Office of the
Privacy Commissioner
of Canada

PRIVACY ACT

ANNUAL REPORT TO PARLIAMENT
2009-2010

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

(613) 947-1698, 1-800-282-1376
Fax (613) 947-6850
TDD (613) 992-9190

Cat. No. IP50-2010E-PDF
ISBN 978-1-100-14832-8

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

October 2010

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, 2009 to March 31, 2010. This tabling is done pursuant to section 38 of the *Privacy Act*.

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

October 2010

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, 2009 to March 31, 2010. This tabling is done pursuant to section 38 of the *Privacy Act*.

Sincerely,

Original signed by

Jennifer Stoddart
Privacy Commissioner of Canada

TABLE OF CONTENTS

COMMISSIONER'S MESSAGE

As I look back over the Canadian privacy landscape of 2009-2010, I am struck by a conflicting sense of satisfaction and unease.

I am proud of the efforts and accomplishments of my Office in helping to safeguard the personal information of Canadians in their dealings with the Government of Canada. As this report on the *Privacy Act* for the past fiscal year reveals, we do make a difference.

And yet, I am apprehensive about a future in which technological pressures and the imperatives of national security threaten to erode Canadians' hard-won rights to privacy.

It has become abundantly clear that we can neither indulge in complacency nor shy away from the challenges to come.

That is why this report is as much about process as it is about the work we did. In addition to accounting for my Office's activities during the 2009-2010 fiscal year, this report also describes the mechanisms being put in place to ensure that the organization stands ready to confront the privacy challenges of the new decade.

In this report you will find summaries of two major privacy audits that spotlight the specific challenges of protecting personal information in the context of evolving information technologies. One turned up troubling deficiencies in the privacy policies and practices governing federal public servants' uses of BlackBerrys and other mobile communications devices. The other reveals that surplus computers and paper documents are often disposed of without adequate regard for the personal information they may hold.

The report also highlights numerous investigations conducted under the *Privacy Act*, including one in which tax department employees had inappropriately accessed salary information of high-profile sports figures.

Reviews of Privacy Impact Assessments performed by federal departments and agencies preparing to introduce new programs or services are also of increasing interest to the

public. One Privacy Impact Assessment that garnered widespread attention related to the federal government's controversial rollout of 44 millimetre-wave full-body scanners at Canadian airports.

This report also contains overviews of several major initiatives that preoccupied us over the past year, where national security demands encroached on the privacy rights of Canadians. Key among those were the massive security cordon surrounding the Vancouver Olympic and Paralympic Games, the many new security measures affecting international travellers, and a series of legislative initiatives aimed at strengthening the hand of authorities using the Internet to combat terrorism and crime.

CHALLENGES REMAIN

While I am pleased to know that my Office has made an impact on these important fronts, the undeniable truth is that vast challenges remain. Evolving technologies, global data flows, increased surveillance, and the government's thirst for personal information mean our work is never done.

And so, against this backdrop, my Office was also taking steps to bolster our capacity to advocate for privacy rights in the years ahead.

The Office recognizes that, among other things, this will demand changes in the way we use our resources. That is why we focused on eliminating our complaint investigation backlog, streamlining our complaints handling processes, and selecting audits and Privacy Impact Assessments on the basis of their relative risks to privacy.

In 2009-2010, the government quashed hopes for a legislative overhaul of the *Privacy Act* in the near term. I do, however, remain optimistic that the 27-year-old law will eventually undergo a much-needed rejuvenation. In the interim, my Office is working with the Treasury Board of Canada Secretariat on administrative measures to further strengthen privacy protections for Canadians.

Because it is better to prevent a privacy intrusion than to lament it after the fact, my Office has also intensified efforts to communicate with government officials who handle the personal information of Canadians. Thus, for instance, we held formal and informal talks with senior officials to address systemic issues, made site visits to departments and agencies that receive more public complaints than the norm, and hosted a workshop on the effective preparation of Privacy Impact Assessments.

In other outreach activities, we also had 59 interactions with MPs and Senators at Parliamentary committees and in other settings, and developed a publication to help Canadian travellers navigate the myriad security measures at airports and border

crossings. And we continued to engage with counterparts around the world to ensure that the privacy rights of Canadians will be protected in an increasingly globalized world.

Meantime, I have emphasized the importance of fortifying the level of expertise that exists within the Office on such emerging priorities as information technology, genetic technology, identity integrity and, of course, the often-elusive integration of national security and privacy.

In that context, I want to pay tribute to Assistant Commissioner Chantal Bernier for her peerless leadership on public-sector privacy issues. She has expertly shaped and guided our approach to privacy protection in the face of emerging technologies and new security measures. By concentrating on the underlying principles, Ms. Bernier has reinforced our relevance and maximized our influence.

Without question, this Office has a firm and realistic grip on the challenges ahead, and is well positioned to confront the future with purpose and conviction. For today, though, this report looks back on the year that was, to tell the story of our journey through 2009-2010.

I am honoured to share it with Parliamentarians and all Canadians.

PRIVACY BY THE NUMBERS – 2009-2010

Inquiries and Complaint Investigations		
Total inquiries received:		10,907
Inquiries linked to the *Privacy Act*	2,572	
Inquiries linked to the *Personal Information Protection and Electronic Documents Act* (PIPEDA)	5,467	
Inquiries that could not be linked exclusively to the *Privacy Act* or PIPEDA	2,868	
Privacy Act complaints received		665
Privacy Act complaints closed		1,154
Audit and PIA Reviews		
Public-sector privacy audits:		2[1]
Privacy Impact Assessment submissions:		
Received		102
Reviewed		33
Legal, Policy and Parliamentary Affairs		
Legal opinions related to the *Privacy Act*		10
Litigation under the *Privacy Act* – decisions rendered		2
Litigation under the *Privacy Act* – cases settled		1
Public-sector policies or initiatives reviewed		61
Policy guidance documents issued		18
Draft bills and legislation reviewed for privacy implications		10
Parliamentary committee appearances made		14
Other interactions with Parliamentarians or staff		45
Other OPC Activities		
Formal visits from external stakeholders		56
Speeches and presentations		164
News releases and communications tools		61
Media interviews		318
Exhibits and other offsite promotional activities		11
Publications distributed		16,207
Visits to principal OPC website		2.06 million
Visits to OPC blogs and other websites		1.06 million
New subscriptions to e-newsletter		304
Access to Information Act requests received		26
Access to Information Act requests closed		31
Privacy Act requests received		16
Privacy Act requests closed		15

[1] Three other audits were completed in 2009 and were already reported in the OPC's *2008-2009 Annual Report to Parliament*.

CHAPTER 1: THE PRIVACY LANDSCAPE

Key Accomplishments in 2009-2010

1.1 SERVING CANADIANS

PUBLIC INQUIRIES

Canadians phoned or wrote to our Office nearly 11,000 times during the 2009-2010 fiscal year. In about one-quarter of the cases, they were inquiring about issues that fell clearly within the purview of the *Privacy Act*. Just as often, the matter fell under the private-sector *Personal Information Protection and Electronic Documents Act*, or PIPEDA. For the remaining half of the inquiries, the issue of concern could not be pinned exclusively to either the *Privacy Act* or PIPEDA.

For matters related to the Government of Canada (and therefore falling under the *Privacy Act*), people contacted us for a wide variety of reasons. One concern, common also in other years, related to the perceived over-collection of personal data and, in particular, the Social Insurance Number. New this year was a modest spike in apprehension about the government's no-fly list and the body scanners introduced at airport security checkpoints.

We put considerable effort into resolving inquiries by providing people with information or directing them to appropriate contact persons or resources. In addition to responding to PIPEDA-related inquiries, we addressed 5,521 inquiries relating specifically to the *Privacy Act*, or where it was unclear which Act applied. This represented a slight increase from the year before.

For more information, see section 4.1.

PUBLIC COMPLAINTS

Our emphasis on resolving issues at the front end helped trim by 12 percent the number of formal complaints registered with our Office. We received 665 complaints related to public-sector issues in 2009-2010, compared to 748 the year before.

Over the past fiscal year, we also refined our efforts to resolve complaints quickly, without the need for a formal investigation. Toward that end we designated an early-resolution officer, who helped complainants find satisfactory solutions to their concerns.

For example, the officer is often able to close a file simply by informing the complainant about similar cases we have investigated in the past. If the department in the earlier cases was found to have complied with the *Privacy Act*, complainants will often accept that there is no point in proceeding.

Some complaints about access to personal information are also resolved when the early-resolution officer is able to show that a department that had declined to release the information was actually correct in its use of statutory exemptions.

In all, 161 complaint files were closed to the satisfaction of complainants in 2009-2010, either before an investigation was launched or because the matter was settled during the course of the investigation. Another 149 cases were discontinued, usually by the complainant, before an investigation was completed.

As in other years, the majority of complaints we received related to problems people encountered in gaining access to their personal information in the hands of government (38 percent of all complaints), or to the time it took for institutions to respond to requests for that information (44 percent).

Complaints about the collection, use, disclosure, retention or disposal of personal information comprised the remaining 18 percent of complaints.

COMPLAINT INVESTIGATIONS

We closed 1,154 complaints under the *Privacy Act* in 2009-2010, up 17 percent from 2008-2009. Significantly, we closed 489 more complaint files than we opened and, in the process, were able to eliminate virtually our entire backlog of unresolved complaint files older than a year.

Eliminating the backlog has been a priority for our Office, and Parliament gave us dedicated funds to achieve this target. At the start of the fiscal year, we had 333

backlogged *Privacy Act* files, down from a high of 595 in 2007. By March 31, 2010, all but 10 had been closed.

Nearly half of the files we closed related to concerns about access to personal information, but investigations revealed that nearly half of those were not well founded.

By contrast, we upheld as well founded nearly 85 percent of the 314 complaints related to the time it took for government institutions to respond to requests for personal information.

Complaints about privacy, including the inappropriate collection, use or disclosure of personal information, comprised only one-quarter of our closed case files. In 43 percent of these cases, however, the allegations were substantiated.

In the course of our investigations, we continued to be troubled by a risk factor that recurs year in and year out: The mishandling of personal information. This is most commonly traced back to simple oversight, inadvertence, or inadequate procedures. We did, however, also encounter plain wrongdoing.

As in other years, there were also instances in which we were able to pin the problem on technology – whether a programming malfunction, inadequate protection of data, or ordinary mechanical equipment failure.

In an effort to stem the more systemic problems, we invested substantial efforts in prevention. For instance, we met with departments and agencies to foster a better understanding of their challenges and our expectations for the protection of personal information. We also underscored the importance of notifying us of data breaches.

More information on our complaints investigation work can be found in section 4.2 of this report, and highlights of our investigations follow in section 4.3.

PUBLIC AWARENESS

Over the course of the year, Commissioners and other officials of our Office delivered 164 speeches, many of them on public-sector privacy matters, and conducted numerous media interviews on such issues as aviation security and the proposed surge in police powers to track terrorists and criminals over the Internet.

We also prepared and distributed a range of communications products, such as calendars and fact sheets. One popular publication, for example, aimed to help international travellers understand the privacy implications of the many security measures at airports

and border crossings, and to inform them of their options for redress. We also produced a booklet highlighting our key policy priorities.

We made extensive use of our website, which we improved and relaunched in April 2009.

1.2 SUPPORTING PARLIAMENT

APPEARANCES BEFORE MPs AND SENATORS

During 2009-2010, our Commissioners and other officials of the Office made 14 formal appearances before MPs and Senators. Issues under consideration included:

- reviews of Canada's *DNA Identification Act* and *Sex Offender Information Registration Act*
- amendments to the *Criminal Code* to target identity theft
- new legislative initiatives such as the proposed *Electronic Commerce Protection Act,* the *Canadian Consumer Product Safety Act,* and the *Human Pathogens and Toxins Act*
- the proposed restructuring of Canada's oversight regime for national security agencies and privacy implications for the wireless communications sector
- aviation security
- reform of the *Privacy Act*.

LAWFUL ACCESS

One of the most significant legislative initiatives we examined during 2009-2010 was a package of bills that collectively aimed to alert authorities to illegal online activities, give police tools to preserve online data as evidence, allow investigators to trace digital transactions and communications, and ensure that police and security agencies are able to intercept a new generation of communications.

The legislation aimed to create an obligation for Internet service providers to disclose subscriber information (such as names and addresses) to police and national security officials on request.

While we acknowledge the challenges faced by law enforcement authorities at a time of rapidly changing communications technologies, we also felt strongly that the privacy implications of the proposed legislation required careful consideration.

Echoing serious questions expressed in a joint resolution by privacy commissioners and ombudsmen from across Canada in September, the Commissioner conveyed her concerns in a letter to Parliamentarians in October.

The two central pieces of legislation, referred to as Bills C-46 and C-47, were first introduced in June 2009 but died at prorogation in December. However, since variations of the idea have been raised from time to time over the years, we expect them to be reintroduced in the new Parliamentary session.

A more detailed discussion of the lawful access legislation and our concerns can be found in section 3.3.

LEGISLATIVE RENEWAL

We continued in 2009-2010 to try to persuade Parliament that the *Privacy Act*, enacted in 1983, is out of date and in urgent need of modernization. We won some support for this view from the House of Commons Standing Committee on Access to Information, Privacy and Ethics, which in June 2009 issued a report titled *The* Privacy Act*: First Steps Towards Renewal*.

Our position was not, however, shared by the Minister of Justice, who stated in his response to the committee report that existing privacy protections under the *Privacy Act* and the *Canadian Charter of Rights and Freedoms* are sufficient.

We subsequently turned our focus to the development of administrative measures that, in the absence of legislative amendments, could advance our objectives of strengthening public-sector privacy rights.

These measures include grounding Privacy Impact Assessments in public law, increasing privacy training among public servants, and making data breach notification the norm across government.

A summary of our proposed administrative changes can be found in section 3.4.

1.3 SUPPORTING FEDERAL GOVERNMENT INSTITUTIONS

DEPARTMENTAL DIALOGUE

In 2009-2010 we had many bilateral talks aimed at strengthening understanding between our Office and officials at federal departments and agencies.

Discussions with institutions such as Citizenship and Immigration Canada, the Correctional Service of Canada and the Canada Border Services Agency helped ensure that key privacy principles are woven into the fabric of federal initiatives. These principles include minimizing the collection of personal information, ensuring it is collected for justifiable reasons, limiting its use, safeguarding it, and disposing of it securely when it is no longer needed.

We also embraced opportunities to address gatherings of access to information and privacy officials, and hosted an inaugural workshop on improving the quality and effectiveness of Privacy Impact Assessments.

OLYMPIC AND PARALYMPIC GAMES

The Vancouver Olympic and Paralympic Games, which took place in British Columbia in February and March of 2010, were the first "mega-event" to be held in Canada since the 9/11 terrorist attacks on the United States.

While organizers were understandably concerned with security at the Games, our Office monitored the activities of security and law enforcement officials to ensure that the privacy rights of spectators, athletes, employees and volunteers were respected.

We tracked the security planning and implementation activities, and liaised regularly with the RCMP-led Integrated Security Unit.

The working relationship with security officials began in early 2009. By the summer, we had created on our website a dedicated access point for documents and research on the privacy impacts of mega-events such as the Olympics. The page featured a fact sheet setting out principles to guide Games security officials in discharging their duties in a way that would not unduly infringe on the privacy rights of individuals.

At the conclusion of the Games, we were satisfied that the security authorities had understood their obligations under the privacy law. It is our hope that the experience gained by law enforcement and national security agencies in upholding privacy rights during the Games will continue to be applied at major national and international events in Canada.

For more information, see section 3.2.

WIRELESS AUDIT

One way we support federal institutions is by verifying that they have the policies, procedures, practices and controls in place to safeguard the privacy and personal information of Canadians. After all, the government collects and holds some exceptionally sensitive information, from tax records and income support entitlements to travel patterns and immigration and refugee claims.

Thus, in 2009-2010, we examined whether four major departments and one agency had adequate privacy safeguards in place for wireless networks and mobile communications devices such as BlackBerrys.

We found that none of the five entities had fully assessed the threats and risks inherent in wireless communications. Three of the four wireless networks we examined afforded the recommended level of encryption. Only three of the organizations required strong password protection for smart phones, and none insisted that data stored on the devices be encrypted.

We also found significant weaknesses in the management of surplus mobile devices, and only one of the audited organizations could demonstrate that current measures provide assurance that all phones are wiped of data before being sent for disposal.

A condensed version of our full audit report can be found in section 2.1.

DISPOSAL AUDIT

In a second privacy audit undertaken in 2009-2010, we sought to determine whether selected departments and agencies complied with the rules and procedures for the disposal of paper documents, as well as for surplus computers and other information technology equipment. This is important in light of the vast amounts of personal information held in the government's paper and electronic files.

We found that, while many satisfactory policies and procedural rules were in place, there were some disturbing deficiencies in practice.

For example, we tested a sample of nearly 1,100 surplus computers that 31 federal departments and agencies had donated to the Computers for Schools program. We found that devices donated by 90 percent of the sample institutions had not been thoroughly wiped of data. Indeed, confidential, highly sensitive and even classified data remained on many of the computers we tested. Some was so sensitive that we had the devices immediately returned to their originating department.

Although there are strict policies governing document shredding and disposal, our investigation revealed that the private companies carrying out the work under contract with the government were not well supervised. Without adequate oversight, two of the four companies we examined had, at some time, violated their contractual obligations. Indeed, at one site there were such clear violations of security rules that the company's security clearance was suspended until the deficiencies were addressed.

A condensed version of our full audit report can be found in section 2.2.

PRIVACY IMPACT ASSESSMENTS

Our Office works with departments and agencies to ensure that privacy protections are taken into account at the earliest possible stages of policy development, and continue to be rigorously observed as programs are implemented and services delivered.

Privacy Impact Assessments have become an important tool to help departments and agencies build privacy protections into new programs and services in a manner that is transparent to the public.

Federal policy requires institutions to submit such analyses to our Office. We do not, however, approve them or endorse projects. Instead, we review the assessments and may recommend ways to improve projects to better protect Canadians' personal information.

We do not have authority under the *Privacy Act* to force institutions to implement our recommendations. Even so, we find that institutions generally work with us to resolve privacy concerns.

We received 102 Privacy Impact Assessments in 2009-2010, up dramatically from 64 the year before. Following a rigorous triage process aimed at focusing our resources on initiatives that posed the greatest potential privacy risk and/or fell into one of our Office's four key priority areas, we completed reviews on 33 of the submissions.

Major Privacy Impact Assessment reviews we conducted are summarized in section 2.3.

CATSA PRIVACY IMPACT ASSESSMENT

One of the most high-profile public-sector issues we addressed in 2009-2010 emerged from a Privacy Impact Assessment we received from the Canadian Air Transport Security Authority (CATSA). It related to a controversial new airport security screening technology that creates images of travellers through their clothes.

CATSA first consulted with us on the scanner technology in September 2007. Following a 2008 pilot project in Kelowna, B.C., CATSA in 2009 submitted to our

Office a Privacy Impact Assessment that related to a full rollout of 44 of the machines in January 2010. The extensive interaction with our Office served to address or minimize our principal privacy concerns.

Indeed, the resulting proposal to employ the machines as optional secondary screening instruments with no data retention set an early standard internationally.

A more complete description of our work on the full-body scanners can be found in section 3.1.

MODERNIZING THE PROCESSES

Given the scope of our jurisdiction over all federal departments and agencies, our Office focused in 2009-2010 on developing a more rational and systematic approach to our audit and Privacy Impact Assessment review processes.

In consultation with government, academics and other stakeholders, we developed a risk-based audit plan that will focus our resources on programs and departments that hold the largest amounts of sensitive personal information.

In light of a 60 percent increase in Privacy Impact Assessments coming through our doors over a single year, we are also applying a triage approach to our review and analysis processes. Thus, Privacy Impact Assessments for initiatives posing the greatest risk to the privacy of Canadians, or those aligned with our Office's leading privacy concerns, went to the front of the line.

In January 2010, our Office also hosted an inaugural workshop to help federal employees better understand our expectations for Privacy Impact Assessments. The event drew 90 participants and, by the end of the fiscal year, a written summary of our expectations was being readied for distribution across the government.

We have also been reorganizing the Office by uniting our Investigation and Inquiries Branch and our Audit and Review Branch under the same Assistant Commissioner. The aim is to increase synergies in our compliance functions, with a view to more effectively pursuing systemic issues raised by public complaints.

