limits	0	0	0	0	0	5	0	5
Extension Notice	0	0	0	0	0	3	0	3
Total	**8**	**11**	**17**	**0**	**8**	**177**	**0**	**221**

DISPOSITION OF TIME LIMITS COMPLAINTS BY INSTITUTION

	Discontinued	Early Resolution	Not well-founded	Settled in course of investigation	Well-founded	Total
Correctional Service of Canada	5	10	1	0	83	99
Service Canada	0	0	0	0	18	18
Canada Post Corporation	0	1	1	7	4	13
Canada Border Services Agency	0	0	0	0	12	12
Canadian Security Intelligence Service	0	0	8	0	3	11
Citizenship and Immigration Canada	0	0	0	0	10	10
National Defence	0	0	0	0	10	10
Canada Revenue Agency	0	0	2	0	5	7
Human Resources and Skills Development Canada/Social Development Canada	1	0	0	0	5	6
Foreign Affairs and International Trade Canada	0	0	0	0	6	6
Royal Canadian Mounted Police	1	0	1	0	2	4
Health Canada	1	0	0	0	2	3
Justice Canada	0	0	1	0	2	3
Privy Council Office	0	0	1	0	2	3
Transport Canada	0	0	0	0	3	3
Canada Public Service Agency	0	0	1	0	1	2
Immigration and Refugee Board	0	0	0	0	2	2
National Parole Board	0	0	0	0	2	2
Agriculture and Agri-Food Canada	0	0	1	0	0	1
Canadian Broadcasting Corporation	0	0	0	0	1	1
Indian and Northern Affairs Canada	0	0	0	1	0	1
Industry Canada	0	0	0	0	1	1
Public Prosecution Service of Canada	0	0	0	0	1	1
Public Works and Government Services Canada	0	0	0	0	1	1
Statistics Canada	0	0	0	0	1	1
Total	**8**	**11**	**17**	**8**	**177**	**221**

Correctional Service of Canada handles by far the most complaints of any department or agency in relation to the time it takes to respond to requests under the *Privacy Act*. One reason for this statistic is that the department holds large volumes of personal information about inmates, who in turn file numerous requests for their information. The department added significant resources last year to process requests, resulting in a 43-percent decline in its complaint load.

Other organizations that saw declines from last year in the number of time-limits complaints they were dealing with included the Department of National Defence, the Canada Border Services Agency, the RCMP, the Canada Revenue Agency and Justice Canada.

DISPOSITION OF ACCESS AND PRIVACY COMPLAINTS BY INSTITUTION

	Discontinued	Early Resolution	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Well-founded Resolved	Total
Correctional Service of Canada	38	2	68	4	19	11	8	150
Royal Canadian Mounted Police	17	1	49	5	13	7	9	101
Canada Revenue Agency	19	5	28	1	8	2	7	70
Service Canada	13	13	4	2	10	4	11	57
Canadian Security Intelligence Service	15	0	40	0	0	0	0	55
National Defence	11	0	21	1	3	4	5	45
Immigration and Refugee Board	2	0	28	0	0	3	6	39
Citizenship and Immigration Canada	9	1	13	0	5	3	0	31
Canada Border Services Agency	4	0	12	3	5	0	3	27
Foreign Affairs and International Trade Canada	3	4	7	0	0	6	3	23
Human Resources and Skills Development Canada/Social Development Canada	8	0	8	0	1	1	2	20
Canada Post Corporation	6	0	3	0	3	0	7	19
Canada Economic Development for Quebec Regions	13	0	0	0	0	0	1	14
Public Service Commission Canada	0	2	2	0	1	6	1	12
Transport Canada	0	0	8	0	1	0	1	10
Justice Canada	2	0	4	1	1	0	1	9
National Parole Board	0	2	4	0	0	1	2	9
Health Canada	4	1	2	0	1	0	0	8
Canada Firearms Centre	5	0	1	0	0	0	0	6
Environment Canada	0	0	2	0	2	0	1	5
Fisheries and Oceans	0	0	3	0	0	1	1	5
Veterans Affairs Canada	1	0	0	0	4	0	0	5
Agriculture and Agri-Food Canada	0	0	0	0	0	4	0	4
Library and Archives Canada	0	0	2	0	2	0	0	4
Canadian Human Rights Commission	1	0	1	0	0	0	1	3
Privy Council Office	1	0	1	1	0	0	0	3
Statistics Canada	1	0	2	0	0	0	0	3
Commission for Public Complaints Against the RCMP	0	0	2	0	0	0	0	2

DISPOSITION OF ACCESS AND PRIVACY COMPLAINTS BY INSTITUTION (cont.)

	Discontinued	Early Resolution	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Well-founded Resolved	Total
Industry Canada	1	0	1	0	0	0	0	2
Military Police Complaints Commission	0	0	0	0	0	2	0	2
Office of the Information Commissioner of Canada	1	0	0	0	0	1	0	2
Inspector General of the Canadian Security Intelligence Service, Office of the	1	0	1	0	0	0	0	2
Ombudsman National Defence and Canadian Forces	0	0	2	0	0	0	0	2
Pension Appeals Board Canada	0	0	0	0	0	1	1	2
Public Service Labour Relations Board	0	0	0	0	0	2	0	2
Public Works and Government Services Canada	0	0	1	1	0	0	0	2
Canadian Forces Grievance Board	0	0	1	0	0	0	0	1
Canadian International Trade Tribunal	0	0	0	0	1	0	0	1
Export Development Corporation	1	0	0	0	0	0	0	1
Finance Canada	0	0	1	0	0	0	0	1
Financial Transactions and Reports Analysis Centre of Canada	0	0	1	0	0	0	0	1
Indian and Northern Affairs Canada	0	0	0	0	1	0	0	1
Indian Residential Schools Resolution Canada	1	0	0	0	0	0	0	1
Natural Resources Canada	0	0	0	0	0	0	1	1
Office of the Commissioner of Review Tribunals	1	0	0	0	0	0	0	1
Public Safety Canada	0	0	0	0	1	0	0	1
Royal Canadian Mint	0	0	0	0	1	0	0	1
Treasury Board of Canada Secretariat	0	0	1	0	0	0	0	1
Vancouver Port Authority	0	0	1	0	0	0	0	1
VIA Rail Canada	0	0	0	0	1	0	0	1
Total	**179**	**31**	**325**	**19**	**84**	**59**	**72**	**769**

TREATMENT TIMES FOR COMPLAINT INVESTIGATIONS UNDER THE *PRIVACY ACT*

By Disposition

Disposition	Average in Months
Well-Founded Resolved	28.32
Discontinued	23.48
Not Well-Founded	23.47
Resolved	21.42
Settled in the Course of Investigation	19.24
Well-Founded	10.40
Early Resolution	4.40
Overall Average	**19.47**

Treatment times are measured from the date a complaint is received to when a finding is made or the case is otherwise disposed of.

Most complaints involving time limits are determined to be well-founded because people generally wait to complain to us until the statutory time limit for an organization to respond to their information request has expired. Since the time limits have been exceeded, these kinds of cases are generally straightforward and can be closed relatively quickly.

Because time-limit cases represent fully one-third of our caseload, the average treatment time for all well-founded cases is less than half that of not well-founded cases.

By Complaint Type

Complaint Type	Average Treatment Time in Months
Language	31.00*
Retention and Disposal	30.50
Access	24.48
Collection	21.74
Use and Disclosure	21.58
Correction/Notation	18.71
Correction/Time Limit	7.20
Time Limits	5.00
Extension Notice	2.67
Overall Average	**19.50**

* The treatment time for this complaint type reflects one case.