Office of the
Privacy Commissioner
of Canada

THE PRIVACY ACT
1982-2012

Annual Report to Parliament 2011-2012

Report on the *Privacy Act*

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. IP50-2012
1910-006X

This publication is also available on our website at **www.priv.gc.ca**

Follow us on Twitter: @privacyprivee

Annual Report to Parliament 2011-2012 — Report on the *Privacy Act*

Privacy Commissioner of Canada

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 947-1698
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) 947-1698
Téléc. : (613) 947-6850
1-800-282-1376
www.priv.gc.ca

October 2012

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 of April 1, 2011, to March 31, 2012. This tabling is pursuant to section 38 of the *Privacy Act*.

Yours sincerely,

Original signed by

Jennifer Stoddart
Privacy Commissioner of Canada

Privacy Commissioner of Canada

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 947-1698
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) 947-1698
Téléc. : (613) 947-6850
1-800-282-1376
www.priv.gc.ca

October 2012

The Honourable Andrew Scheer, 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 of April 1, 2011, to March 31, 2012. This tabling is pursuant to section 38 of the *Privacy Act*.

Yours sincerely,

Original signed by

Jennifer Stoddart
Privacy Commissioner of Canada

Table of Contents

Table of Contents

About the *Privacy Act*

The *Privacy Act*, which took effect in 1983, obliges approximately 250 federal government institutions to respect the privacy rights of individuals by limiting the collection, use and disclosure of their personal information.

The *Privacy Act* also gives individuals the right to request access to personal information about themselves that may be held by federal government institutions. If individuals feel that the information is incorrect or incomplete they also have the right under the Act to ask that it be corrected.

Commissioner's Message

THE EVOLUTION OF PRIVACY OVER THREE DECADES

"It was the best of times, it was the worst of times, it was the age of wisdom, it was the age of foolishness, it was the epoch of belief, it was the epoch of incredulity, it was the season of Light, it was the season of Darkness, it was the spring of hope, it was the winter of despair …"

– Opening lines, A Tale of Two Cities, by Charles Dickens

When Canada's *Privacy Act* was born 30 years ago, only a few people had even heard the phrase "surveillance society," and even fewer were voicing concerns about its emergence.

To illustrate that concept, the first Annual Report of the Office of the Privacy Commissioner of Canada featured a cover cartoon of a man peering through a keyhole.

How innocent that seems in retrospect.

Who among us back then could possibly have dreamt of the pervasive surveillance of which government systems are now capable?

Who imagined video cameras would scrutinize people innocently going about their daily lives on a community's main street? Or that scanning devices would peek through our clothes at airports? Or that the old-fashioned paper letters of that time offered more security from the prying eyes of the state than the electronic mail that would replace them?

The appetite of governments for personal information about citizens over the past three decades has proven to be voracious.

Time and again, Privacy Commissioners have raised red flags warning the public and

Parliament about the risks of collecting too much information on citizens.

Over the years, a number of investigations by our Office have unearthed cases of denial of access or improper collection or disclosure.

A 2008 audit found that the Royal Canadian Mounted Police's (RCMP) national exempt databanks (which are shielded from public access) were crowded with tens of thousands of records that should not have been there. Exempt databanks serve to withhold the most sensitive national security and criminal intelligence information, and yet more than half of the files examined as part of our audit did not meet the threshold for continued exempt bank status.

A decade earlier, when the federal air navigation system was privatized, the Office's concerns about personal information being handed over by Transport Canada led to the culling of one million pages of outdated or irrelevant material.

Evolution of Privacy

The evolution of privacy issues during our first 30 years has been truly remarkable.

In 1982, when the *Privacy Act* was passed by Parliament, the country was two years away from the introduction of the first mobile phone. Electric typewriters still dominated in government and business. Visionaries were discussing something called the Internet.

The headline privacy issues of the 1980s reflected these simpler times.

When the personal information of about 16 million taxpayers was stolen from a National Revenue office in 1986 – "the Chernobyl of privacy disasters" we called it – the miniaturized details were recorded on rectangles of photographic film known as microfiche.

A prominent cause for complaints to our Office in those days were demands to produce a Social Insurance Number, which many people carried on a card in their wallet.

At the same time, however, new personal information concerns emerged; our Office flagged potential privacy risks from data matching, cross-border information flows, smart cards and genetics.

Together, the proliferation of low-tech privacy violations and the appearance of new threats combined to propel privacy "from a peripheral social issue, from being a rather esoteric, rarefied – almost cult – concern into the mainstream of public consciousness," as the first Privacy Commissioner, John Grace, wrote in 1990.

This move into the mainstream was reflected in the Office's workload, with many double-digit percentage increases in the number of complaints year over year during the 1980s.

And then things really got hectic.

Second Decade

The *Privacy Act*'s second decade, from 1992 to 2002, featured the emergence of increased risks to privacy stemming from the very nature of Canada's fast-changing society – the explosion in computing technology, the increase in software sophistication and the transformation of personal information into a commodity.