More information on these transformations can be found in section 2.4.

FEDERAL ADMINISTRATIVE TRIBUNALS

Our Office has long been concerned when federal administrative tribunals and quasi-judicial bodies post to the Internet decisions containing extraneous personal

information. The challenge of balancing openness and privacy in the Internet age continues to prompt inquiries and complaints.

These administrative bodies consider issues such as the denial of pension and employment insurance benefits, compliance with workplace rules and professional standards, allegations of regulatory violations, and challenges to federal public service hiring processes. Tribunal decisions posted publicly often contain personal details, such as salaries and health problems, which many people would not feel comfortable sharing widely.

We accept that there are instances in which the public has an interest in knowing the identities of individuals who are the focus of tribunal proceedings. In the majority of cases, however, we believe that an appropriate balance can be struck between transparency and openness without publishing people's identities on the Internet.

In 2009-2010, we moved to further clarify our position and to explain the application of the *Privacy Act* to administrative tribunals. In consultation with our provincial and territorial counterparts, we developed guidelines aimed at helping tribunals fulfill their mandates and serve the public interest, while remaining compliant with the Act.

Details on these efforts can be found in section 4.7.

GUIDANCE FOR ONLINE GOVERNMENT

Government employees are being encouraged to embrace innovative online tools to enhance performance and connect with Canadians. Thus there is an increasing use of departmental blogs, wikis such as GCPedia, and social media and other networking platforms such as GCConnex. Even Twitter and YouTube are gaining a toehold in Canada's public service.

Our Office continues to work with the Treasury Board Secretariat and other government departments to develop policies and guidelines that will help federal institutions move into the online and collaborative world in a way that preserves fundamental values such as privacy.

PRIVACY BENCHMARKS

The Treasury Board Secretariat has also been drawing up privacy benchmarks and guidance for the entire federal public sector. Our Office has been engaged in the peer review process for this material, which includes a revised policy on privacy protection, improved statistical reporting on *Privacy Act* compliance in departmental and agency annual reports, and new guidance on personal information-sharing agreements between Canadian government organizations and partnered departments and agencies abroad.

We welcome this focus on strengthening safeguards for personal information and privacy, particularly in the increasingly digital, networked environment in which the modern government operates.

1.4 ADVANCING KNOWLEDGE

NATIONAL SECURITY WORKING GROUP

Our Office has had a longstanding interest in the privacy issues raised by national security measures. We appeared at the O'Connor Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar in 2005, and again at the Major Inquiry into the investigation of the bombing of Air India Flight 182 in 2007.

Citizens' rights to privacy in the context of national security, and the ideal legal safeguards for both, remain at the forefront of government decision-making. These issues also go to the heart of our organizational mandate.

To highlight the privacy issues raised by national security programs in Canada and abroad, our Office established an internal working group of staff with expertise in the fields of audit and review, law, investigations, information security, intelligence studies, and security review and oversight.

With the help of briefings from national security experts, the group contributes to the Office's overall knowledge of the field. This investment of effort has allowed us to move quickly on emerging files. For example, by reviewing international developments in national security law and programs and examining Canada's own model, we were able to recommend to Parliament ways to improve oversight and review mechanisms across Canada's intelligence and security community.

GENETIC PRIVACY WORKING GROUP

Controlling who has access to our genetic information and how it is used is emerging as one of the critical privacy issues of the 21st century. That is why our Office has identified genetic privacy as one of four strategic priorities that will help guide our policy, research, public education and investigative work over the next several years.

During 2009-2010, we participated in Parliament's review of the *DNA Identification Act*. We appeared before House of Commons and Senate committees to express concerns about proposals to expand the national DNA database by taking samples from more offenders for a broader range of offences, allowing "familial searches", and increasing international information sharing.

We also co-sponsored with Genome Canada a workshop on privacy issues that arise when biological samples are collected and then banked for genetic research. We helped organize a second workshop on the possible use of genetic information by insurers and employers. A third workshop on direct-to-consumer genetic testing was held after the end of this reporting period.

These workshops brought together federal policy-makers, researchers, academics and other stakeholders to explore public policy issues related to the growing availability of genetic information. The events generated policy options papers that will serve as a reference for policy-making in the field. They are available online at http://www.genomecanada.ca/en/ge3ls/policy-portal/directions.aspx

IDENTITY INTEGRITY WORKING GROUP

Governments today collect and share ever more personal information, often for reasons associated with national security or public safety. The amount of information that can be collected, cross-matched, shared and stored accelerates with every new technological innovation.

Many Canadians ask to see their personal information held by government, each for his or her own reason. Some are simply curious to know what is known about them, while others wonder why they are receiving unwanted attention from a government agency.

Our Office set up an Identity Integrity Working Group that, among other things, is seeking to better understand the forces behind the escalating collection of personal information. The group is also exploring how Canadians react to repeated attempts to collect their personal information, and examining standards and frameworks to give individuals more control over their own data.

INFORMATION TECHNOLOGY AND PRIVACY WORKING GROUP

A growing number of Canadians are choosing to engage with the federal government through electronic means. Within the government as well, public servants are being encouraged to interact, network and blog, to build online teams and interdepartmental working groups, and to contribute knowledge to digital resources.

One factor driving these trends is the rapid development of information technologies. Within this context, our Office's Information Technology and Privacy Working Group studies developments that could have an impact on privacy.

During 2009-2010, the group invited experts to help them explore new technologies and their implications for privacy. A key focus was geospatial technologies and their

potential to disclose the identities of individuals from supposedly anonymous or de-identified data sets.

The group also shared their learning with other OPC staff through a series of presentations on topics such as malicious code and botnets.

IT RESEARCH ANALYSTS

Many of the complaints we receive from the public involve technological issues. To help us deal with the most complex ones, we established in 2009-2010 a small team of information technology research analysts.

Their job is to analyze and evaluate information and communications technologies and their implications for privacy policy, the privacy rights of Canadian citizens, and the legislated mandate of the OPC.

The team then advises senior management and other OPC staff in relation to investigations and inquiries, audits and Privacy Impact Assessment reviews, and reviews of proposed legislative and policy changes. Their work also supports appearances by the Commissioner and other senior staff before Parliamentary and other audiences.

1.5 GLOBAL INITIATIVES

OVERVIEW OF OPC EFFORTS

We live in a world where dramatic advances in information and communications technologies are launching unimaginable volumes of personal information around the globe. Like other data protection authorities, we have an interest in ensuring that this personal information is adequately protected when it moves across borders.

During 2009-2010, our Office continued to work on global privacy solutions in collaboration with international organizations and data protection authorities from other nations.

In an increasingly interrelated world, effective privacy protection for Canadians requires robust privacy standards and mechanisms to facilitate co-operation among enforcement authorities. We believe we can help achieve these goals by being involved internationally.

Here are some of the highlights of our work in this area:

THE SPANISH INITIATIVE

At the 31st International Conference of Data Protection and Privacy Commissioners in Madrid in November 2009, the world's data protection authorities endorsed a Draft International Standard on the Protection of Privacy.

The draft standard was developed by an international working group of many stakeholders, including our Office, under the leadership of Spanish Commissioner Artemi Rallo Lombarte. Reaching agreement on broad data protection principles was a valuable first step towards a harmonized approach to data protection.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION

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

Properly known as the International Organization for Standardization, the organization is currently developing framework standards for identity management and privacy. It is also identifying requirements for additional future standards and guidelines related to specific privacy-enhancing technologies.

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. He is, moreover, responsible for presenting the views of the International Conference of Data Protection Commissioners to this ISO working group, and is Canada's representative on a newly created ISO Privacy Steering Committee.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The Organisation for Economic Co-operation and Development (OECD) has long led the development of global solutions to privacy and security issues. Indeed, the OECD Guidelines on the Protection of Privacy and Transborder Data Flows mark their 30th anniversary in 2010.

The OECD planned a series of commemorative activities in 2010, which were to kick-start a discussion in 2011 on whether the guidelines need to be revised. The Commissioner headed a group to help plan the events. Our Office contributed to an OECD discussion paper on the new privacy environment and 21st century challenges to the protection of personal information.

ASIA-PACIFIC ECONOMIC CO-OPERATION

We are also at the table as the Asia-Pacific Economic Co-operation group implements its APEC Privacy Framework. Most of the work at APEC's Data Privacy Subgroup is focused on developing privacy rules to govern transborder data flows.

Our Office has been particularly involved in developing a framework to facilitate co-operation among enforcement authorities.

FRANCOPHONIE

Our Office continues to be involved in the work of the *Association francophone des autorités de protection de données personnelles*, which represents data protection authorities in French-speaking jurisdictions.

In late-2009, Assistant Commissioner Chantal Bernier made a presentation on personal data protection in a globalized world at the association's third international conference in Madrid.

In November 2009 our Office published an overview of the Canadian approach to privacy protection. Collaborating with the privacy commissioners of Quebec and New Brunswick, two of Canada's provinces with large francophone populations, we issued a report that was widely distributed within the Francophonie.

EUROPEAN COMMISSION

The European Commission is reviewing the relatively distinctive European data protection framework, which could ultimately lead to greater harmonization with the rest of the global community.

In 2009, our Office met with a working group advising the European Commission on data privacy and security. The meeting helped us better understand the European activities, and to explain how Canada is addressing the challenge of cross-border data flow.

CHAPTER 2: PRIVACY IN A CONNECTED WORLD

Focus on our Audit and Privacy Impact Assessment Review Work

For decades, information technologies have been enhancing our lives in countless ways. Most people today can scarcely envisage a world without the Internet and the many other advances that the digital age have brought.

Just as they download music, buy books or sell surplus sofas online, Canadians are choosing to interact electronically with the federal government. More and more, people are likely to search for information on a departmental website, e-file their taxes, or apply online for a government job, program or service.

The government, for its part, is determined to remain in step with the public, and is investing in the technological infrastructure and in-house expertise necessary for this fast-paced new Web 2.0 world.

Public servants are being encouraged to interact, network and blog, to build internal and external teams through sites such as GCConnex, and to contribute knowledge to online resources such as departmental wikis and the GCPedia. Microblogging and social networking are becoming increasingly popular, reinforced by the recruitment of a younger, tech-savvy workforce.

But every innovation also introduces new risks to privacy. As public servants post their thoughts and experiences to blogs and social networking sites, there is a heightened chance of blurring the line between their personal and professional lives. In such circumstances, the political neutrality of public servants can sometimes fall into question.

As more and more data circulates, moreover, there is also the potential for unauthorized disclosure of personal information. And, with the power of modern computers, a typical data breach may no longer affect just a few dozen people, but potentially hundreds of thousands.

These were some of the issues preoccupying our Office in 2009-2010. As described in this chapter, we conducted two privacy audits that examined the government's stewardship of the personal information of Canadians in this digital era.

One studied the potential privacy risks posed by the widespread use of wireless networks and handheld electronic communications devices by public servants. The other considered whether the government's policies and practices for disposing of surplus computers and paper documents posed a threat to sensitive or confidential personal information.

In light of the government's growing interest in social networks and other modern tools of internal and external engagement, we also looked at a proposal by the Public Service Commission to monitor media outlets, personal websites, and social networking sites such as Facebook for signs of potentially inappropriate political activity by public servants.

2.1 WIRELESS AUDIT

OVERVIEW

Thousands of federal public servants in Ottawa and other regional offices carry smart phones or other mobile devices with which they communicate by voice or data when they are not in their offices. Some federal departments also maintain wireless access points, so that public servants equipped with laptops and other mobile devices can connect to their office computers. These technologies allow government workers to be productive while away from their desks.

Wireless Technology

Wireless, such as Wi-Fi, technology allows electronic devices to communicate and transmit data over radio frequencies rather than physical cables. If not properly secured, the data may be exposed, intercepted, manipulated or sabotaged. A hacker could also hijack an authorized user's privileges to gain unauthorized access to a system.

However, in an audit of four large federal government departments and one Crown corporation (see box), our Office found that certain practices, coupled with an absence of policy requirements and practical safeguards for privacy and wireless data security, could put the personal information of Canadians at risk.

THE PROBLEM

Some departments handle vast amounts of personal information of Canadians. This is especially true of the five we looked at in our audit – Health Canada, Human Resources and Skills Development Canada, the Correctional Service of Canada, Indian and Northern Affairs Canada, and Canada Mortgage and Housing Corporation (better known as CMHC). Consequently, special care must be taken to ensure that the data is kept secure and safe from unauthorized disclosure.

We know that security gaps and lax practices can allow information to be unintentionally or unlawfully disclosed over wireless networks and through the use of wireless mobile devices.

In the simplest example, a person speaking on a cellphone in a bus could be overheard by fellow passengers. A note being tapped out on a laptop or smart phone may be spotted over the writer's shoulder. At a more sophisticated level, passwords, encryption and other security practices must be employed to prevent unauthorized people from gaining access to the data transmitted over wireless networks and devices.

The Audited Organizations

The entities we examined keep large amounts of sensitive personal information in order to deliver their programs and services. Here are some examples:

- Canada Mortgage and Housing Corporation – information from those seeking assistance under housing programs administered by CMHC
- Correctional Service of Canada – records on people imprisoned for two or more years
- Health Canada – medical information on people living in some 200 First Nations communities
- Human Resources and Skills Development Canada – data on recipients of public pension and employment insurance benefits
- Indian and Northern Affairs Canada – personal information on First Nations, Inuit and Métis peoples

Another consideration relates to the loss or theft of wireless devices that could contain personal information. When a device goes missing, it is possible to send a command to remotely wipe it of data. However, this has to occur *before* the service is deactivated, since deactivation disables the device's capacity to receive and act on a command to wipe the data. We were told of cases where, in the absence of formalized procedures, these steps were taken in the wrong order and data was left on the missing devices.

We also considered issues raised by the mobile devices that the government no longer needs. The five audited entities alone store thousands of surplus devices. Some are eventually refurbished or recycled, so it is crucial that they first be wiped clean of data.

WHAT WE LOOKED FOR

We reviewed the policies, procedures, practices and controls that CMHC, the Correctional Service of Canada, Health Canada, Human Resources and Skills Development Canada, and Indian and Northern Affairs Canada use to reduce the privacy risks associated with wireless technologies, including smart phones, cellular telephones and Wi-Fi networks.

We also tested surplus wireless devices (smart and cellphones) and scanned for wireless access points in and around the organizations' premises.

The Policy Rules

In 2002, Treasury Board established a policy that sets out safeguards to protect the confidentiality and integrity of government assets, including personal information. The policy and its related standards, which specify mandatory security requirements, are consistent with national and international standards and best practices for protecting data.

Federal institutions are required to conduct their own assessments to determine whether safeguards above the policy's baseline levels are necessary.

OUR FINDINGS AND RECOMMENDATIONS

Risk assessment – None of the entities we audited had fully assessed the threats and risks inherent in wireless communications. (Human Resources and Skills Development Canada had an initiative underway but it was not completed at the time of our audit.) In the absence of such analyses, the audited entities could not demonstrate that all material risks were identified and appropriately managed.

We recommended that CMHC, the Correctional Service of Canada, Health Canada and Indian and Northern Affairs Canada undertake a threat and risk assessment for their wireless networks and smart phones.

User responsibility – None of the forms that users signed in exchange for using a government cellular or smart phone contained provisions specifying the user's responsibility to operate the device in a manner that protects privacy.

User training – Only one of the entities was able to demonstrate that all smart phone users had received training on the acceptable use of wireless devices, measures to protect data stored on them, or the implications of using the technology in public areas.

We recommended that the Correctional Service of Canada, Health Canada, Human Resources and Skills Development Canada and Indian and Northern Affairs Canada ensure that employees are made aware of the privacy risks inherent in the use of smart phones.

Passwords – Only three of the five entities (Health Canada, Human Resources and Skills Development Canada, and Indian and Northern Affairs Canada) had implemented protocols requiring that smart phones carry strong password protection. The Correctional Service of Canada required passwords, but did not specify that they be "strong". While CMHC urged staff to use passwords, the decision to activate the feature was left to individual users.

We recommended that CMHC and the Correctional Service of Canada require their employees to use strong passwords for their smart phones.

Data encryption – None of the five audited organizations required that data stored in the devices' memory be encrypted.

We recommended that all five organizations ensure that data stored on smart phones is encrypted.

Encryption of Wi-Fi networks –The Wi-Fi networks at CMHC and Indian and Northern Affairs Canada were protected by encryption levels recommended by Communications Security Establishment Canada. Based on our review of the configuration of the one Wi-Fi network at the Correctional Service of Canada, we were satisfied that appropriate measures were in place to protect data transmissions over the network. Health Canada used Wi-Fi computing in certain remote locations and departmental officials informed us that a weak level of encryption was used. Human Resources and Skills Development Canada did not have any Wi-Fi networks.

We recommended that Health Canada review its wireless networks to ensure that the access points are set with security encryption recommended by Communications Security Establishment Canada.

PIN-to-PIN messaging – Also known as peer-to-peer messaging, this direct communication between two smart phones uses personal identification numbers (PINs) to circumvent an organization's corporate server. Communications Security Establishment Canada says this form of messaging is vulnerable to interception and urges departments not to use it unless they develop specific policies and supplementary security measures to safeguard the confidentiality of PIN-to-PIN communications.

We found that all of the entities allow the use of PIN-to-PIN messaging and none was able to demonstrate that it had implemented measures to address the security issues related to the use of this communication method.

We recommended that all five organizations ensure that the use of PIN-to-PIN messaging is consistent with the guidance issued by Communications Security Establishment Canada.

Lost or stolen wireless devices – Four of the five audited entities could not provide documented procedures outlining the steps that should be taken to mitigate the risk of data exposure in the event that a wireless device is lost or stolen. We found that practices varied between the entities and, in some cases, within the audit entity itself.

We recommended that the Correctional Service of Canada, Health Canada, Human Resources and Skills Development Canada and Indian and Northern Affairs Canada establish documented procedures for responding to incidents of lost or stolen wireless devices.

Storage of surplus devices – Four of the institutions had secure storage measures for their surplus wireless devices, including locked filing cabinets or secure rooms with limited access. However, surplus smart and cellular phones at one Human Resources and Skills Development regional office were stored in an unlocked filing cabinet in an area accessible to all staff. Some of the devices contained data.

We recommended that Human Resources and Skills Development Canada ensure that all of its surplus wireless devices are stored in secure areas.

Device disposal – A sample of surplus wireless devices that we tested from the Correctional Service of Canada, Health Canada and Human Resources and Skills Development Canada had not been wiped clear of data. Some were destined for disposal by Crown Assets Distribution, the organization within Public Works and Government Services Canada that is responsible for the sale, distribution, disposal and reuse of surplus federal goods. All surplus smart and cellular phones at Indian and Northern Affairs Canada, however, had been wiped of data.

We recommended that CMHC, the Correctional Service of Canada, Health Canada and Human Resources and Skills Development Canada establish controls to ensure that data stored on surplus wireless devices is purged prior to disposal.

CONCLUSION

The *Privacy Act* requires federal departments and agencies to respect the privacy rights of Canadians. This obliges them to protect their personal information holdings through adequate policies and procedures, safeguards and disposal practices.

None of the five institutions we audited had completed threat and risk assessments of their wireless networks and portable wireless devices, although Human Resources and Skills Development Canada was in the process of doing so at the time of our audit. In the absence of such an analysis, entities cannot demonstrate that all material risks have been identified and addressed.

In examining existing policies on wireless devices, we found they generally lacked key elements. There was also an absence of documented procedures to mitigate the risk of data exposure resulting from losses or theft.

We found that key safeguards to protect personal information on wireless devices were not always used. For example, two of the five entities did not use strong password protection and none of the entities required that data be encrypted on their smart phones.

How We Did the Audit

We began with a survey of 34 government organizations to get an overview of wireless use within the Government of Canada. The five organizations we selected for closer examination manage significant amounts of personal information in order to fulfill their respective mandates.

We interviewed staff and reviewed policies, procedures, processes and controls. We also examined a sample of surplus wireless devices to determine whether they had been wiped clean of data before being sent for disposal.

We monitored the wireless airspace within and around the premises of audited entities. We obtained a legal opinion to confirm that our activity in this regard did not violate any provincial or federal laws.

Audit activities were carried out in Ottawa-Gatineau, Toronto, Montreal, Quebec City, Winnipeg, Vancouver and Abbotsford, B.C.

The organizations' responses

All organizations have responded, agreeing in whole or part with our recommendations. The full audit report, including the institutions' detailed responses, is being published concurrently with this annual report and is available on our website.

With one exception, the audited entities did not, as a general practice, educate wireless users on how to operate these devices in a manner that protects privacy.

We also found that controls for managing surplus wireless devices were inadequate. With the exception of Indian and Northern Affairs Canada, moreover, none of the audited entities could demonstrate that adequate measures were in place to ensure that data is wiped from smart and cellular phones before they are sent for disposal.

In testing Wi-Fi networks, we found that encryption levels varied. Three of the four entities had implemented security encryption that met the level recommended by Communications Security Establishment Canada.

The use of wireless technologies and devices to transmit and store personal data poses certain privacy risks. Based on our audit work, we concluded that the Canada Mortgage and Housing Corporation, Correctional Service of Canada, Health Canada, Human Resources and Skills Development Canada, and Indian and Northern Affairs Canada need to strengthen certain policies, procedures and/or controls to further mitigate these risks.

2.2 DISPOSAL AUDIT

OVERVIEW

The federal government collects and uses vast amounts of personal information to deliver its programs and services. We wanted to know what happens to the information when it is no longer needed for its original purpose, or resides on obsolete computers.

Our audit examined whether selected federal institutions dispose of the personal information securely. We were particularly interested in arrangements to outsource portions of the disposal process to private-sector entities.

The absence of adequate controls over the disposal of unneeded government documents was the subject of one of the most egregious privacy breaches our Office has ever encountered.

In 1998, acting on a tip from a reporter, we discovered several tonnes of confidential federal government records, relating to thousands of Canadians, sitting baled and ready for shipment in a warehouse belonging to the private company hired to shred and recycle the documents.

Our investigation revealed that four truckloads of the documents were destined for the United States, South Korea and China. The material, which included personal income tax, immigration, parole and pension records, was being offered intact to the highest bidder because whole paper was worth more than shredded paper on the recycling market.

We also found evidence that National Archives Canada and Public Works and Government Services Canada were aware of financial, security and technical problems with the company before granting it clearance to transport and shred federal records.

At that time, the Privacy Commissioner recommended that Library and Archives Canada use off-site shredding services only if the companies could guarantee security, and only if the shredding was performed under supervision.

We examined mechanisms for the destruction of unneeded paper documents, some of which is carried out under contract by private shredding companies.

We also reviewed procedures for the disposal of surplus computers through the Computers for Schools program and Crown Assets Distribution.

While many satisfactory policies and procedural rules are in place, we were disturbed by some serious deficiencies in practice. For example, more than four in 10 computers donated to the Computers for Schools program had not been wiped of data by the donating institution, and some of the information was highly sensitive and even classified.

We also discovered that one private paper-recycling company shredded documents into strips 50 percent wider than its contract allowed.

WHY THIS IS IMPORTANT

Whether applying for a passport, collecting Canada Pension Plan benefits, or filing personal income tax returns, individuals are generally not in a position to oppose the collection and use of their personal information by government. The data is often highly sensitive and its unauthorized disclosure could have severe consequences for people's privacy, the integrity of their identity, their economic circumstances and even their personal safety.

Although our privacy audits usually scrutinize practices for managing personal data that is still in active use, this audit spotlights the importance of controls at the end of the process, as organizations dispose of data they no longer need.

Indeed, federal institutions are obliged to protect information destined for disposal with the same care they afford to data still in use. The public's trust in the government's ability to safeguard highly sensitive personal information is at stake.

WHAT WE FOUND

1. LIBRARY AND ARCHIVES CANADA

Overview

Treasury Board establishes controls to manage protected and classified assets awaiting destruction. These controls relate to appropriate storage facilities to prevent unauthorized access, theft or loss, and measures to protect records from the time they leave the organization until their destruction.

Library and Archives Canada Regional Service Centres manage records on behalf of more than 90 federal departments and agencies. These centres perform various functions, including disposing of records after obtaining concurrence from client institutions. Much of the disposal work is contracted out to private-sector shredding or paper-recycling firms.

Our investigation established that Library and Archives Canada has a comprehensive and consistent set of administrative policies and procedures for the secure disposal of federal government records.

However, we found that the organization does not systematically monitor the destruction practices of off-site shredding companies through periodic inspections and annual audits.

In fact, we found that two of the four shredding companies that Library and Archives Canada uses have, at one time or another, violated their contractual obligations. Those obligations, for example, require that staff hold an appropriate security clearance, that records be destroyed so that the information cannot be reconstructed, and that documents be disposed of on a timely basis to mitigate the risk of unauthorized access, loss or theft.

Off-site shredding

The audit focused on the off-site destruction of low-sensitivity (Protected A) and sensitive (Protected B) information. The unauthorized disclosure of Protected B information could reasonably be expected to cause serious injury to an individual, organization or government.

Library and Archives Canada manages the disposal of classified information, whose unauthorized disclosure could cause injury to the national interest. Classified records are destroyed on-site under tightly controlled conditions.

We visited three shredding companies and received briefings on their disposal processes and the measures they use to protect records awaiting destruction.

Treasury Board policy establishes baseline (minimum) specifications for the secure destruction of classified and protected documents. Library and Archives Canada has imbedded a more stringent requirement into its own standard.

We found, however, that this requirement was not consistently applied.

We recommended that Library and Archives Canada ensure that the terms and conditions written into off-site destruction contracts are consistent with its own security standard.

Contract violations not monitored

Treasury Board's contracting management standard states that departmental policies and procedures should provide for regularly scheduled and surprise inspections of contractor work sites. In a 2002 letter to our Office, the National Archivist stated that Library and Archives Canada would implement a rigorous and detailed audit protocol for off-site records destruction contracts.

We expected to find an effective and well-documented monitoring regime. While we were told that inspections are generally performed annually, Library and Archives Canada was unable to produce records to support this assertion.

Our own audit included a review of contracting files and available inspection reports relating to the four off-site shredding companies used by Library and Archives Canada. This examination revealed that two of the companies had at some time violated their contractual obligations.

In one instance, Library and Archives Canada officials showing up for an unannounced inspection of a shredding company found full pallets of material that had arrived for destruction 12 days earlier, even though the paper should have been destroyed within three days of receipt.

In another case, employees were not appropriately security screened and the average width of shredded material exceeded contract specifications by 50 percent. Records on file suggest that the company had not been in compliance for several years. Public Works and Government Services Canada suspended the company's security clearance until the deficiencies were addressed.

We concluded that Library and Archives Canada has not fully met the National Archivist's 2002 commitment with respect to monitoring off-site records destruction contracts. Without clear accountability and enforcement, shredding companies may circumvent contract requirements without consequences.

We recommended that Library and Archives Canada establish a protocol for monitoring off-site records destruction contracts to ensure that privacy and security requirements are being met in a timely and consistent manner.

We also recommended that Library and Archives Canada ensure that off-site destruction contracts include a requirement that the service provider issue a certificate of destruction that records the date that records are destroyed and the name of the authorized person who conducted or witnessed the destruction.

2. COMPUTERS FOR SCHOOLS PROGRAM

Overview

The Computers for Schools program, founded in 1993 and managed by Industry Canada, collects and refurbishes surplus computers donated by government and private-sector sources, and distributes them to schools, public libraries, aboriginal communities and not-for-profit learning organizations throughout Canada. There are more than 40 refurbishing workshops and warehouses for the program across Canada.

Treasury Board directs federal departments and agencies to offer all surplus information technology equipment, including computers, printers, modems, hard drives and network cards, to the Computers for Schools program first. To date, the program has refurbished more than a million computers.

Our 1994-1995 annual report noted that approximately 95 percent of the donated machines still had programs and data on them, despite Treasury Board policy requiring them to be wiped clean. By the following year, some 35 to 45 percent of the computers had been wiped, still far short of requirements.

Beginning in December 2009, we took another look at this issue. We found that, while adequate policies were in place, federal departments and agencies were still not exercising due diligence in ensuring that computers are wiped of data before being donated to the Computers for Schools program.

We found numerous computers that contained personal information, classified information, and documents subject to solicitor-client privilege. Indeed, the information residing on some hard drives was so sensitive that we had them immediately returned to their originating department.

Policy and procedural controls

While data security is the responsibility of the donating institution, any inadvertent exposure of information that compromises privacy and security could also undermine the integrity of the Computers for Schools program.

Our examination of the program's security policies, procedures and practices found that the various roles, responsibilities and reporting requirements were described in significant detail.

Industry Canada does not, however, reconcile the number of computers that are donated by federal institutions under the Computers for Schools program with the number that are wiped through the program's refurbishment process.

In the absence of a reporting mechanism, computers may be lost or stolen with no means of detection.

Security weaknesses

Computers for Schools program agreements require computer-refurbishment workshops and storage areas to have safeguards to prevent unauthorized access. All Computers for Schools workshops and warehouses must complete an annual security questionnaire, which is submitted to Industry Canada.

We examined questionnaires submitted between 2008 and 2010. A significant number indicated non-compliance with certain policy requirements of the Computers for Schools program. The deficiencies generally related to the storage and tracking of hard drives, and employee security screening.

As the questionnaires highlight potential security vulnerabilities, we examined whether they are subject to systematic analysis and follow-up with Computers for Schools licensees. Our audit revealed they are not.

Security deficiencies that are not addressed could place program assets, including personal information, at risk.

We therefore recommended that Industry Canada ensure that all reported security weaknesses are analyzed and addressed.

Sensitive data found on computers

Treasury Board policy requires that, prior to disposal, all surplus computers be purged of classified and protected information so it cannot be recovered.

Accordingly, we tested a sample of 1,093 computers from 31 federal institutions at Computers for Schools workshops in Vancouver, Winnipeg, Toronto, Gatineau, QC, Halifax, and Truro, N.S.

In 458 (42 percent) of the computers, originating from 28 (90 percent) of the institutions, we found that the hard drives had not been completely erased. Later forensic analysis of a subsample of these hard drives established that many contained personal or classified information, or records subject to solicitor-client privilege.

In fact, the information on several hard drives was so sensitive that we took immediate steps to have them returned to their original department.

The Computers for Schools program was not designed to be a computer hard drive sanitization service for federal institutions. That responsibility rests with the donating institutions themselves. The audit revealed, however, that many federal departments and agencies are not complying with Treasury Board policy by properly wiping computers of data before donating them to the program.

In short, deficiencies highlighted by the Privacy Commissioner 15 years ago persist today, leaving the privacy of Canadians at risk.

We recommended that Industry Canada work with the Treasury Board Secretariat to request that federal institutions provide a signed declaration to the Computers for Schools program certifying that all donated computers and related assets have been wiped of data.

It was not within the scope of the audit to examine in detail the operations of Computers for Schools licensees – people who refurbish and distribute computers on behalf of the program. However, upon discovering that many computers that are sent to the program from departments and agencies still house sensitive data, we looked at how six workshops in five regions of Canada refurbish computers and send them on to schools. We randomly selected 414 hard drives for testing and found that all had been wiped.

3. CROWN ASSETS DISTRIBUTION

If the Computers for Schools program cannot use a computer or other technological device offered to it by a federal institution, the equipment is transferred to Crown Assets Distribution for sale through public auction. Crown Assets Distribution is a directorate within Public Works and Government Services Canada that is responsible for the sale, distribution and disposal of surplus federal goods.

Departments and agencies are solely responsible for preventing the unauthorized release of information contained in surplus assets, regardless of the disposal mechanism used.

Crown Assets Distribution is not responsible for ensuring that institutions comply with this obligation and is not funded to provide a hard drive sanitization service to federal institutions. In many cases, in fact, the organization does not even take physical possession of the equipment; it remains at the disposing institution until it is sold.

In considering the privacy risk associated with computer disposal through Crown Assets Distribution, it is worth noting that, in 2009, only 336 desktop computers and 1,104 laptops were disposed of in this way. By comparison, federal donations to the Computers for Schools program exceeded 60,000 computers.

Moreover, Crown Assets Distribution sells the overwhelming majority of its computers without hard drives. Even so, we examined the organization's procedures and processes, and tested surplus computers at one of its warehouses.

We found that Crown Assets Distribution does not dispose of any equipment without a signed Report of Surplus, in which departmental material managers confirm that all security requirements have been addressed before a device is disposed of.

Conclusion

Maintaining the security of personal information until it is disposed of by an approved method is an important obligation on government institutions under the *Privacy Act*.

Library and Archives Canada has a comprehensive set of administrative policies, procedures and practices for managing the disposal of records on behalf of government institutions. Security requirements in off-site destruction contracts comply with government policy and provide adequate controls to ensure records are transported, stored and disposed of in a secure manner.

However, while Library and Archives Canada has assumed that off-site shredding companies are complying with their contractual obligations, there is no mechanism to confirm that this is so. In the absence of an effective monitoring regime, shredding companies can circumvent requirements to protect privacy, and some have done so.

The organizations' responses

As this report was being written, the audited organizations had not yet submitted their formal responses. Informally, however, all had agreed with our recommendations. The full audit report, including the institutions' detailed responses, is being published concurrently with this annual report and is available on our website.

Federal departments and agencies have sole responsibility for preventing the unauthorized release of computer data contained in their surplus electronic assets, regardless of the disposal mechanism used.

The overwhelming majority of surplus computers are donated to the Computers for Schools program, and Treasury Board policy requires that they be wiped first of all classified and protected information. In testing computers from 31 federal departments and agencies, we found that 28 of them (90 percent) had not fulfilled their obligation in this regard.

A concerted effort is needed to strengthen compliance with this policy requirement. Until that happens, the privacy of Canadians will remain at risk.

2.3 PRIVACY IMPACT ASSESSMENT REVIEWS

Privacy Impact Assessments help federal institutions determine the effect of proposed new programs or services on privacy. Under a 2002 Treasury Board policy, departments and agencies are required to conduct Privacy Impact Assessments at the earliest possible stage in the development of a new or significantly modified initiative, and to submit them to our Office for review. The objective is to identify potential privacy risks and to devise strategies to eliminate or mitigate them.

Privacy Impact Assessments are an important focus for our Office, and we try to work with institutions to ensure that the process yields the maximum privacy protections for Canadians. We do not approve assessments or endorse projects. Rather, we review the institutions' submissions and make recommendations on how projects can be improved to better safeguard the privacy of Canadians.

We cannot oblige institutions to implement our recommendations, or even to heed our advice. Even so, we find that institutions generally work with us to resolve privacy concerns.

Another important benefit of the Privacy Impact Assessment process is its transparency when departments and agencies publish summaries of completed assessments on their websites. The highlights of some noteworthy Privacy Impact Assessments are also made public by being included in this annual report.

In 2009-2010, our Office received 102 new Privacy Impact Assessment submissions. This was a record number, up nearly 60 percent from the previous year. We believe this increase reflects a welcome receptiveness to Treasury Board's policy on the part of institutions, which are assessed for their privacy performance against the Management Accountability Framework.

For our part, we have been refining a triage process so that we can most effectively deploy our limited resources. Thus we selected for full review those initiatives that posed the greatest privacy risks, or that fell into one of our four priority areas – national security, information technology, genetic technology or identity integrity.

Focusing first on those projects, we sent out 33 letters of recommendation and detailed advice. We retained the remaining files for our reference and potential future review.

SIGNIFICANT PRIVACY IMPACT ASSESSMENT FILES

Here are summaries of key Privacy Impact Assessments we reviewed over the past fiscal year:

1. POLITICAL IMPARTIALITY MONITORING APPROACH

The Public Service Commission submitted a Privacy Impact Assessment for a program that would cross-reference government databases of current and former public servants with candidate lists in federal, provincial and municipal election campaigns. The Political Impartiality Monitoring Approach, or PIMA, would also monitor the Internet, including media outlets, personal websites and social networking sites such as Facebook, for signs of potentially inappropriate political activity by public servants.

We recognize that the Commission has a mandate to ensure an impartial public service. Even so, we were concerned that this initiative could yield an ongoing and unlimited database about the opinions, political affiliations, personal causes, hobbies, religious affiliations and group memberships of past and present public servants, deputy heads and Governor in Council appointees.

We asked the Public Service Commission to show that the PIMA is actually necessary by providing, for example, evidence of an upward trend in partisanship within the public service. We also asked why potentially sensitive personal information would be collected in the absence of specific allegations against an individual.

In its response to our recommendations, the Public Service Commission indicated that the scope of the PIMA was to be narrowed and that our Office would receive a new Privacy Impact Assessment on the modified approach before the end of 2010.

We remain concerned about the potential privacy risks posed by the PIMA and have asked the Commission to specifically consider the necessity, proportionality and effectiveness of the initiative in its revised project. We will continue to monitor this issue closely.

2. SECURE CERTIFICATE OF INDIAN STATUS

In 2009, Indian and Northern Affairs Canada submitted a preliminary Privacy Impact Assessment on its plans to develop a Secure Certificate of Indian Status card. A new card was already in the design stage when the U.S. government announced stricter rules for identification documents that would be acceptable for Canadians wishing to cross the land border between the two countries.

Under America's Western Hemisphere Travel Initiative, documents used to enter the U.S. must show citizenship as well as identity. Passports are acceptable, as are enhanced driver's licences such as those issued by British Columbia.

Provinces collect information from applicants for enhanced driver's licences and forward it to the Canada Border Services Agency, where it is held in a database that can be accessed by the U.S. Customs and Border Protection agency when the individual arrives at a border crossing.

The enhanced driver's licence is a voluntary option for drivers who want to use a licence instead of a passport to cross the border. Indian and Northern Affairs Canada, however, proposed making all Secure Certificate of Indian Status cards automatically compliant with the U.S. border rules. That meant that all application information for the status cards would have to go to Canadian border authorities, and potentially to U.S. border authorities as well.

A key privacy principle is that personal data should only be disclosed to parties with a justifiable need to access it. Unrestricted sharing of information increases the risk of data breaches. This is particularly significant with Indian status cards, because First Nations citizens require these cards to access a wide range of entitlements under the *Indian Act*.

We conveyed our concerns to Indian and Northern Affairs Canada and the Assembly of First Nations. On the premise that First Nations peoples should have a right to choose whether to use the Secure Certificate of Indian Status card, a passport, or another acceptable document as a border-crossing instrument, we recommended that Indian and Northern Affairs Canada amend the status card application form to include a specific opt-in provision enabling the card to be used at borders.

We also expressed concerns about other matters, such as the level of security of the related information technology, and the need for better notice and consent on application forms. And we called for detailed information-sharing agreements among all relevant parties.

In its response, Indian and Northern Affairs Canada said it would no longer require all Secure Certificate of Indian Status cards to be compliant with the U.S. border regulations. New application forms have been developed that detail potential information-sharing arrangements and give applicants the choice to accept or decline the border-crossing features.

The department will also carry out a full Privacy Impact Assessment on the Secure Certificate of Indian Status initiative to further address our concerns.

3. ELECTRONIC MONITORING SYSTEM

During 2009-2010, our Office reviewed a Privacy Impact Assessment on a Correctional Service of Canada pilot project involving the electronic monitoring of federal offenders.

Inmates who qualified for conditional release programs and who volunteered for the Electronic Monitoring Program Pilot agreed to wear electronic ankle bracelets equipped with a GPS (global positioning system), which transmitted to a monitoring network. The Correctional Service of Canada was alerted if an offender violated preset conditions, such as curfews or restrictions on residency or location. Signed consent was obtained from participating offenders before the monitoring started.

We had concerns about the program's rationale and effectiveness, which we expressed in our October 2009 letter of recommendation to the institution.

Our Office generally views geo-location monitoring equipment as privacy intrusive. We acknowledge that some degree of intrusion into an offender's privacy is necessary and appropriate in order to protect public safety. However, we questioned whether the Correctional Service of Canada had demonstrated that the monitoring bracelets actually increased public safety to a degree justifying the intrusion on privacy.

In this case, the device provides much more information about the movements of an offender in the community than would be known through other forms of supervision, such requiring the offender to live in a halfway house or to check in regularly with a parole officer.

In December 2009, an internal Correctional Service of Canada evaluation report raised further questions about the effectiveness of the pilot, noting there had been numerous technical malfunctions in the devices and problems with the monitoring process. The report observed that even some of the anklet-wearing offenders themselves doubted that the surveillance technology had made them more accountable for good behaviour.

The pilot was intended to lay the groundwork for legislation that would have allowed the Correctional Service of Canada to roll out such a program nationally. However, the bill, introduced in June 2009, died on the order paper when Parliament was prorogued in December. By the end of this reporting period, it remained unclear whether new legislation would be forthcoming.

The Correctional Service of Canada pledged to undertake a new Privacy Impact Assessment in the event that a national program is contemplated. We have asked for an update on the status of the project, in light of the internal evaluation report's questions about the project's effectiveness.

This project highlights the need for a broader societal examination of geo-location instruments. These devices hold the potential for function creep, expanding from monitoring prisoners and parolees to tracking the whereabouts of children, the elderly, employees and other individuals.

2.4 MODERNIZING THE PROCESS

PRIVACY IMPACT ASSESSMENT TRIAGE

In 2009-2010, we received 102 new Privacy Impact Assessments for review, up 59 percent from the year before. In light of the steadily rising numbers of these assessments coming through our doors, we continued to transform our internal review and analysis processes.

A key element of this transformation is our triage system. Privacy Impact Assessment files for initiatives posing the greatest risk to the privacy of Canadians, or those aligned with any of our Office's four priority areas (genetic technologies, information technologies, national security and identity protection), go to the front of the line. This helps focus our resources and ensure that our advice is timely and relevant.

NEW APPROACH FOR REVIEWS

We have also changed the way we review the Privacy Impact Assessments that are selected for further analysis.

Since the Privacy Impact Assessment policy came into effect in 2002, our Office has reviewed submissions in relation to the *Privacy Act* and the 10 universally recognized principles of the Canadian Standards Association Model Code for the Protection of Personal Information. We also weigh submissions against Treasury Board information-management policies and generally accepted best practices for the public and private sectors.

Certain high-profile and controversial government programs, however, have recently accentuated the need to also consider broad societal privacy risks and concerns. Examples of such initiatives are:

- the Canadian Air Transport Security Authority's whole-body imaging scanners;

- the National Integrated Interagency Information Sharing Initiative, which involves personal information sharing among federal public safety portfolio institutions and federal and municipal partners;

- the Public Service Commission's monitoring of social media sites for indications of political activity on the part of public servants;

- the RCMP's automated licence plate recognition program.

We verified that these initiatives were assessed against their broader impact on democratic society, civil liberties, and our fundamental human right to privacy.

The Supreme Court of Canada has recognized privacy as a constitutional right essential to the exercise of fundamental freedoms, and the *Privacy Act* as having quasi-constitutional status. In light of this, we have started emphasizing to government institutions the importance of answering the following four questions in their Privacy Impact Assessments:

- Is the proposed measure demonstrably necessary to meet a specific purpose?

- Is it likely to be effective in meeting that purpose?

- Is the loss of privacy proportional to the benefit to be derived?

- Is there a less privacy-invasive way of achieving the same end?

The four-part test was adapted from one developed by Chief Justice Brian Dickson of the Supreme Court of Canada in *R. v. Oakes* (1986) as a tool to gauge whether the violation of a provision of the *Canadian Charter of Rights and Freedoms* could be justified.

PRIVACY IMPACT ASSESSMENT WORKSHOP

In January 2010, our Office hosted what we intended as the first in a series of workshops for federal government employees responsible for preparing Privacy Impact Assessments.

Although the government's Privacy Impact Assessment policy is now in its eighth year and the Treasury Board Secretariat has issued tools and guidance for completing such analyses, we wanted to ensure that our expectations for the assessments submitted to our Office were better understood.

The workshop drew 90 participants, representing 40 federal institutions. Assistant Commissioner Chantal Bernier outlined our new approach for grounding Privacy Impact Assessment reviews in public law, and managers discussed our Office's expectations with respect to the submissions we receive from government departments and agencies.

A lively question-and-answer session yielded material for future workshops. A written summary of our expectations was prepared for publication in 2010-2011.

RISK-BASED AUDIT

The *Privacy Act* empowers us to audit any federal department or agency, at any time, to ensure compliance. With such a vast audit universe, we wanted to develop a systematic approach targeting programs and departments at greatest risk.

We therefore developed in 2009-2010 a risk-based audit plan that:

- identified the major holders of personal information of Canadians;
- assessed the sensitivity of that information;
- considered the risks that this information could pose if it was improperly used;
- reviewed the privacy risk-management regimes that are in place; and
- consulted with stakeholders, including federal departments and agencies, privacy experts and academics.

The plan was set for implementation in 2010-2011.

CHAPTER 3: PRIVACY AND SECURITY

Focus on our Policy and Legislative Work

Back in 1942, when the Humphrey Bogart classic *Casablanca* was first released, the final airport scene was a poignant farewell to romance.

Today, the idea of a lone couple, standing by night on a foggy tarmac, evokes only a grainy, black-and-white flight into nostalgia.

Indeed, in this post 9/11 era, airport and border security measures are asserting ever-tightening constraints on travellers. Year after year, new surveillance technologies, scanners and controls are introduced, with an eye to keeping the skies safe from terrorists.

While passengers may grumble about the inconvenience, most acknowledge the need for the measures.

From our perspective, national security is also of paramount importance. But we contend that any security measure must also take the privacy of citizens into account.

The two priorities, in fact, are not mutually exclusive; they are mutually reinforcing. They complement each other, morally and functionally. Morally, both privacy and safety characterize the society in which we have chosen to live. Functionally, they work together to streamline and focus each other.

One key element of privacy is the judicious collection, use and disclosure of personal information, particularly in the area of travel and border security. The uncontrolled compilation and exchange of personal information can have unforeseen, and often grave, consequences. Indeed, people have not only been inconvenienced, they have also been detained, deported, denied entry to Canada, and even rendered abroad for torture on the basis of false or uncorroborated data.

Over the past fiscal year, much of our Office's policy, legislative and legal affairs work centred on national security issues and their impact on privacy. At times, we questioned whether the appropriate balance had been struck.

This chapter outlines the highlights of our efforts in the area of aviation and border security, Olympic Games security, telecommunications surveillance powers and other priorities.

It concludes with a report on other work we do in fulfillment of our mandate, including our legislative activities.

3.1 AVIATION SECURITY

Several national security initiatives captured our attention during 2009-2010, but aviation security occupied the foreground.

1. ROUNDTABLE FORUM ON AVIATION SECURITY

In February 2010, officials from our Office joined members of Parliament, experts, academics and other stakeholders in a roundtable discussion on aviation security.

Organized by opposition MPs, the goal of the session was to scrutinize the privacy and other impacts of the burgeoning range of air security measures.

As a panellist at the forum, Assistant Commissioner Chantal Bernier explored the convergence of privacy and security, mapped out the legal context, and described the Office's approach to gauging the privacy impacts of security measures.

That approach weighs the necessity, effectiveness and proportionality of a potentially privacy-invasive security measure, and whether a less intrusive alternative exists.

2. TRAVELLER FACT SHEET

We published a comprehensive fact sheet for Canadians entitled *Checking In: Your privacy rights at airports and border crossings*. The publication describes the searches and reviews of personal data that travellers can legally find themselves subjected to by Canadian authorities. It also informs travellers of their right to redress if they feel their privacy has been invaded or their rights to travel unjustly denied.

For example, the Canada Border Services Agency reviews all information on individuals travelling to Canada and can share this information with other agencies, in Canada or abroad. Travellers, however, may request a copy of the data to ensure it is correct, and apply to the agency's Admissibility Branch to arbitrate disputes.

3. AIRPORT SCANNERS

In the arena of aviation security, one of our higher-profile activities in 2009-2010 was our review of the Privacy Impact Assessment submitted by the Canadian Air Transport Security Authority (CATSA) for the millimetre-wave security scanners that the government planned to deploy at airports across Canada.

The technology was controversial because, even as it enables screening officers to detect non-metallic weapons and other concealed threats beneath a passenger's clothing, it is equally capable of revealing images of the person's body.

CATSA conducted a pilot project on the scanners in Kelowna, B.C. in 2008 and we reported on their preliminary Privacy Impact Assessment in last year's annual report.

During 2009-2010, we continued to consult with CATSA on its plans to deploy seven units at four Canadian airports. We challenged the organization to ensure that any measure proposed for passenger screening – including whole-body imaging – is strictly proportionate to the identified threat.

CATSA assured us that its decision to select this technology was based on rigorous threat and risk assessments. The agency also agreed with our recommendations that the scanners be used only as a secondary screening method. It further pledged that:

- participation would remain anonymous and voluntary;
- a physical pat-down would be offered as an alternative;
- screening officers would be separated from and unable to see the individual being screened;
- the images would not be correlated with any other personal information and would not be identifiable; and
- all images would be deleted immediately after the scanning is completed.

The agency also agreed to seek out and develop less privacy-invasive technologies, regularly reassess the need for whole-body scanners against new intelligence, ensure the public has clear and accurate information on which to base informed choices, and track and report public complaints and concerns.

In January 2010, in the wake of the failed Christmas Day "pants bomber" attempt on a Detroit-bound Northwest Airlines flight, Transport Canada ramped up its deployment plans, announcing that 44 units would be installed at airports across the country.

As the fiscal year ended, we continued to meet regularly with CATSA to discuss the rollout and technical aspects of the scanners, along with any changes in the way the program operates.

3.2 OTHER PUBLIC SAFETY AND SECURITY INITIATIVES

1. OLYMPIC AND PARALYMPIC GAMES

In February and March 2010, the Vancouver Olympic and Paralympic Winter Games became the first international "mega-event" to take place in Canada since the 2001 terrorist attacks on the United States.

While Olympic organizers focused on security at the Games, our Office also saw value in ensuring that the security and law enforcement activities did not unduly infringe on the privacy rights of spectators, athletes and their entourages, employees, volunteers and local residents.

For a full year preceding the Games, our Office, in conjunction with the Office of the Information and Privacy Commissioner of British Columbia, was in regular communication with officials of the Integrated Security Unit, the RCMP-led authority responsible for security at the Games.

In the spring of 2009, we developed a fact sheet that set out a framework of guiding principles

Privacy safeguards built into anti-doping agreement

In late-2009 we received a preliminary Privacy Impact Assessment on an information-sharing agreement signed between the Canada Border Services Agency and the International Olympic Committee (IOC).

The agreement, part of the IOC's anti-doping efforts, would see the Canada Border Services Agency share personal information of visiting athletes and other Games participants with the IOC, in order to combat the importation of drugs and other controlled substances.

While we accepted that a "clean" event could enhance the reputation of the Games, we were not persuaded that the broad public interest in such an outcome outweighed the invasion of privacy. Indeed, we were concerned that disclosing personal information to a non-state entity (the IOC) could set a dangerous precedent.

In response to our recommendations, the border services agency undertook to make the agreement more privacy sensitive by restricting its application to the period of the Games, obtaining adequate consent from the individuals affected, and disclosing personal information only on a case-by-case, need-to-know basis.

The agency further agreed to report only on substances within its enforcement mandate (which does not include all substances banned under world anti-doping rules), and to ensure that the collected personal information was handled with appropriate security safeguards.

intended to help Games officials carry out their security functions in a manner respectful of privacy rights of individuals.

The fact sheet became a centrepiece for a distinct web resource we created for Canadians. The dedicated section of our website served as an access point for documents and research on the privacy impacts of mega-events such as the Olympics.

As the Games drew to a close, we were satisfied that security officials understood the obligations of enforcement authorities to uphold privacy rights, and that they had carried out their duties accordingly.

We came away convinced that the Vancouver Olympic Games provided a valuable lesson in balancing security and privacy rights at mega-events – lessons that could be refined and applied again at future national or international gatherings on Canadian soil.

2. NATIONAL DNA DATABANK

Our Office continued its efforts to ensure that privacy rights are respected in the use and evolution of the RCMP's National DNA Databank.

The Assistant Commissioner represents the Office's positions as a member of the National DNA Databank's Advisory Committee. Moreover, we have frequently put forward our views to Parliament since the databank was established under the *DNA Identification Act*, which came into force in 2000.

Our Office did not oppose the creation of the databank and we support the safeguards that have been built into the law. For example, genetic and personal data are kept separate, only authorized people have access to the information, and the samples cannot be used for research.

However, we have sounded the alarm over the gradual expansion of the regime to encompass a broader range of offences. The law was originally intended to apply only to serious offences involving violence, but its scope was later widened under the *Anti-Terrorism Act* and other legislation.

In an April 2009 appearance before the Senate Standing Committee on Legal and Constitutional Affairs, the Assistant Commissioner raised a series of concerns. In particular, we are troubled by proposals that would:

- allow authorities to take and bank DNA samples on arrest rather than only on conviction;

- permit familial searches (using the DNA of offenders in the database to identify relatives as possible suspects in a crime); and

- increase international information sharing, especially if it means linking Canada's database to a central system that would give foreign states routine access.

3. RCMP NATIONAL SEX OFFENDER REGISTRY

In May 2009, the RCMP submitted to our Office a Privacy Impact Assessment related to the National Sex Offender Registry. The registry had, in fact, been established five years earlier under the *Sex Offender Information Registration Act*, so the Privacy Impact Assessment clearly failed the test of timeliness.

The assessment put forward the privacy considerations related to the existing form of the registry and focused primarily on the registry's technological infrastructure. Although late, it did address some of the concerns we expressed about the internal handling and verification of personal information, as well as greater transparency about the operation of the program.

Still, there were notable gaps in the RCMP's analysis. For instance, it did not discuss Bill C-34, legislation to broaden the scope of the registry, which was making its way through Parliament at the time. The legislation has since been reintroduced in the Senate as Bill S-2.

The Privacy Impact Assessment we reviewed also failed to provide information about the extent to which the registry is used, and whether it is effective in preventing or solving sexual offences.

The proposed expansion of the registry remains of concern to our Office. In April 2009, we appeared before the House of Commons Standing Committee on Public Safety and National Security, which was conducting a statutory review of the *Sex Offender Information Registration Act*.

We raised concerns about transparency and the information that is available about the registry, which at the time had been operational for almost 10 years.

We also called for a formal and independent evaluation of the effectiveness of the registry by an independent third party. Some academics and the Auditor General of Ontario are among critics who have questioned the effectiveness of registries in reducing sexual crimes or helping investigators solve them.

Indeed, the RCMP officer in charge of the national Sex Offender Registry told the same committee that the registry had not helped in any cases where the crime was unsolved and the offender was unknown. In a few cases where the suspect was already known to investigators, the registry had furnished updated information, such as a photograph or address.

We have encouraged the RCMP to undertake a new Privacy Impact Assessment for any plans to expand the existing registry, and to do so in a more timely fashion than before.

4. RCMP Automated Licence Plate Recognition Program

The Automated Licence Plate Recognition program is a joint initiative involving British Columbia's Ministry of the Solicitor General and the B.C. RCMP police services, including the major crimes unit and the Integrated Municipal/Provincial Auto Crime Team.

The program uses video cameras mounted on marked and unmarked police vehicles, coupled with pattern recognition software, to read, record and identify licence plates on parked and moving cars on B.C. highways. The plates are automatically run against databases containing information on stolen vehicles, suspended drivers and uninsured vehicles. A match triggers further investigation and police intervention.

Our review of a Privacy Impact Assessment from the RCMP turned up concerns. For example, while traditional traffic surveillance technologies capture specific infractions such as speeding or running red lights, the automated plate recognition program captures information on all vehicles within camera range, even in the absence of any infraction. This incidental data was referred to as "non-hit" information.

It is our view that general and ubiquitous surveillance, without adequate safeguards, could undermine the capacity of law-abiding Canadians to maintain anonymity in their daily lives. Similar programs in the United Kingdom have been criticized for targeting individuals for police questioning merely because their cars were spotted near protests.

We challenged the RCMP to demonstrate that the program is needed to meet a real, pressing and substantial problem. We also urged them to clearly inform the public about the program and the uses of the information, to reduce the amount of information collected, and to restrict the databases against which it can be matched.

A response from the RCMP indicated that the program was modified to incorporate many of our recommendations. For example, the RCMP agreed to stop retaining "non-hit" information for this iteration of the program.

However the RCMP argued that such information could prove valuable and may need to be kept in future. In that case, the RCMP would submit a new Privacy Impact Assessment to our Office to justify this plan.

In light of our ongoing concerns, we will continue to watch this project closely.

3.3 LAWFUL ACCESS

Substantial amounts of effort in 2009-2010 were devoted to the analysis of a package of legislative proposals that aimed, collectively, to strengthen the power of police and security officials to extract from electronic communications the information they can use to fight crime.

In June 2009, the government introduced Bills C-46, the *Investigative Powers for the 21st Century Act,* and C-47, the *Technical Assistance for Law Enforcement in the 21st Century Act*.

The legislation, which raised serious privacy issues, passed second reading and was referred to committee. Like all government-sponsored bills, these died on the order paper when Parliament was prorogued in December 2009. However, by the end of the fiscal year, it appeared that similar legislation could be reintroduced in the new session.

In conjunction with Bill C-58 (which has since been reintroduced as C-22) to curb child pornography and Bill C-31 to speed up warrant approvals, Bills C-46 and C-47 aimed to alert authorities quickly to illegal online activities, give police tools for the preservation of data to be used as evidence, allow investigators to trace digital transactions and communications, and ensure that police and security agencies could intercept a new generation of communications.

Bills C-46 and C-47, referred to as lawful access legislation, would apply to a broad range of telecommunications service providers operating in Canada, from Facebook and Google to Rogers and Telus. Newer tools, such as online chat, peer-to-peer messaging and Voice-over-Internet-Protocol services such as Skype, would all fall under the new umbrella, as would PIN-to-PIN messaging on BlackBerrys or text messaging on mobiles.

The legislation would also give authorities the power to demand the preservation of communications data covering a specified period, for possible release to other government investigators in Canada or abroad.

Of significant concern to us was that, for access to records related to a subscriber's identity, including full name, home address, e-mail, phone number or IP addresses, investigators would not need judicial authorization.

OPC RESPONSE

Over the summer of 2009, our Office met with experts in surveillance and interception, including officials from the Department of Justice and Public Safety Canada, the telecommunications industry, law enforcement, civil society groups, as well as experts in the fields of information policy, network security and intelligence operations.

In September, privacy commissioners and ombudsmen from across Canada met in St. John's, NL, where they unanimously supported a joint resolution urging lawmakers to exercise caution as they consider this legislation.

The communiqué asked Parliament to ensure the necessity of and justification for the new powers, and called on them to consider their scope and invasiveness. Legislators were also urged to strengthen the provisions for oversight and to provide for annual public reporting on the use and effectiveness of the new powers.

By late October, both bills had been debated in the House and referred to the Standing Committee on Public Safety and National Security. The Commissioner wrote to the committee ahead of time, outlining some of our immediate concerns and committing to develop further materials for MPs to consider during their detailed study of the legislation.

In her letter, the Commissioner underlined that there was no clear evidence to demonstrate the necessity of the sweeping changes. She also noted that international obligations, such as the European Community Convention on Cybercrime, could be met without eroding privacy protections of Canadians, that lowering legal thresholds for the use of invasive powers raised the potential for unnecessary breaches of privacy, and that the proposed review mechanisms and reporting requirement were inadequate.

The Commissioner emphasized that the Office understands the challenges faced by law enforcement and national security authorities at a time of rapidly changing communications technologies. Even so, whenever new surveillance powers or programs are proposed, the government must demonstrate that the measures are necessary, effective and proportionate to the invasion of privacy. They must, moreover, be the least invasive alternative available.

3.4 OTHER PARLIAMENTARY ACTIVITIES

1. REVIEWS OF DRAFT LEGISLATION

Aside from the telecommunications bills, our Office was engaged in the examination of several other pieces of legislation during 2009-2010. Here are some of the legislative initiatives we studied:

- **Bill C-4, amendments to the *Criminal Code* on identity theft and related misconduct.** We supported this bill in appearances before both Senate and House committees. The legislation received Royal Assent in October 2009.

- **Bill C-6, the *Canadian Consumer Product Safety Act*.** We appeared before the Senate on this bill, which was at third reading in the Senate before prorogation. The bill would have allowed Health Canada to build a database and share more information. We were generally satisfied with the safeguards proposed by the department.

- **Bill C-11, *an Act to Promote Safety and Security with Respect to Human Pathogens and Toxins*.** In an appearance before the Senate, we commented on the proposed safeguards and implications of gathering health information. The bill, which increased Health Canada's capacity to conduct public health surveillance, received Royal Assent in June 2009.

- **Bill C-31, amending the *Criminal Code*, the *Identification of Criminals Act* and other legislation.** This bill, which would have expanded the use of telephone warrants for a range of government investigatory powers, received second reading in the House, was debated and referred to a special legislative committee in late November 2009. The committee was planning to hear witnesses on the issue of fingerprinting upon arrest and related Charter issues. The bill, however, died on the order paper at prorogation.

2. INFORMAL LEGISLATIVE REVIEWS

Our Office also conducted informal reviews of the privacy implications of the following:

- C-9 – proposed amendments to the *Transportation of Dangerous Goods Act*, related to security clearances for transportation workers

- C-14 – proposed *Criminal Code* amendments to enable police to seek to have preventative arrest or restrictive release conditions applied to previously convicted gang members or terrorists

- C-19 – proposed *Criminal Code* amendments related to compelling testimony in investigative hearings and enforcing recognizance with conditions on suspects in terrorism cases

- C-34 – proposed *Protecting Victims From Sex Offenders Act* to broaden the scope of the National Sex Offender Registry

- C-43 – proposed *Strengthening Canada's Corrections System Act,* which would broaden the circumstances in which the Correctional Service of Canada could disclose information about prisoners

3. OTHER PARLIAMENTARY APPEARANCES

Aside from formal and informal meetings with parliamentarians, we discussed privacy issues with MPs and Senators at several Parliamentary committee appearances. These included:

- the Senate Standing Committee on Legal and Constitutional Affairs on the provisions and operation of the *DNA Identification Act*
- the House of Commons Standing Committee on Public Safety and National Security on the statutory review of the *Sex Offender Information Registration Act*
- the House of Commons Standing Committee on Public Safety and National Security on the review and oversight system for national security bodies
- the House of Commons Standing Committee on Access to Information, Privacy and Ethics on reform of the *Privacy Act*
- the House of Commons Standing Committee on Justice and Human Rights and the Senate Standing Committee on Legal and Constitutional Affairs on *Criminal Code* amendments related to identity theft
- the Senate Standing Committee on Social Affairs, Science and Technology on Bill C-6, the *Canada Consumer Product Safety Act*
- the Senate Standing Committee on Transport and Communications on emerging information and communications technologies.

4. PRIVACY ACT RENEWAL

Our capacity to serve Canadians is enabled by our legislated powers and authorities that, in the case of the public sector, are set out in the *Privacy Act*.

Enacted in 1983, the legislation was put in place when telex machines and typewriters still dominated government offices. Although it was considered progressive for its time because it drew on European standards for privacy protection, it is today a statute showing its age.

And so it was with great enthusiasm that our Office shared ideas for modernizing the law with the House of Commons Standing Committee on Access to Information, Privacy and Ethics in hearings, document exchanges and informal meetings.

This collaboration spanned two years and three Parliamentary sessions, with committee members also hearing from experts across government, academia and civil society. The study culminated in the committee's June 2009 publication of a report on the state of the law, titled *The* Privacy Act*: First Steps Towards Renewal*. We greatly appreciate the energy and effort that all members of the committee invested in examining our recommendations.

We were therefore disappointed when the Minister of Justice responded by stating that existing privacy protections under the *Privacy Act* and the *Charter of Rights and Freedoms* are sufficient.

We continue to believe that substantive revisions to the *Privacy Act* will be necessary to fully safeguard the privacy rights of Canadians in this increasingly challenging era of technology, national security pressures and global data flows.

In the meantime, we have been exploring administrative measures that we hope will address some of the more immediate shortcomings in the legislation.

5. ADMINISTRATIVE MEASURES

Until comprehensive updates to the *Privacy Act* are made, our Office is forging ahead with administrative solutions to some of our most pressing concerns. During 2009-2010, we resolved to move ahead with measures including:

- efforts to increase data breach notification and holding departments and agencies accountable for this transparency;
- a streamlined complaint resolution process, including a possible grouping of complaints to achieve greater systemic impact;
- new criteria requiring Privacy Impact Assessments to demonstrate that a potentially privacy-intrusive measure is both necessary and effective, that the infringement on privacy is proportionate, and that no less privacy-intrusive alternatives exist; and
- the development of broad-based training to sensitize federal public servants about their obligations under the *Privacy Act*.

As the new fiscal year got underway, our Office continued to engage in a fruitful dialogue with the Treasury Board Secretariat and the Canada School of Public Service.

CHAPTER 4: MEETING THE CONCERNS OF CANADIANS

Our work with inquiries, complaints and the law

One of the most significant ways in which the Office of the Privacy Commissioner of Canada serves Canadians is by responding to their concerns about privacy and the protection of their personal information.

Sometimes we are able to help them simply by answering a question or two. At other times, we intervene in a disagreement between them and a government institution, with an eye to resolving the dispute in the timeliest and most appropriate manner for all parties.

Even so, matters can and do continue to evolve into formal complaints that we address in a number of ways, including full investigations. On rare occasions, issues even have to be ironed out in Federal Court.

The past fiscal year marked a turning point for our Investigation and Inquiries Branch because we eliminated a staggering backlog of older files and re-engineered our processes to avoid backsliding.

This chapter describes our activities in the areas of inquiries and complaints resolution, the changes in our internal processes, and our legal work.

4.1 INQUIRIES AND EARLY RESOLUTION OF COMPLAINTS

In 2009-2010, we received calls and letters from Canadians inquiring about 2,572 privacy-related matters arising from their dealings with the Government of Canada. We received a further 2,868 inquiries last year about issues that related to privacy, but where it was unclear whether the public- or the private-sector privacy law applied.

The total of these inquiries was down 18 percent from just two years earlier. Since the number of visits to our various Office websites and blogs swelled by 1.58 million between 2007-2008 and 2009-2010, we can surmise that more people are going online to find answers to their privacy-related questions. We have encouraged this trend by

revamping our digital presence and posting a broad range of information and resources for various target audiences.

Our inquiries unit responded to 2,643 inquiries related directly to the *Privacy Act* in 2009-2010, and another 2,878 where the applicable law could not be determined. This was virtually unchanged from the previous year. (See Appendix 3 for full statistics.)

Over the past year, we have been working to refine our inquiries classification system. Once implemented, it will better capture accurate information on priority concerns and trends.

But, even without those details, it is clear that people contact us most commonly because they are having trouble accessing their personal information in the hands of government. Questions about the collection, use or disclosure of personal information combine to yield just about as many calls and letters.

Controversies reported in the media also tend to generate spikes in inquiries. Over the past year, for instance, we were contacted about the new full-body security scanners at airports, the federal Passenger Protect Program (better known as the no-fly list), a client-satisfaction survey conducted by a polling firm on behalf of the Canadian Firearms Program, and a balloon-borne border surveillance initiative operated by a U.S. company.

EXPANDED ROLE FOR INQUIRIES OFFICERS

Inquiries officers are often able to answer people's questions or concerns immediately. Alternatively, they may direct them to other sources of information or assistance, such as the access-to-information and privacy co-ordinators at the relevant government departments.

In many instances, the key lies in clarifying the caller's concerns. With further probing, for example, it may emerge that the issue should be addressed by a different jurisdiction.

If it is clear that the matter falls within our jurisdiction, our inquiries officers explain what we can do within the limits of our authority. They also discuss the exceptions and exemptions under the law that could explain to the caller's satisfaction why a department behaved as it did.

There are also instances when we can inform callers about previous cases that set useful precedents. Equipped with that information, individuals may be able to go back to the department to press for their rights.

Not uncommonly, our officials contact representatives at the subject department to advise them that an issue is brewing. Departments will often work with us to resolve issues informally and quickly.

EARLY RESOLUTION

Indeed, wherever possible, we aim for a speedy resolution of people's concerns, in the belief that a timely response is generally better than letting problems fester.

If, however, it is clear that an individual wishes to proceed to the complaint stage, the inquiries officer makes sure to collect contact information and details of the allegation, so as to expedite the ensuing investigation.

Over the past fiscal year, we also refined our efforts to resolve complaints without the need for a formal investigation. An early-resolution officer was designated to take charge of that task.

We found that the officer was often able to handle a file simply by informing the complainant about similar cases we have investigated in the past. For example, if departments in similar cases in the past were found to have complied with the *Privacy Act*, complainants tend to accept that there is no point in proceeding with another investigation.

Some complaints about access to personal information are also resolved in this way when the early-resolution officer is able to demonstrate that the department acted properly in the way it applied statutory exemptions to the release of personal information.

In all, 68 complaint files were formally closed as "early resolution" cases in 2009-2010, up from 42 the year before. In another 93 instances, the matter was settled during the course of the investigation. In a further 149 cases, complainants chose to discontinue their complaints.

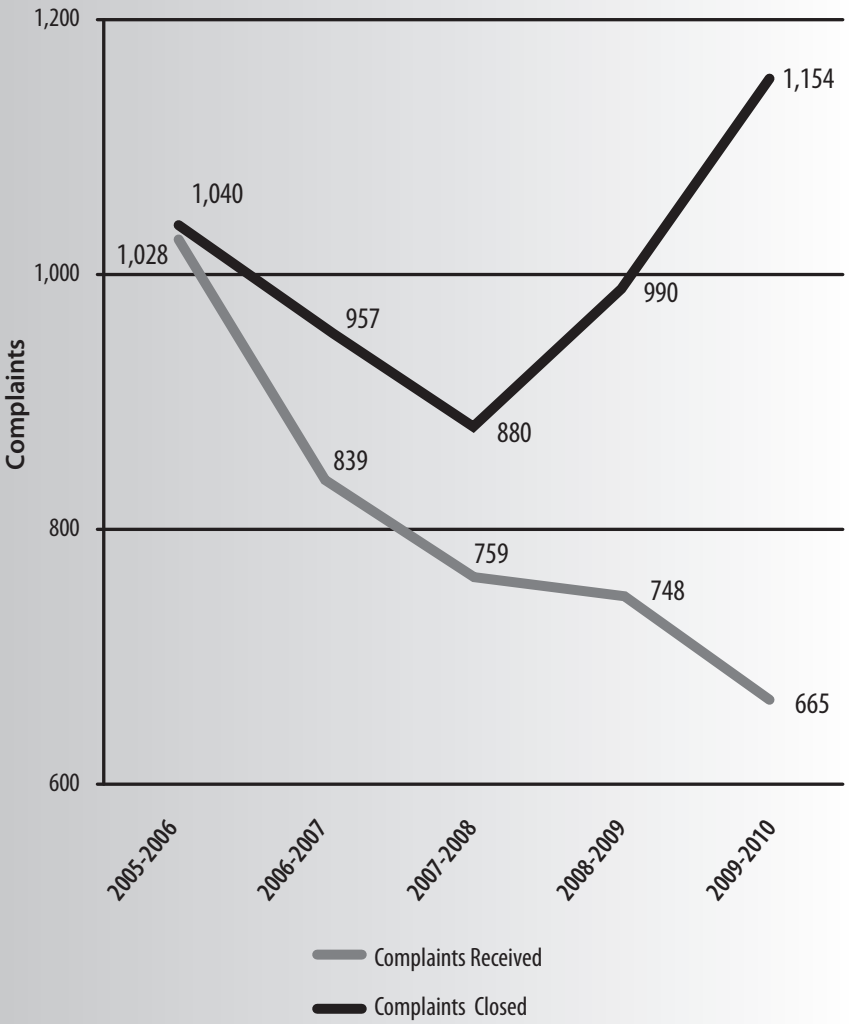
While early resolution can be beneficial for all parties, it is not always appropriate. Some issues are too complex, or appear on their face to involve an egregious privacy violation. Others point to systemic problems. The complaints registrar, who is responsible for conducting triage on incoming complaints, refers cases of that nature directly to an investigator.

4.2 COMPLAINTS AND INVESTIGATIONS

COMPLAINTS RECEIVED

By trying to resolve concerns at the front end, the number of formal complaints lodged with our Office continued to decline. In 2009-2010, we received 665 complaints under the *Privacy Act*, down 11 percent from the year before and 36 percent from five years earlier.

Five-year Overview of Complaints Received and Closed



The largest share of complaints originated in Ontario (35 percent), British Columbia (23 percent) and Quebec (13 percent). Six in 10 of the complaints from B.C. and Alberta were lodged by prisoners and others against the Correctional Service of Canada.

Canadians living abroad have the same rights of access to their personal information as those living in Canada, and nine people chose to exercise those rights in 2009-2010.

As in previous years, the most common types of complaints related to the time it took for a department or agency to respond to a request for access to personal information (44 percent of complaints), and to other difficulties that people encountered in gaining access to their information (38 percent of complaints).

The remaining 18 percent of complaints related to the collection, use, disclosure or retention of personal information by government departments or agencies.[2]

Most Common Complaint Types Received

	Number	Percentage
Time Limits: Concerns that an institution took too long to respond to a request for access to personal information	292	44
Access: Difficulties gaining access to personal information	251	38
Privacy: Concerns about an institution's collection, use, disclosure, retention or disposal of personal information	122	18
Total	**665**	**100**

The number of complaints filed against an institution does not necessarily mean the organization is not compliant with the *Privacy Act*. Because of their mandates, some institutions are required to hold a substantial amount of personal information. Therefore, they are more likely to receive numerous requests for access to that information, which may, in turn, lead to complaints about the way the data is handled.

As in other years, the largest number of complaints we received (290, or 44 percent of the total) were laid against the Correctional Service of Canada. Two-thirds of those complaints related to the time it took for the federal prison authority to respond to requests for personal information.

The Royal Canadian Mounted Police (RCMP), the Canada Revenue Agency and the Department of National Defence were next, with 60, 49 and 47 complaints, respectively.

[2] Detailed data tables are in Appendix 3.

While the Correctional Service of Canada actually saw a 16 percent increase in complaint numbers since 2008-2009, some departments, including Human Resources and Skills Development Canada, Citizenship and Immigration Canada and the Canada Border Services Agency, saw noteworthy declines.

As discussed elsewhere in this report, our Office met with departments and agencies with higher numbers of complaints, in order to foster a better understanding of their circumstances and how we can help them better meet the privacy expectations of Canadians.

OVERVIEW OF COMPLAINTS CLOSED

In all, we closed 1,154 complaint files in 2009-2010. That was up 17 percent from the year before, and 31 percent from 2007-2008. Last year we closed 489 more complaints than we received, which reflects our determined effort to eliminate a backlog of files older than one year from the date of receipt.

Indeed, we started the fiscal year with 333 backlogged files, and ended it with just 10 cases left to close – and even those were nearing finalization by March 31st.

Even as we closed more cases, our emphasis on early complaint resolution allowed us to shrink the time it took to resolve each one, from a weighted average of 19.5 months in 2008-2009 to 12.9 months in 2009-2010.

In 400 of the cases we closed (a little more than one-third), some or all of the allegations made by the complainants were determined upon investigation to be well founded. In two-thirds of the files, the complaint centred on the time it took for a government institution to respond to a request for personal information.

In a further 56 well-founded complaints, the government agreed to take corrective action. All but two of those cases, which we categorize as "well founded and resolved," involved complaints about a denial of access to personal information.

A small minority of cases (37, or 3 percent of the total), were classed as "resolved," after a thorough investigation traced the problem back to a misunderstanding. In these instances, we found that the allegation was justified but a negotiated settlement was possible.

In 30 percent of the cases, meanwhile, the allegations could not be substantiated and we issued a finding of not well founded.

Other cases were closed without the completion of a formal investigation, either because the case was resolved before an investigator was assigned (6 percent), the matter was settled during the investigation (8 percent), or the complainant dropped the case (13 percent).

COMPLAINT TYPES CLOSED

Access – The most common type of complaint we handled last year related to problems people encountered in accessing their own personal information in the hands of the federal government. In all we closed 549 such complaints, nearly half of our entire caseload.

In one-third of these access cases, complainants dropped their complaints or settled the matter before an investigation was completed. This indicates that many complainants accepted that they could not receive the documents they were seeking because exemptions permitted under the *Privacy Act* had been properly applied.

The remaining 361 access complaints went on to be investigated, but three-quarters of them were determined not to have been well founded. Of the 64 cases that were upheld as well founded, 54 were resolved by the institution at the conclusion of the investigation.

A further 28 access cases were investigated and found to have merit, but were resolved through negotiation.

Time limits – Complaints about the time it took for government institutions to respond to requests for personal information comprised the second most common category of files we closed last year—27 percent of our caseload.

We upheld as well founded nearly 85 percent of the 314 time-limit complaints we closed during the year. This is not surprising because complaints are usually only filed after an institution's statutory deadline to respond to a request for personal information has passed. If the deadline for a response has been missed, a complaint about undue delay is substantiated practically by definition.

Of all the time-limit complaints we closed last year, 71 percent were directed against the Correctional Service of Canada. Even though the institution received an increase in resources two years ago to deal with this issue, the situation continues to worsen. In 2008-2009, 45 percent of all time-limit complaints (99 of 221) were directed against the federal corrections service. While that marked an improvement over the year before, when half (174 of 346) of all complaints in this category involved the Correctional Service of Canada, the trend reversed again for 2009-2010.

The department holds large volumes of personal information about inmates, who in turn file numerous requests for their information.

Privacy – Privacy complaints (those involving the collection, use, disclosure, retention or disposal of personal information) combined to account for another one-quarter of all complaints we investigated.

Of those 291 cases, fewer than half (43 percent) were determined to be well founded, or well founded and resolved. In the vast majority of those files, the issue related to the improper use or disclosure of personal information.

Detailed statistics on the disposition of all complaints can be found in Appendix 3.

COMMON RISKS

In the course of our investigations, we continued to be troubled by a risk factor that recurs year in and year out: the mishandling of personal information. This is most commonly traced back to simple inadvertence or inadequate procedures. We did, however, also encounter plain wrongdoing.

As in other years, there were also instances in which we were able to pin the problem on technology – whether a programming error, inadequate protection of data, or ordinary mechanical equipment failure.

In an effort to stem the more systemic problems, we invested substantial efforts in prevention. We met with departments and agencies to foster a better understanding of their challenges and our expectations for the protection of personal information.

DATA BREACHES

We also underscored the importance of notifying us of data breaches. Indeed, over the past few years, our Office has made substantial efforts to gain a better handle on unauthorized disclosures of personal information.

In the past fiscal year, 38 data breaches were reported to us by federal departments or agencies, slightly fewer than the average over the past five years.

As in other years, breaches were most likely to originate in the way organizations managed data. Our investigations turned up flaws in procedures that sometimes led to the unauthorized exposure of personal information, often through human error. There were also some technical glitches.

The next section describes key cases closed by our Investigation and Inquiries Branch in 2009-2010, followed in section 4.4 by a discussion on progress in the area of data breach notification.

The chapter continues with an update on our efforts to improve service to the public by eliminating our investigation backlog and streamlining and modernizing our internal processes (section 4.5).

The chapter ends with an overview of our work in the courts (section 4.6), and in relation to administrative tribunals (section 4.7), as well as our own Office's handling of access-to-information and privacy complaints (section 4.8).

4.3 SPOTLIGHT ON CASES

RISK: DATA-MANAGEMENT PROCEDURES

Federal departments and agencies handle huge amounts of personal information of Canadians, mostly in privacy-sensitive ways. Even so, the sheer volume of data in government hands introduces the risk that personal information may be inappropriately disclosed.

Indeed, the single biggest source of use and disclosure complaints investigated by our Office could be traced back to the way government institutions handle personal information.

In some cases, our investigations determined that the institution had appropriate procedures that were properly followed. In other instances, however, we discovered that faulty procedures and even deliberate malfeasance led to the wrongful exposure of personal information.

1. INTERNET POSTING HIGHLIGHTS INAPPROPRIATE ACCESS TO TAX RECORDS BY CRA WORKERS

In the wake of allegations in the media that personal tax information of several high-profile sports figures was being posted to an Internet chat group by a Canada Revenue Agency employee, the Commissioner initiated a complaint and this Office launched an investigation.

We found that a former Canada Revenue Agency employee had posted to the chat group personal information of this nature, which he appears to have gleaned over his years with the agency. We further confirmed that other agency employees in various tax centres, likely motivated by curiosity, also inappropriately accessed the tax information of these athletes.

There was no evidence that the employees who accessed the information had disclosed it to outside sources – and in particular to the former staffer who had posted the

information on the Internet. Therefore, we could not issue a finding on that portion of the complaint.

Even so, accessing people's personal tax information without authorization and for purposes unrelated to the employee's duties constitutes a breach of the *Privacy Act*.

Accordingly, the portion of the complaint dealing with the improper use of personal information by Canada Revenue Agency employees was well founded.

The Canada Revenue Agency advised us that it suspended one of the employees who accessed the personal tax data of these individuals without authorization, and fired two others. The agency also implemented corrective measures, including modernizing the National Audit Trail system, in order to better monitor employee access to computer systems containing taxpayer information.

2. TORONTO PORT AUTHORITY WORKER MISUSES PERSONAL DATA FOR POLITICAL FUNDRAISER

A Member of Parliament complained that an employee of the Toronto Port Authority improperly used the organization's e-mail database to invite people to a fundraising event for another MP.

Our investigation determined that a port authority employee sent an e-mail to approximately 60 people, soliciting a financial donation and inviting their participation at a fundraising function. Recipient addresses were all confined to the "bcc" (blind carbon copy) field of the e-mail, where they could not be viewed by other recipients. In the signature block, however, the employee was identified as working for the Toronto Port Authority, which left the impression that the organization sanctioned the correspondence.

Our investigation found that the employee obtained the e-mail addresses from business cards, which we established are records collected by, and under the control of, the port authority. The employee selected both business and personal addresses for the mass e-mailing. We take the view that "personal" (typically home) addresses constitute personal information.

We determined that the employee had used this personal information without the knowledge or authorization of the port authority, and for reasons unrelated to the organization's business activities.

We therefore concluded that the complaint was well founded.

The Toronto Port Authority reminded employees of their responsibilities for the acceptable use of information under the control of the institution. The organization also pledged to give its workers training on the *Privacy Act*.

We were satisfied that appropriate corrective measures were taken to prevent a recurrence of this type of incident. Consequently, no further recommendations were made.

3. RCMP and private polling firm safeguarded data on gun licensees

As a result of several complaints and media coverage, the Commissioner initiated a complaint against the Royal Canadian Mounted Police (RCMP) in October 2009. At issue was the handling of personal information that had been collected by the RCMP's Canadian Firearms Program, and used by EKOS Research Associates Inc. to survey firearms licensees about their dealings with the program.

The RCMP gave the public opinion research firm contact information for gun licence holders and the polling firm interviewed 1,270 individuals in September 2009. Respondents consented to participate in the survey and were advised that they could stop the interview at any time.

Our investigation showed that, in addition to customer-satisfaction questions, EKOS collected some demographic data, along with information on the guns owned by survey respondents.

In its report to the firearms program, EKOS provided no identifying data about respondents, other than their age and gender. EKOS also returned to the RCMP all data and documentation associated with the project.

We further found that EKOS met all RCMP and Government of Canada contractual requirements on the secure and confidential handling of personal information.

In applying the *Privacy Act* to these observations, the Assistant Commissioner was satisfied that the Canadian Firearms Program is authorized to collect personal information for the purpose of administering and enforcing the *Firearms Act*. Using that information to conduct a client-satisfaction survey to improve the program's services is consistent with the purpose for which the information was initially collected, and therefore complies with the Act.

Moreover, the RCMP was found to be compliant with the Act when it provided EKOS with personal information allowing the polling company to carry out its activities

because the contract contained the same confidentiality and security provisions that bind regular employees of the contracting institution.

As a consequence, the complaint was determined to be not well founded.

Even so, we concluded that the RCMP could have done some things better. We recommended that the Canada Firearms Centre, which was created in 1996 to administer the firearms program, clarify its public information on the actual and potential uses of the personal information it collects.

Program officials also acknowledged that a Privacy Impact Assessment could have helped ensure that all privacy issues were identified, mitigated or resolved before the project was launched.

4. INNOCENT TARGETS OF WHISTLEBLOWER LAW SHOULD LEARN OF VINDICATION

A public servant complained that she was unable to access her personal information, which had been collected by Public Works and Government Services Canada in the course of an investigation under the *Public Servants Disclosure Protection Act*, better known as the whistleblower law.

The department's investigation into an allegation of wrongdoing under the legislation completely exonerated the individual. She was not, however, informed of this outcome. After trying unsuccessfully to obtain access to the personal information that had been collected about her in connection with the inquiry, she complained to our Office.

We determined that section 22.3 of the *Privacy Act* had been applied correctly. It states that a department head shall refuse to disclose personal information that was created for the purpose of making a disclosure under the *Public Servants Disclosure Protection Act*, or for a related investigation.

We therefore determined that the complaint was not well founded.

Even so, we were disturbed that people accused of wrongdoing under the whistleblower law are not told when an investigation finds them innocent of the charges. The consequences of a false accusation of malfeasance can be extremely serious, for the individual concerned and for the workplace in general.

Consequently, we urged Public Works and Government Services Canada to inform the subjects of inquiries when allegations of wrongdoing are unsubstantiated. Nearly a year after completing its investigation, the department advised the individual in writing that none of the allegations made against her had been proven.

In the interests of procedural fairness and natural justice, the Commissioner also asked the Treasury Board Secretariat to develop mechanisms to enable departments and agencies to inform all affected individuals when an allegation of wrongdoing is unsubstantiated. Although Treasury Board had urged senior officials of departments and agencies to do so shortly before the whistleblower law came into force in 2007, no guidelines to that effect have been published.

5. PERSONAL DATA OF 191 EI CLAIMANTS DISCLOSED

Our Office received 82 complaints after the Quebec regional office of Human Resources and Skills Development Canada inadvertently disclosed to an individual the personal information of 191 others.

The case involved a group of employees who had claimed employment insurance (EI) following a labour action. One individual, in appealing the denial of his claim, was furnished with an appeal docket to enable him to prepare for his hearing before the EI Board of Referees.

The package, however, accidentally included the names, dates of birth, employee identification numbers and Social Insurance Numbers of the individual's 191 fellow employees. The investigation also established that a second list, containing the employment and leave status of certain employees, was also inadvertently disclosed.

Of the 82 complaints we received, our investigation confirmed in 79 instances that the information had, indeed, been released and the complaints were therefore well founded. Two instances were not well founded and one case was discontinued.

Officials of Human Resources and Skills Development Canada moved quickly to retrieve the improperly disclosed data, notify the affected parties, and advise them on reducing their risks of identity theft. The individuals were also given the name of a contact person at the department.

The department notified our Office of the breach and flagged the Social Insurance Numbers of the affected individuals, so that the Social Insurance Registration Office in Bathurst, N.B., could monitor the numbers for fraudulent activity.

Human Resources and Skills Development Canada also took steps to prevent a similar recurrence in future. It reminded officials with its Quebec regional office about proper procedures for protecting personal information while processing appeals to the EI Board of Referees.

6. SASKATCHEWAN PENITENTIARY SUFFERS DATA BREACHES

During 2009-2010, our Office received several reports about unauthorized disclosures of personal information of inmates at the Saskatchewan Penitentiary. In last year's annual report, we recounted an incident in which the personal information of 184 of the same institution's prisoners was found in the garbage.

Here are two incidents reported to our Office from the Saskatchewan prison over the past fiscal year:

- An inmate found 25 interview authorization forms in the penitentiary trash. The forms contained the names and fingerprint identifier numbers of inmates and details on the timing and location of their authorized interviews. The inmate claimed there were many other forms in the garbage, but he only retrieved enough to convince our Office that the prison should be more careful with personal information.

- An inmate submitted a proposal to management. When it was returned to him by Correctional Service of Canada staff, it contained the personal information of 13 other inmates, including their names and fingerprint identification numbers.

Correctional Service of Canada undertook to remind staff of the need for diligence when creating, using and disposing of sensitive or protected information. It also committed to reminding them that inmates or other individuals affected by a data breach have the right to complain to our Office.

7. PROCESSING OF ACCESS TO INFORMATION REQUESTS SPARKS ACCIDENTAL DISCLOSURES

As in previous annual reports, we found again over the past year that personal information has been disclosed, often to the media, during the processing of access to information requests. The errors were usually attributed to the high volume of data being handled.

Here are some examples of incidents that came to our attention during 2009-2010:

- The Correctional Service of Canada reported that the personal information of an inmate detained in New Brunswick had been inadvertently disclosed to the media in response to an access to information request. The department said it had adequately protected the inmate's name, location and other personal identifiers.

However, other information that was released could, by deductive reasoning, serve to identify him and, in fact, his name subsequently appeared in several news articles.

Our Office reminded the Correctional Service of Canada to carefully review and evaluate all information before release, to reduce the chances that the simple association of other information would lead to the identification of an individual.

In response to our other recommendations, the institution notified the inmate of the breach of his personal information and advised him of his right to complain to our Office. He was also informed that corrective measures had been taken to reduce the likelihood of similar incidents in future.

- Personal information of nine people who had written to various elected representatives on other matters was accidentally disclosed when Transport Canada responded to a request for information under the *Access to Information Act*. The personal information was not published in the resulting media articles.

Transport Canada informed the affected parties about the breach and advised them of their right to complain to our Office. The department also asked the reporter who received the personal information in error to return the package.

Further, Transport Canada's access to information and privacy officials introduced new quality control measures to reduce the chances of error in processing and mailing responses to requests for access to information.

- As a result of a filing error, Canada Post inadvertently released 36 pages of medical information of a retired employee in response to a request for access to information. The information had been held by a disability management provider and was released to another Canada Post employee by the same name.

All of the information released in error was returned to the disability management provider and the company was reminded of its responsibilities to safeguard personal information entrusted to it. The affected individual was notified of the disclosure and was advised of the right to complain to this Office.

8. UPDATE: CITIZENSHIP AND IMMIGRATION CANADA ADDRESSES LONGSTANDING PRIVACY CONCERN

We reported last year on a case involving the collection of personal information by Citizenship and Immigration Canada as part of its application process for temporary resident visas. The complainant, who was sponsoring a relative's application, protested

that he wanted to be able to submit his financial records in support of the application directly to the department, rather than indirectly through the relative.

Although the case was satisfactorily settled, our Office was disturbed that similar complaints had come to our attention as far back as 1998. We therefore exercised our ombudsman powers to persuade the department to change its procedures.

In a November 2009 letter, the deputy minister of Citizenship and Immigration Canada confirmed that Canadians sponsoring applicants for temporary resident visas can now choose to supply personal supporting documentation, such as tax assessments or bank statements, directly to the department. This option serves as an alternative for sponsors who do not wish to hand their personal information to the applicants to submit. The new policy was conveyed to overseas missions and publicized on the department's website.

RISK: TECHNOLOGY

Pervasive in the modern world, technology is integral to government operations. And yet all equipment, from basic mechanical machines to sophisticated computer systems, is vulnerable to malfunctions. It is therefore no surprise that, every year, incidents come to our attention in which the personal information of Canadians is put at risk through technological defects. In some cases, the problems lead to accidental disclosures; in others, they are deliberately exploited.

1. HACKER TARGETS ONLINE COMPLAINTS TO CANADA POST OMBUDSMAN

In October 2009, a call from a newspaper reporter alerted the Office of the Ombudsman for Canada Post that a computer programming flaw had enabled an unauthorized third party to gain access to personal information submitted through the ombudsman's online complaint system. The data accessed included names, addresses, e-mail addresses and phone numbers of complainants, as well as details of their complaints.

In all, 131 postal service complaints submitted online between Aug. 4 and Sept. 2, 2009 were exposed in the security breach.

Canada Post immediately disabled the website, and notified and apologized to all affected individuals in writing. The website has since been fixed and reactivated.

The organization further advised us that it tests the vulnerability of its computer system annually, but that the computer system in the ombudsman's office fell outside the scope of these reviews. Canada Post committed to including that system in its regular reviews.

2. MECHANICAL MALFUNCTION, COMPOUNDED BY HUMAN ERROR, LEADS TO DATA SPILL

In March 2009, the Quebec processing centre of Human Resources and Skills Development Canada mailed 11,900 forms to applicants for the Guaranteed Income Supplement. Due to a mechanical breakdown in the machine used to print, fold and insert correspondence into envelopes for mass mailings, some people received forms destined for other people, along with their own.

Forty-four cases of the mix-up were reported to the department.

According to our investigation, the forms contained the names of applicants for the supplement (and their spouse, where applicable), addresses, and Social Insurance Numbers, although the SINs were inverted and given an additional code in order to make them difficult to identify. No benefit information was disclosed.

We also determined that human error played a role. The technician overseeing the mass mailing noticed at the outset that some forms were being folded and inserted in duplicate into envelopes. He recalibrated some equipment settings and allowed the job to continue. He did not make use of mechanisms to detect duplicate documents, and did not notify managers of the errors.

The department became aware of the incident when call centre agents began receiving calls from affected individuals. The institution notified our Office in April and the Commissioner initiated a complaint in June.

Following an investigation, the complaint was determined to have been well founded.

Human Resources and Skills Development Canada, which conducted its own investigation into the incident, took steps to improve the functioning of its mailing equipment and to review and strengthen its quality-control procedures.

Because of the technician's silence, our Office further underscored the role that human error had played in compounding the problems created by the mechanical defect. Accordingly, we recommended that the department better sensitize employees to their obligations to safeguard personal information. The department undertook to update its employees' knowledge of the *Privacy Act* and related policies and procedures.

3. MALFUNCTION IN VETERANS AFFAIRS COMPUTER LEADS TO UNAUTHORIZED DATA DISCLOSURE

A computer error led officials at Veterans Affairs Canada to improperly disclose the personal information of several people in response to an access to information request.

The personal information included the names of nine individuals (including the requester) who were erroneously identified as having received $20,000 compensation payments for exposure to dangerous U.S. military defoliants when, in fact, their claims had been denied.

The names of people who received the one-time, tax-free payments related to the testing of unregistered herbicides such as Agent Orange at Canadian Forces Base Gagetown in New Brunswick in 1966 and 1967 are not considered to be personal information as they are listed in the Public Accounts of Canada. However, because the complainants had been denied the compensation, their names in connection to these payments are deemed to be personal information.

In the wake of this breach, Veterans Affairs Canada corrected the system error that led to the disclosure. The affected individuals were also notified and advised of their right to complain to our Office.

4. BORDER AUTHORITY ABSOLVED OF IMPROPERLY GATHERING PERSONAL DATA FROM BLOG

An individual alleged that the Canada Border Services Agency inappropriately collected information from his personal online blog after the agency ended his term position.

The complainant posted information on the Internet of his own accord, which was clearly aimed for public consumption. Nevertheless, he filed several complaints after his tracking device logged evidence that his site had been visited by people using government computers.

Our investigation determined that some government institutions may allow employees to access the Internet on their own time, subject to the government's Acceptable Use Policy. However, browsing a site from a government workstation does not necessarily mean that a department is collecting personal information.

In this instance, it was determined that several Canada Border Services Agency employees had, in fact, viewed the blog, but had done so in a personal capacity that was deemed to accord with the policy. Our investigation found no evidence that the agency had collected personal information in connection with the visits.

Accordingly, the complaints were determined to be not well founded.

RISK: NATIONAL SECURITY

In 2009-2010, the privacy rights of Canadians were repeatedly tested as the federal government took new steps to strengthen national security. Airports and national borders were the focus of many initiatives that involved the collection of personal information. The deployment of full-body scanners and extensive crowd surveillance at the Vancouver Olympic and Paralympic Games were other new security measures with impacts on privacy.

But while such initiatives generated inquiries to our Office, few proceeded to the complaint stage during the reporting period.

BORDER SECURITY AGENT'S QUESTIONS UPSETTING BUT LEGITIMATE

Following his return to Canada from a European vacation in the fall of 2008, a traveller complained that an official of the Canada Border Services Agency had improperly collected his personal information.

The complainant, who had been directed to a secondary inspection, alleged that a border agent asked for the names of his personal contacts in Europe and took notes about the prescription medications found in his baggage.

Our investigation determined that the official collected the information for the sole purpose of enforcing the *Customs Act*, which allows agents to question passengers and to take notes related to their entry into Canada. Border agents may also examine goods brought into the country to ensure public safety and security.

The complaint was determined to be not well founded.

Although the complaint was not well founded, we felt the case illustrates the breadth of the Canada Border Services Agency's powers and the organization's corresponding obligation to ensure respect for privacy in the exercise of those powers.

We suggested that the agency consider how it uses its powers and communicates with the public on matters that touch on privacy. For example, we proposed that the agency encourage its officers to explain to the travelling public, whenever possible, why their personal information is being collected. We noted that the agency delivers a privacy training program across the country, which could serve as a vehicle for sensitizing its officials.

ACCESS TO PERSONAL INFORMATION

BE SPECIFIC ABOUT EXEMPTIONS, CORRECTIONAL SERVICE TOLD

The Canadian Association of Elizabeth Fry Societies complained on behalf of an inmate that the Correctional Service of Canada had refused to provide access to her personal information.

The inmate had given the organization, which works with women and girls in the justice system, permission to act on her behalf in requesting access to her prison records. The original request was submitted to the Correctional Service of Canada in June 2007. When the department did not respond within the permissible 60-day deadline, the organization filed a second request on Oct. 4, 2007.

On Oct. 19, 2007, 123 days after the original request was made, the inmate committed suicide in prison.

When the organization later followed up on its request for the inmate's personal information, the Correctional Service of Canada responded that it was withholding the information in its entirety, pursuant to section 22 of the Act. That section lists several possible reasons under which a government institution may withhold information.

An investigation by our Office found that the Correctional Service of Canada had not specified which paragraph or paragraphs of section 22 it had invoked to support its decision.

In May 2009, the Assistant Privacy Commissioner concluded that section 22 had not been applied properly to exempt the requested information and the complaint was substantiated as well founded.

The Correctional Service of Canada initially declined to turn over the records and the matter was appealed in court. In a ruling released in April 2010, shortly after this reporting period, the Federal Court ordered the institution to disclose the records to the Canadian Association of Elizabeth Fry Societies.

4.4 REPORTING ON DATA BREACHES

Our Office continues to urge departments and agencies to advise us, in line with federal guidelines, of the unauthorized loss or disclosure of personal information.

In the past fiscal year, 38 data breaches were reported to us by federal departments or agencies, slightly fewer than the average over the past five years.

Federal public-sector data breaches reported to OPC 2005-2006 to 2009-2010

2005-2006	55
2006-2007	54
2007-2008	44
2008-2009	26
2009-2010	38

Data breach reporting has many benefits, including promoting the development and use of more privacy-sensitive procedures.

Treasury Board guidelines strongly recommend that departments and agencies inform our Office about unauthorized disclosures of sensitive personal data, as well as mitigation measures planned or undertaken.

Reportable breaches, according to the guidelines, are those that involve sensitive personal data such as financial or medical information, or personal identifiers such as the Social Insurance Number. Breaches are also reportable if they expose individuals to identity theft or other forms of fraud, or cause embarrassment or harm to a person's career, reputation, financial position, health or safety.

Institutions, like many individuals, may be understandably reluctant to confess to errors. And, indeed, only a handful of departments are currently reporting the bulk of incidents.

A privacy breach involves improper or unauthorized collection, use, disclosure, retention and/or disposal of personal information.

A breach may be the result of inadvertent errors or malicious actions by employees, third parties, partners in information-sharing agreements or intruders.

It is strongly recommended that institutions notify the OPC of the breach and of the mitigation measures being implemented, if the breach:

- involves sensitive personal data such as financial or medical information, or personal identifiers such as the Social Insurance Number;
- can result in identity theft or some other related fraud; or
- can otherwise cause harm or embarrassment which would have detrimental effects on the individual's career, reputation, financial position, safety, health or well-being.

Notification should occur as soon as possible after the institution becomes aware of the breach (within days).

When notifying the OPC, provide information as to the nature and extent of the breach, the type of personal information involved, the parties involved, anticipated risks, steps taken or to be taken to notify individuals, and any remedial action taken.

– Excerpts from *Guidelines for Privacy Breaches,* a policy of the Treasury Board of Canada Secretariat http://www.tbs-sct.gc.ca/atip-aiprp/in-ai/in-ai2007/breach-atteint-eng.asp

But, once they overcome their initial discomfort, some departments recognize that there are benefits to breach reporting. For example, if our Office is advised of a breach and the institution's mitigating measures, we are often able to resolve people's concerns in a way that they no longer feel the need to lay a formal complaint against the department.

We have also observed that institutions get better with experience. For example, one organization that reports to us regularly has developed a risk-based analytical approach to determine its course of action in response to a breach.

In the past year, our Office took steps to promote more consistent breach reporting. We now have a dedicated notification officer and phone number that departments and agencies can contact to report breaches and obtain help and guidance.

Here are examples of data breaches reported to our Office during 2009-2010:

1. The Bank of Canada advised us in December 2009 of a technical malfunction that had come to light a little over a month earlier. As a result of the error, seven clients of the Canada Payroll Savings Plan who were using the secure online access website, www.mybonds.gc.ca, were able to see personal information of six other clients who had accessed the site moments before. The information included the other people's names and account numbers.

The trouble was traced back to a technical problem that cropped up during scheduled maintenance. The bank also noted that a similar issue had occurred in June 2009, leading to the disclosure of personal information of a handful of people.

The Bank of Canada informed the affected clients about the incident and reset their passwords. Some accounts were flagged and monitored for inappropriate activity. Clients were also advised to monitor their personal and financial information for signs that it was being misused.

2. In November 2009, Canada Post reported that a package of passport applications, sent by courier from the office of an Ontario Member of Parliament, never arrived at the processing centre of Passport Canada in Gatineau, QC. While the parcel was traced as far as Ottawa, it was never found.

It was unclear exactly who the applicants were, or even how many were affected, as the applications were gathered at a passport event at the MP's constituency office. While it was thought that approximately 50 forms were lost, individuals were only identified when they called Passport Canada to inquire about the progress of their applications.

Canada Post and Passport Canada agreed to a joint plan under which identified individuals would be advised of the situation and offered an expedited passport processing service at no added cost, free credit monitoring and $100 in compensation for replacing lost identity documents.

3. In September 2009, the Office of the Auditor General of Canada discovered that 84 confidential reports about its employees had gone missing after paper versions of the documents had been improperly filed or stored.

The reports, which are submitted by staff in connection with the office's *Code of Values, Ethics and Professional Conduct*, contain personal information including, in some cases, information on reportable assets or conflicts.

The Office of the Auditor General advised our Office in January 2010 that it had notified the affected individuals, and none had raised significant concerns about the breach. The Auditor General's office also pledged to avoid a recurrence of the problem by adopting a paperless process, including the use of encrypted e-mails for employees to submit their reports. A single person would also be tasked with cataloguing and storing the forms on the organization's records-management system.

4.5 MODERNIZING THE PROCESSES

1. REACHING OUT TO FEDERAL INSTITUTIONS

During the past fiscal year, our Office ramped up efforts to engage in constructive dialogue with key departments. The objective was to open lines of communication and better understand one another's requirements.

From our side, it was important to help departments resolve outstanding privacy issues, and to promote the importance of notifying our Office of privacy breaches. We endeavoured to share information on best practices and mechanisms to improve complaint response times.

Departments, for their part, were often eager to convey the complexities they face in the control of personal information.

Approximately 250 federal departments, agencies and Crown corporations currently fall under the *Privacy Act*, so it will be a long time before we visit them all. But, to start, we focused on institutions that, because of the volume of personal information they handle, tend to be the subject of frequent complaints.

In 2009-2010, therefore, we met with officials from the Canada Revenue Agency, the RCMP, Human Resources and Skills Development Canada, and the Correctional Service of Canada.

We are pleased by the outcome of those discussions, and plan to continue meeting with officials of other institutions.

2. RETOOLING BRANCH OPERATIONS

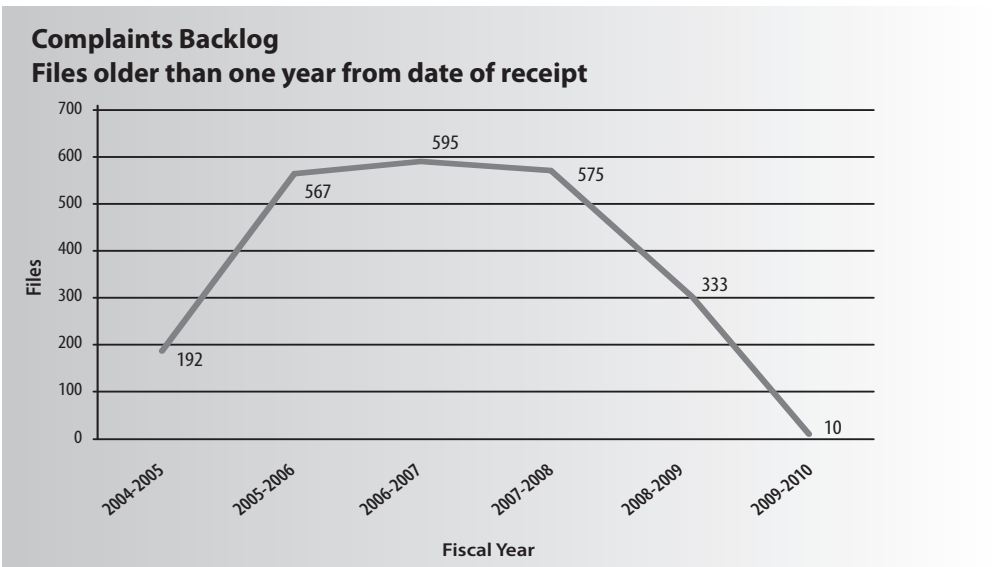
One of our Office's key accomplishments in 2009-2010 was the virtual elimination of our backlog of complaint files that were older than one year from the date of receipt.

In recent years, a shortage of investigators, combined with an increasing number of complaints dealing with highly complex issues, had led to a backlog that reached a high of 595 in 2006-2007.

Dealing with the backlog has been one of our Office's top priorities. With the receipt of additional financial resources from Treasury Board, our backlog reduction initiative began in earnest in 2008.

We streamlined our processes, hired and trained new investigators, contracted external resources and implemented a "backlog blitz" aimed at resolving old complaint cases.

As a result, we began the 2009-2010 fiscal year with 333 backlogged files, and whittled that down to just 10 when the year ended – and even that last handful of files was nearing completion.



The elimination of the backlog ushers in a new era for the Office. Our investigators are excited to work with clients who are not frustrated by delays, on files where the evidence remains fresh.

Our focus now is on the early resolution of issues and the efficient processing of complaints, in order to avoid a future backlog. As described earlier, we are now intensifying our efforts at the "front end," by investing more time on inquiries and directing would-be complainants to information and resources.

We also have a complaint form that explains in detail the information that our Office will need. This can help save time after the file is assigned to an investigator.

The creation of a new position of Complaints Registrar is another important change. The registrar assesses the complexity and priority of the case, and whether it can be resolved quickly.

Those that can be resolved quickly now go to a new early resolution team. Key to the early resolution process are techniques such as negotiation and persuasion and a solid knowledge of past complaint findings.

Complaints determined to involve a serious, systemic or otherwise complex matter are immediately streamed to an investigator.

4.6 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. Accordingly, review applications may not be made with respect to the wrongful collection, use or disclosure of personal information by government institutions. Over the years, our Office has often recommended that the federal government broaden the grounds under which an application for a court review under section 41 may be made.

Some of the cases of interest that came before the Federal Court in 2009-2010 are described below. Certain decisions taken by the Commissioner or the Assistant Commissioner have also been the subject of judicial review applications in Federal Court.

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

Canadian Broadcasting Corporation v. Privacy Commissioner of Canada
Federal Court File No. T-122-10

Our Office received a notice of application from the Canadian Broadcasting Corporation (CBC) seeking judicial review of an order issued by the Assistant Privacy Commissioner for the production of certain records under the control of the CBC. Our Office requested the information from the CBC during the course of an investigation into a complaint filed under the *Privacy Act*.

The CBC refused to provide the documents on the grounds that they were excluded under section 69.1, which specifically exempts from the Act personal information that the CBC collects, uses or discloses for journalistic, artistic or literary purposes.

The CBC argued that, since it views the documents as excluded under that section, the Commissioner does not have the power to compel production of these documents in order to satisfy herself that they are, indeed, excluded under the Act.

The Assistant Commissioner, however, was of the view that it was necessary to see the withheld records in order to carry out her investigation. An order for the production of those records was therefore served on the CBC.

The CBC has filed a similar application against the Information Commissioner of Canada regarding an order for production of documents. The *Access to Information Act* contains similar, but not identical, provisions regarding exclusions for the CBC, and powers to compel information from a federal institution.

Our Office filed its notice of appearance on Feb. 5, 2010.

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

We have previously reported on this case in last year's annual report. In this case, 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 Privacy Commissioner was granted intervener status to participate in the application and assist the court to determine the legal issues with respect to privacy.

These issues related to the right of an administrative tribunal to divulge personal information by way of a report posted on the Internet, and the application, if any, of the open-court principle to the decision of an administrative tribunal.

However, the parties reached a settlement and the applications were discontinued on Aug. 24, 2009.

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

In this matter, also reported on in last year's annual report, 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 in determining the legal issues with respect to privacy.

This matter also raised issues about the disclosure of personal information on the Internet and the extent of application of the open-court principle.

Four other federal institutions were also granted intervener status – the Public Service Labour Relations Board, the Public Service Staffing Tribunal, the Military Police Complaints Commission and the Canadian Transportation Agency.

Following a case management conference, the matter is proceeding in accordance with a court-ordered timetable, pursuant to which the Privacy Commissioner was to file written arguments by June 2, 2010.

X v. Privacy Commissioner of Canada and Information Commissioner of Canada
Court File No. DC-09-88-JR

This is a judicial review application, filed in the Ontario Superior Court of Justice, Divisional Court, in which the applicant sought an order of mandamus requiring the OPC and the Office of the Information Commissioner of Canada to complete investigations regarding complaints filed by the applicant with both offices.

The OPC was nearing completion of its investigation at the time the application was filed. The OPC issued a report of findings to the complainant, which resolved the matters raised in the application and effectively rendered the issue of mandamus moot.

The applicant nonetheless sought to continue the application. Therefore, the OPC filed a motion to strike the application on the grounds of lack of jurisdiction (because the application was filed in provincial court) and mootness.

On Jan. 22, 2010 the court dismissed the application. The applicant has sought leave to appeal the order.

4.7 FEDERAL ADMINISTRATIVE TRIBUNALS

DISCLOSURE IN THE INTERNET ERA

In recent years, the *Privacy Act* annual report has highlighted the privacy concerns that arise when federal administrative tribunals and quasi-judicial bodies publish on the Internet decisions containing sensitive personal information. While the principle of open courts is vitally important in a well-functioning democracy, we have expressed concerns about its application to quasi-judicial bodies in the digital era.

Weigh disclosure of personal information carefully, tribunal told

An individual complained that the Public Service Staffing Tribunal improperly e-mailed his personal information, including sensitive medical information, to hundreds of other people.

The trouble began when his employer reclassified an entire group of positions upwards. All incumbents, with the exception of the complainant, were promoted to the new level. The individual complained to the tribunal that he should also have been promoted, along with all of his colleagues.

In considering the case, the tribunal asked the man to supply further supporting documentation, which he did. The tribunal, deeming the hundreds of former colleagues to have been parties to the complaint, then forwarded to all of them the man's entire file, including attachments of sensitive personal information. The tribunal never counselled the man on what sort of information to furnish, or advised him that his entire file would be circulated to all parties.

Following an investigation, the Assistant Commissioner upheld the complaint as well founded. She noted that while the tribunal was required under its regulations to circulate copies of the complaint to all parties, there was no obligation to include supporting documentation.

She emphasized this point in her recommendations, adding that, if the complaint itself happens to contain sensitive medical or other personal information, the tribunal should exercise its discretion to transmit that information only to people with a clear need to know it.

The Public Service Staffing Tribunal was reluctant to change its processes. In the absence of legislative authority to challenge the disclosure in court, the Office encourages this and other administrative tribunals to adhere to our guidelines for the publication of decisions containing sensitive personal information.

These bodies, which are covered by the *Privacy Act*, consider a range of issues, such as disputes over pension and employment insurance benefits, challenges to federal public service hiring processes, and compliance with particular workplace rules.

Much of the information that comes before them is highly personal and sensitive, such as salaries, physical and mental health problems, disputes with bosses, and allegations of wrongdoing in the workplace. Other information of questionable relevance may also come up, 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.

We acknowledge that there are cases where the public has a compelling interest in learning the identities of the individuals involved in tribunal proceedings. The *Privacy Act* was never intended as an instrument to conceal wrongdoing, or to shield people who commit fraud, pilfer the public purse, or who pose a danger to their fellow citizens. When such exceptional matters come to the attention of federal tribunals and a genuine public interest is at stake, the Act has provisions to permit the disclosure of personal information.

RCMP told to publish findings of disciplinary proceedings without identifying details

A Royal Canadian Mounted Police (RCMP) officer complained that her personal information was improperly disclosed when an RCMP disciplinary tribunal posted its findings on an internal website and disclosed them to a newspaper reporter.

In addition to details of the disciplinary matter, the published findings of the RCMP's Adjudication Board referred to the officer by name, and noted that she had married and changed her surname.

The member complained to us about an invasion of her privacy.

The RCMP justified the adjudicator's decision to publish its findings on the grounds that the public has a right to know about police disciplinary matters.

Following an OPC investigation, the Assistant Commissioner acknowledged the RCMP's need to reassure the public that it is addressing discipline issues in a timely and appropriate manner. That obligation, however, can generally be met without publishing Adjudication Board findings in identifiable form. As the disciplinary board's hearings were open to the media, a depersonalized version of the outcome would likely have been enough to validate the process.

The Assistant Commissioner also noted that the *Privacy Act* gives institutions, including the RCMP, discretion to disclose the name of the subject of a hearing if a public interest in the information is so compelling as to clearly outweigh the resultant invasion of privacy. A public interest disclosure, however, can only be justified in exceptional circumstances.

The complaint was upheld as well founded.

The RCMP declined to implement the recommendations while awaiting the outcome of a Treasury Board Secretariat review of federal administrative tribunal hearings.

For the most part, however, we have taken the view that the open courts principle can be reconciled with the tribunals' obligations under the *Privacy Act*. One way to do this is to depersonalize decisions posted online by, for example, substituting random initials for actual names. Even without identifying information, a published tribunal decision can contribute to informed public debate and ensure accountability of the quasi-judicial system.

In the wake of numerous investigations by our Office, and recommendations to protect the privacy of individuals whose cases have no broader public interest, some tribunals have agreed to depersonalize their published decisions. Others, however, continue to post whole decisions, including extensive amounts of personal information.

Privacy protections are now inconsistent across these institutions, but we are not empowered under the *Privacy Act* to bring this matter before the courts for further guidance.

OPC GUIDELINES

We are, however, continuing to seek stronger safeguards for Canadians' personal information. In consultation with our provincial and territorial counterparts, we developed broad guidelines to address the challenge of maintaining the transparency of administrative justice, while also protecting the privacy of individuals.

Recognizing that tribunals are diverse in terms of their enabling legislation and mandates, the guidelines call for a general approach, rather than a one-size-fits-all prescription.

In order to lessen the risk of privacy-related conflicts, we urge tribunals to inform the parties clearly and in advance about the laws and policies governing their information-handling procedures.

Where there is discretion as to disclosure of personal information in decisions posted on the Internet, tribunals ought to develop a policy to guide their practices.

As a best practice, the guidelines encourage tribunals to edit from the public posting all data elements, such as addresses and dates of birth, that are not relevant to the decision itself. They should also consider whether de-identified or anonymized versions of the decision could be viable alternatives to full disclosure.

Where tribunals do opt to reveal names online, the guidelines recommend they use web robot exclusion protocols, so that a search by name, using a common search engine such as Google, will not instantly return the full decision.

Last February, the Heads of Federal Administrative Tribunals Forum put forward a position that echoed many of our recommended approaches. The forum, however, was more open to the idea that its members might publish the names of individuals participating in their proceedings.

We hope that our guidelines, which are available on the OPC website, will eventually be adopted by Treasury Board.

4.8 ACCESS TO INFORMATION AND PRIVACY

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

1. ACCESS TO INFORMATION ACT

In 2009-2010, our Office received 26 new requests under the *Access to Information Act* for government records under our control, two fewer than the year before. Another six requests in 2009-2010 were carried forward from the previous year. A further 26 access requests that we received during the past fiscal year were seeking records under the control of other federal institutions and were therefore redirected.

In all, we completed 31 access to information requests by the end of the fiscal year and one request was carried forward.

We received notice of three complaints submitted to the Information Commissioner under the *Access to Information Act*, compared to none the year before. All alleged denial of access to government records.

The Information Commissioner determined that one complaint was not substantiated, the second was discontinued, and the third remained outstanding at the end of the fiscal year.

2. PRIVACY ACT

We received 16 requests under the *Privacy Act* for personal information contained in documents under our control, and closed 15 in the fiscal year. Another 45 privacy requests that we received in 2009-2010 were seeking records under the control of other federal institutions and were therefore redirected.

We received no complaints under the *Privacy Act* during the fiscal year, the same as the year before.

THE YEAR AHEAD

A few months after the end of this reporting period, Mr. Justice John Major published the findings of his inquiry into the 1985 bombing of Air India Flight 182. His report, cogently titled *A Canadian Tragedy*, shone a spotlight on the often murky intersection of national security and individual rights, including the right to privacy.

For our Office, this is fertile ground we have been tilling for some time. We take the view that privacy, as contemplated by the *Privacy Act*, is a fundamental human right, an essential precursor to freedom of speech, assembly and movement. Having been on the vanguard of public reflection over the challenges of integrating privacy and security, we welcomed the Major Inquiry's insights and perspectives.

As part of its comprehensive findings, the report cast doubt on the effectiveness of some of the government's contemporary security measures, including the no-fly list and the anti-terrorist financing regime. Both had already come under scrutiny from our Office for their impact on the privacy rights of Canadians.

The Major report called on Transport Canada – and, by logical extension other government agencies involved in security – to work with us to devise criteria and tools against which to evaluate the privacy impacts of proposed security measures.

Fortunately, substantial work in this area is already underway, as our Office has identified national security as one of our four key policy priorities. Indeed, we are persuaded that national security, information technology, genetic technology, and the protection of identity are four of the most significant emerging challenges to our notion of privacy in the 21st century.

STRUCTURING OUR ANALYSIS

In order to enhance our effectiveness in the face of these emerging challenges, our Office recognizes the importance of articulating the values and principles that guide our approach to privacy. We also advocate a thoughtful and structured public debate to ensure that Canadians are fully engaged in the challenges and their solutions.

We are moving toward these objectives in several ways. For instance, as this report describes, we are actively elaborating on the underlying privacy values by entrenching a public law methodology in key activities.

Influenced by the 1986 Supreme Court of Canada ruling in *R. v. Oakes*, this approach states that when a government contemplates any measure that could infringe on privacy rights, the proposal ought to be justified against a four-part analysis: Is the measure necessary? Is it effective? Is the infringement on privacy proportionate to the potential benefit to be derived? And is there some viable alternative that would be less intrusive on privacy rights?

The analysis forces organizations to think beyond the basic mechanics of data collection and protection, and to consider *why* they want to pursue the measure in the first place. What is to be achieved, how will the Canadian public be informed, and who is to be accountable for the protection of the personal information are all key considerations in this analysis.

The four-part test already figures in our expectations for departmental Privacy Impact Assessments submitted to our Office for review. It will also serve as a cornerstone of a series of policy guidance documents now under development.

POLICY GUIDANCE

One of the key outcomes of roundtable discussions held in 2007 and 2008 in collaboration with the Public Policy Forum was to document the expressed need for concrete guidance on integrating privacy into the development of government policy.

In response, our Office launched a process that will culminate in the development of policy guidance papers in our four priority privacy areas. The documents are aimed at government policymakers, legislators, academics and the wider privacy community. They are intended to be practical and useful, not prescriptive – much like the "tools and criteria to evaluate proposed security measures" recommended by the Air India Inquiry.

The first such guidance document, relating in fact to national security, is expected to be published later this year. Drafted with extensive input from academics, civil society, public safety and security officials, oversight agencies, the legal community and others, it will start by explaining what personal information is, and describing what a reasonable expectation of privacy means.

It will next encourage policymakers contemplating a new security measure to reflect on what they are trying to accomplish, and to consider their initiative through the lens of the four-part test.

The paper then guides policymakers through three further stages: The design, the implementation and the ongoing operation of their proposed security initiative.

The guidelines will outline the specific issues that policymakers should bear in mind, as well as concrete steps they could take to address them, from internal governance and management structures through the establishment of public complaint, redress, oversight and reporting mechanisms.

GOVERNANCE OF THE OPC

When it comes to governance and management structures, our own Office is also in a period of transition.

Up to the year described in this annual report, considerable effort had been invested in the organization's stabilization and growth. Much of our focus was on improving processes, with the elimination of the massive complaint-investigation backlog serving as a key manifestation of our success.

With that behind us, a broader examination of the OPC's future is underway. We are currently re-examining our governance structures with the aid of an outside expert. We are also continuing to press for changes to the *Privacy Act,* and to implement administrative measures that will bolster our capacity to safeguard the privacy rights of Canadians.

Some strategic changes are already underway, and we expect they will have a positive impact in the year ahead.

For example, our investigations and audit branches now report to the same Assistant Commissioner. This will help strengthen our compliance activities by creating greater synergy between what we hear from Canadians through inquiries and complaints, and how we monitor the protection of personal information in the public sector through audits and Privacy Impact Assessment reviews.

OPC ACTIVITIES

With our backlog of older complaint files now cleared away and our investigative function retooled, our Office is in a better position to focus on complex or precedent-setting cases, and those that fall within our four policy priorities. We will also continue to devote resources to the "front end," which means buttressing our public inquiries unit and our capacity to resolve issues before they become formal complaints.

Our Audit and Review Branch has also significantly re-engineered its processes, including moving toward a more formalized, risk-based approach to selecting subjects for privacy audits and Privacy Impact Assessments for review.

In the year ahead, we will also document our audit methodology in an audit manual. For that we have looked to the standards and good practices of organizations such as the Canadian Institute of Chartered Accountants and the Institute of Internal Auditors.

Meantime, we will continue to enrich our processes for reviewing Privacy Impact Assessments, in recognition of the value these analyses bring to government and the public at large. We also hope to continue our interaction with the access to information and privacy community through workshops, consultations and other activities, with the aim of maximizing the effectiveness of the Privacy Impact Assessment process.

Another ongoing focus is the Treasury Board Secretariat's development of a new directive on Privacy Impact Assessments, which is expected to supplant the existing policy as part of the government's policy suite renewal process. We have a number of questions about the directive and want to make sure that privacy concerns will be clearly addressed.

On the legislative front, 2010-2011 is already shaping up as a busy year. We have turned our minds to amendments to Canada's private-sector privacy law, the *Personal Information Protection and Electronic Documents Act*, as well as anti-spam legislation previously known as the *Electronic Commerce Protection Act* and reintroduced in late May as the *Fighting Internet and Wireless Spam Act.*

We will also continue to monitor legislative proposals related to surveillance and the interception of electronic communications, as well as other measures to strengthen the powers of law enforcement and national security agencies.

Throughout these intensive activities, we remain committed to engaging Canadians on privacy issues. Today's challenges to privacy are of an historically unprecedented scope and complexity. It is not only desirable but essential that Parliament and the public at large be part of an informed national dialogue.

In the belief that such a conversation will culminate in a consensus on the protection of privacy in Canada in the 21st century, the Office of the Privacy Commissioner of Canada will remain at the forefront of that effort.

APPENDIX 1 – DEFINITIONS

COMPLAINT TYPES

1. 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 – *Info Source* (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.

2. 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 *Info Source*): 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.

3. 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.

FINDINGS AND OTHER DISPOSITIONS UNDER THE *PRIVACY ACT*

1. INVESTIGATIVE FINDINGS

Well founded: The government institution failed to respect the *Privacy Act* rights of an individual. This category includes findings formerly classified separately as **Well founded/Resolved**, in which the investigation substantiated the allegations and the government institution agreed to take corrective measures to rectify the problem.

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*.

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.

2. OTHER DISPOSITIONS

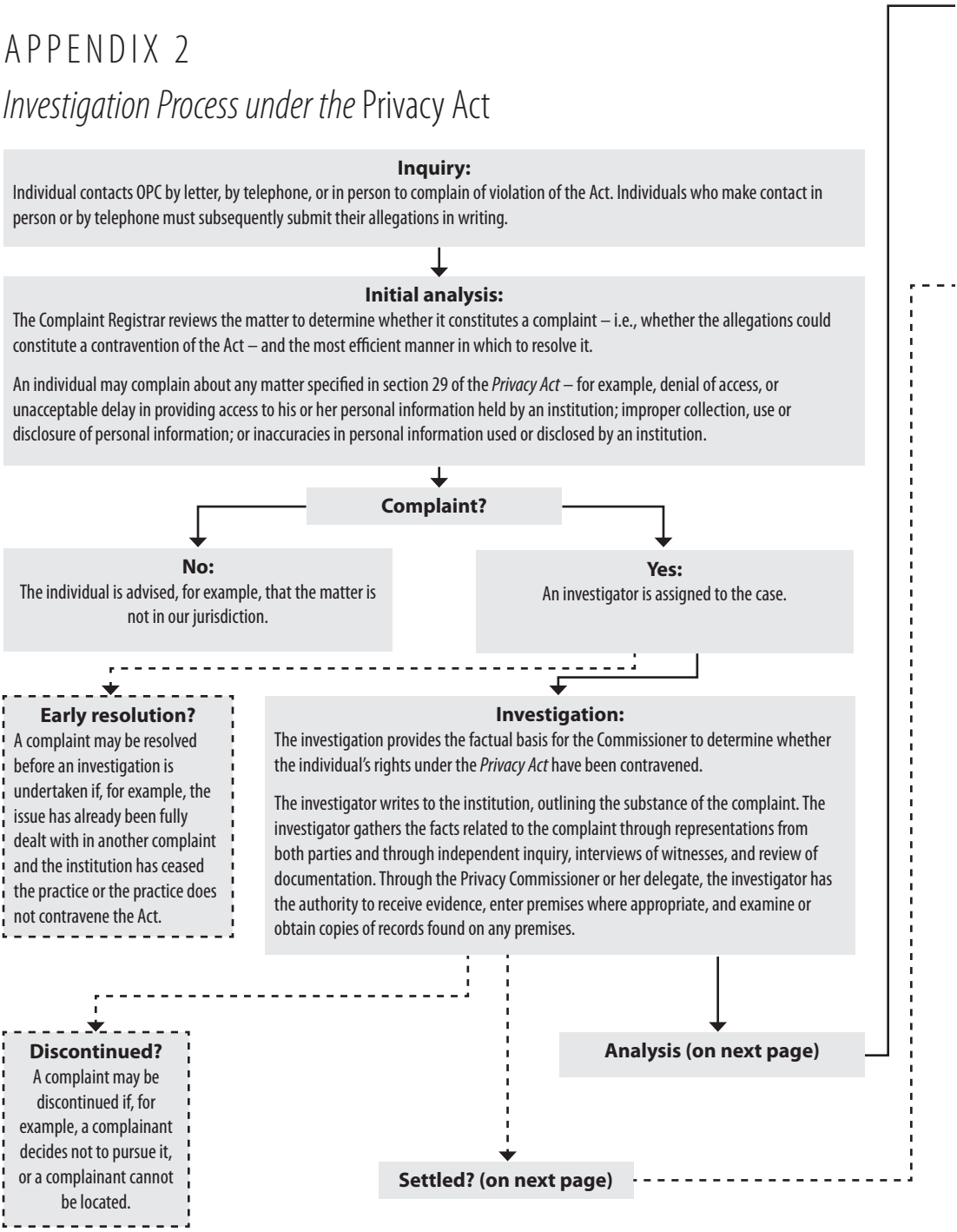
Early resolution: Applied to situations in which the issue is dealt with before a formal investigation is undertaken. For example, if an individual complains about an issue the OPC has already investigated and found to be compliant with the *Privacy Act*, we explain this to the individual. We also receive 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".

Settled during the course of 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 various reasons. For example, 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



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, 2009 to March 31, 2010*

INQUIRIES STATISTICS

Inquiries Received under the *Privacy Act*	
By telephone:	1,448
Written (letter, e-mail, fax):	1,124
Total:	2,572

General* Inquiries Received	
By telephone:	2,587
Written (letter, e-mail, fax):	281
Total:	2,868

Responses to Inquiries under the *Privacy Act*	
By telephone:	1,450
Written (letter, e-mail, fax):	1,193
Total:	2,643

Responses to General* Inquiries	
By telephone:	2,586
Written (letter, e-mail, fax):	292
Total:	2,878

* 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	Total by complaint type
Access	239	36	Access 251
Correction-Notation	10	1	
Fees	2	<1	
Time Limits	264	40	Time limits 292
Extension Notice	28	4	
Collection	17	3	Privacy 122
Use and Disclosure	98	15	
Retention and Disposal	7	1	
Total	**665**	**100**	**665**

As in previous years, the most common complaints to our Office related to access to personal information (a combined 251, or 38 percent of the total), and to the length of time that government departments and agencies were taking to respond to access requests (292, or 44 percent of all complaints). Privacy complaints, which include problems related to the collection, use, disclosure, retention or disposal of personal information, comprised a total of 122 complaints, representing 18 percent of the total. See Appendix 1 for definitions of complaint types.

TOP-10 INSTITUTIONS BY COMPLAINTS RECEIVED

Organization	Access	Time Limits	Privacy	Total
Correctional Service of Canada	69	192	29	**290**
Royal Canadian Mounted Police	37	10	13	**60**
Canada Revenue Agency	12	22	15	**49**
National Defence	19	20	8	**47**
Canadian Security Intelligence Service	21	4	1	**26**
Canada Border Services Agency	17	3	6	**26**
Canada Post Corporation	8	2	13	**23**
Human Resources and Skills Development Canada	10	5	5	**20**
Citizenship and Immigration Canada	7	3	5	**15**
Justice Canada	3	8	0	**11**
Others	44	23	31	**98**
Total	**247**	**292**	**126**	**665**

The number of complaints filed against an institution does not necessarily mean the organization is not compliant with the *Privacy Act*. Because of their mandates, some institutions hold a substantial amount of personal information. Therefore, they are more likely to receive numerous requests for access to that information, which may in turn lead to complaints about the institution's collection, use and disclosure, retention and disposal of personal information, and the manner in which it provides access to that information.

COMPLAINTS RECEIVED BY INSTITUTION

	Total
Agriculture and Agri-food Canada	1
Atomic Energy of Canada Limited	2
Canada Border Services Agency	26
Canada Post Corporation	23
Canada Revenue Agency	49
Canadian Heritage	1
Canadian Human Rights Commission	1
Canadian Security Intelligence Service	26
Canadian Wheat Board	1
Citizenship and Immigration Canada	15
Correctional Service of Canada	290
Financial Transactions and Reports Analysis Centre of Canada	2
Fisheries and Oceans	1
Foreign Affairs and International Trade Canada	9
Health Canada	9
Human Resources and Skills Development Canada	20
Immigration and Refugee Board	2
Indian and Northern Affairs Canada	4
Industry Canada	2
Justice Canada	11
Library and Archives Canada	2
National Defence	47
National Parole Board	8
Natural Resources Canada	3
Parks Canada	2
Public Health Agency of Canada	4
Public Prosecution Service of Canada	1
Public Safety Canada	3
Public Sector Integrity Canada	4
Public Service Commission of Canada	4
Public Service Labour Relations Board	1
Public Works and Government Services Canada	7
Royal Canadian Mounted Police	60
Social Science and Humanities Research Council of Canada	2
Statistics Canada	7
Toronto Port Authority	1
Transport Canada	8
Treasury Board of Canada Secretariat	3
Veterans Affairs Canada	2
Western Economic Diversification Canada	1
Total	**665**

COMPLAINTS RECEIVED BY PROVINCE/TERRITORY

Province/Territory	Total	Percentage
Ontario	234	35
British Columbia	151	23
Quebec	87	13
Alberta	58	9
Saskatchewan	50	8
New Brunswick	41	6
Nova Scotia	14	2
Newfoundland and Labrador	10	1
Manitoba	9	1
International *	9	1
Northwest Territories	1	<1
Prince Edward Island	1	<1
Total	**665**	**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 2009-2010. 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

		Investigative Findings			Other Dispositions		Total
		Well founded[3]	Not well founded	Resolved	Resolved early or settled during investigation	Discontinued	
Access	Access	64	263	27	90	86	530
	Correction/ notation	0	5	1	7	3	16
	Fees	0	0	0	1	0	1
	Language	0	1	0	1	0	2
Time Limits	Time Limits	253	15	0	13	13	294
	Correction/ Time Limits	2	0	0	0	0	2
	Extension Notice	11	6	0	0	1	18
Privacy	Collection	3	18	1	9	6	37
	Retention and Disposal	4	4	2	2	2	14
	Use and Disclosure	119	39	6	38	38	240
Total		**456**	**351**	**37**	**161**	**149**	**1,154**

Access: We closed a total of 549 complaints about access to personal information, comprising nearly half (48 percent) of all the complaints we closed last year. Of those, 269, or just about half, were not substantiated upon investigation. However, 64 of those cases were well founded and, in 54 instances, the institution agreed to resolve the concern by the conclusion of the investigation. Another 28 access cases were investigated and found to have merit, but were resolved through negotiation.

Time Limits: Complaints about the time it takes for institutions to respond to requests for access to personal information were the second most common category of files we closed last year – a total of 314, or 27 percent of our caseload. Because most complainants only come to us after the statutory deadline for their complaint has passed, 266 (or 85 percent) of those complaints were well founded.

[3] Includes 56 findings formerly classified as Well founded/Resolved. Of those, 54 were access cases, one was a complaint over the collection of personal information, and one related to the use and disclosure of personal information.

Privacy: Cases involving the collection, use, disclosure, retention or disposal of personal information combined to account for 291, or one-quarter, of all complaints we investigated. Of those, 126 (43 percent) were determined to be well founded and, in the vast majority of those cases, the issue related to the improper use or disclosure of personal information.

DISPOSITION OF TIME LIMITS COMPLAINTS BY INSTITUTION

Institution	Well founded	Not well founded	Early Resolution	Settled in course of investigation	Discontinued	Total
Atomic Energy of Canada Limited	0	0	0	0	2	**2**
Canada Border Services Agency	2	0	0	0	0	**2**
Canada Post Corporation	2	0	0	0	4	**6**
Canada Revenue Agency	13	0	3	0	0	**16**
Canadian Food Inspection Agency	3	0	0	0	0	**3**
Canadian Heritage	1	0	0	0	0	**1**
Canadian Security Intelligence Service	2	2	0	0	0	**4**
Citizenship and Immigration Canada	2	1	0	0	0	**3**
Correctional Service Canada	202	7	7	2	5	**223**
Foreign Affairs and International Trade	2	0	0	0	1	**3**
Health Canada	4	0	0	1	1	**6**
Human Resources and Skills Development Canada	6	1	0	0	0	**7**
Justice Canada	2	1	0	0	0	**3**
National Defence	13	0	0	0	0	**13**
National Parole Board	0	2	0	0	0	**2**
Parks Canada	1	0	0	0	0	**1**
Privy Council Office	2	0	0	0	0	**2**
Public Health Agency of Canada	1	0	0	0	0	**1**
Public Works and Government Services Canada	0	2	0	0	0	**2**
Royal Canadian Mounted Police	6	3	0	0	1	**10**
Transport Canada	2	0	0	0	0	**2**
Treasury Board of Canada Secretariat	0	2	0	0	0	**2**
Total	**266**	**21**	**10**	**3**	**14**	**314**

DISPOSITION OF ACCESS AND PRIVACY COMPLAINTS BY INSTITUTION

Institution	Well founded[4]	Not well founded	Resolved	Early Resolution	Settled in course of investingation	Discontinued	Total
Agriculture and Agri-Food Canada	0	0	0	0	5	1	**6**
Canada Border Services Agency	9	28	4	1	1	6	**49**
Canada Mortgage and Housing Corporation	0	2	0	0	0	0	**2**
Canada Post Corporation	2	15	0	2	3	7	**29**
Canada Revenue Agency	4	31	0	6	5	9	**55**
Canada Science and Technology Museum Corporation	1	0	0	0	0	0	**1**
Canadian Air Transport Security Authority	0	1	0	0	0	0	**1**
Canadian Food Inspection Agency	1	0	0	0	3	0	**4**
Canadian Nuclear Safety Commission	1	1	0	0	0	0	**2**
Canadian Security Intelligence Service	0	32	0	3	0	5	**40**
Citizenship and Immigration Canada	2	12	1	1	2	2	**20**
Commission for Public Complaints against the RCMP	1	1	1	0	0	1	**4**
Correctional Service of Canada	38	52	9	18	25	25	**167**
Environment Canada	2	0	0	0	0	1	**3**
Export Development Corporation	1	0	0	0	0	0	**1**
Financial Transactions and Reports Analysis Centre of Canada	0	1	1	0	1	0	**3**
Fisheries and Oceans	2	4	0	0	1	0	**7**
Foreign Affairs and International Trade Canada	2	5	0	4	4	3	**18**
Health Canada	2	2	0	1	0	5	**10**
Human Resources and Skills Development Canada	88	13	3	3	6	12	**125**
Immigration and Refugee Board	1	0	0	1	0	16	**18**
Indian and Northern Affairs Canada	1	5	0	1	1	0	**8**
Industry Canada	0	2	0	0	0	0	**2**
Justice Canada	1	7	0	0	3	6	**17**

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

Institution	Well founded[4]	Not well founded	Resolved	Early Resolution	Settled in course of investingation	Discontinued	Total
Library and Archives Canada	0	4	0	1	0	0	**5**
Marine Atlantic Inc.	0	1	0	0	0	0	**1**
National Defence	7	11	3	2	7	8	**38**
National Parole Board	0	5	0	3	0	1	**9**
National Research Council Canada	0	1	0	0	0	0	**1**
Natural Resources Canada	1	2	0	1	0	0	**4**
Office of the Chief Electoral Officer	1	0	0	0	0	0	**1**
Office of the Correctional Investigator Canada	0	1	0	0	0	0	**1**
Office of the Information Commissioner of Canada	0	0	0	0	0	2	**2**
Parks Canada	0	0	0	1	0	0	**1**
Privy Council Office	0	1	1	0	0	0	**2**
Public Prosecution Service of Canada	0	0	0	1	0	0	**1**
Public Safety Canada	1	3	0	1	0	0	**5**
Public Sector Integrity Canada	0	0	0	0	4	1	**5**
Public Service Commission of Canada	1	0	1	0	0	5	**7**
Public Service Labour Relations Board	1	0	0	0	1	1	**3**
Public Service Staffing Tribunal	1	0	0	0	0	1	**2**
Public Works and Government Services Canada	0	3	1	0	1	0	**5**
Ridley Terminals Inc.	0	1	0	0	0	0	**1**
Royal Canadian Mounted Police	13	76	10	9	10	14	**132**
Social Science and Humanities Research Council of Canada	0	1	1	0	0	0	**2**
Toronto Port Authority	1	0	0	0	0	0	**1**
Transport Canada	1	2	0	1	2	2	**8**
Treasury Board of Canada Secretariat	1	1	0	0	1	1	**4**
Veterans Affairs Canada	2	3	1	0	0	0	**6**
Western Economic Diversification Canada	0	0	0	1	0	0	**1**
Total	**190**	**330**	**37**	**62**	**86**	**135**	**840**

[4] Includes 56 findings of Well founded/Resolved.

TREATMENT TIMES FOR COMPLAINT INVESTIGATIONS UNDER THE *PRIVACY ACT*

BY COMPLAINT TYPE

Complaint Type	Number of Complaints	Average Treatment Time (Months)
Language	2	20
Retention/Disposal	14	20
Access	530	18
Collection	37	17
Use/Disclosure	240	11
Correction/Notation	16	9
Time Limits	294	5
Correction/Time Limit	2	4
Extension Notice	18	4
Fees	1	2
Weighted average		**12.9**

BY DISPOSITION

Disposition	Number of Complaints	Average Treatment Time (Months)
Well founded and resolved	56	22
Settled in the course of investigation	89	22
Discontinued	149	21
Resolved	37	18
Not well founded	351	15
Well founded	400	6
Early resolution	72	3
Weighted average		**12.9**

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

Over the past year, a primary focus was to eliminate our backlog of case files older than a year. We therefore closed 1,154 files, up 17 percent from the 990 we closed in 2008-2009. Despite this increased workload, our emphasis on early resolution strategies enabled us to reduce the average treatment times by one-third, from 19.5 months in 2008-2009 to 12.9 months in 2009-2010.