The issues became more complex and mainstream consciousness was slow to awake to these risks. Public education became a high priority.

Our 1995-1996 Annual Report devoted two pages to describing the electronic trail of personal information that an ordinary Canadian unwittingly left behind during an average day in the brave new Information Society.

By then, Privacy Commissioner Bruce Phillips had abandoned his initial hope that voluntary measures by the private sector could effectively protect personal information. Instead he was urging the government to develop federal private-sector privacy legislation.

To the nation at large, Mr. Phillips also made an eloquent plea – one which has echoed down to the present – for Canadians to construct an ethical foundation for the new cyber technology. "Otherwise we are conducting a technical exercise in a moral vacuum," he cautioned, "molding our lives to fit technology, not making technology fit our lives."

The warning proved prescient.

Five years later, our 1999-2000 Annual Report revealed the hitherto unpublicized existence of a "citizen profile in all but name" created by Human Resources Development Canada.

An audit by our Office found that the innocuously named Longitudinal Labour Force File contained up to 2,000 items of information about individual Canadians, drawn from income tax returns, provincial and municipal welfare rolls, national employment services, child tax credits, the Social Insurance master file and elsewhere. Because records were never purged, the database included files on 33.7 million individuals, more than the total population then alive.

Within two weeks of the publication of that Annual Report, the government announced the database would be dismantled.

Mr. Phillips recalls that incident was "the biggest headline-grabber of my tenure" and also how Canadians were seized with the issue: "I think it generated tens of thousands of requests to the Department by Canadians wanting to know what this database contained about them."

The privacy workload continued to mount, despite several consecutive years of severe constraint on resources.

Third Decade

The waning years of the second decade witnessed two developments that would have a significant impact on the third decade of our Office's history.

First, the extension of our mandate to the private sector with the phasing in of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and, second, the terrorist attacks of September 11, 2001.

The latter gave birth to a belief among Western governments that national security demanded the collection of more and more personal information about individuals – by open or surreptitious means – and required cross-matching that information across disparate databases.

Our 2001-2002 Annual Report highlighted what then Commissioner George Radwanski called a "Big Brother" database which would have retained for seven years as many as 30 pieces of personal information about all air passengers flying into Canada.

Fortunately, the next Annual Report was able to state that "our opposition, supported by public opinion, eventually led the Minister of National Revenue to revise the initiative, significantly reducing the impact on privacy."

Meanwhile, national security concerns in the United States had a spillover effect in Canada.

The introduction of enhanced driver's licences, which contain RFID chips that can be electronically scanned, is one of several instances where privacy issues have arisen because of U.S. national security initiatives.

Enhanced driver's licences were proposed as an alternative to passports when the United States tightened its entry requirements. In 2007, the Canada Border Services Agency was working with the U.S. Department of Homeland Security to set up a system for using enhanced driver's licenses at surface border crossings. During the program's trial phase, the two agencies agreed that the data files of thousands of Canadians would be handed over to Homeland Security for storage in its database in the U.S.

Since 2002, the federal government has required that institutions carry out Privacy Impact Assessments for initiatives that raise privacy concerns.

While reviewing the Privacy Impact Assessment related to enhanced driver's licences, our Office learned details of the plan; we then pointed out that the proposed data transfer was not only problematic for protecting the privacy of Canadians, but also unnecessary for the system to work.

As a result, when Homeland Security scans an enhanced driver's licence today, its system pings a database in Canada, which allows access to verify only that one individual's file.

Matters could have been very different if the Privacy Impact Assessment hadn't been conducted. Had the wholesale export of personal information to the United States taken place as proposed, it might have been too costly to reverse.

A Tool with Impact

Later in this report, we provide more examples of the significant contribution of the assessment process to fostering a privacy-sensitive environment within the federal public service.

Another privacy protection measure which has amply demonstrated its worth in this tumultuous third decade is the detailed privacy audits we can carry out on government departments or programs.

While the Privacy Impact Assessment process is essentially preventative, the audits are remedial and identify systemic privacy issues, often after individual investigations have uncovered evidence of problems.

One such audit led to our first-ever special report to Parliament in 2008, mentioned earlier, about thousands of files containing personal information wrongly sequestered in RCMP exempt banks.

More recent audits have uncovered concerns related to the so-called "no-fly" aviation security program and the Financial Transactions Reports Analysis Centre of Canada (FINTRAC), the agency responsible for keeping tabs on possible criminal money-laundering.

Later in this Annual Report, we detail observations about the handling of personal information uncovered by an audit at Veterans Affairs Canada, already the subject of public criticism for violating a veteran's privacy.

Other significant privacy concerns in recent years involve pending legislation to provide law enforcement authorities with stronger enforcement powers. "Lawful access" legislation, introduced in February 2012, proposes to create an expanded surveillance regime that would have serious repercussions for privacy rights.

Hope and Concern

In retrospect, the past three decades have been, as the opening Dickens quotation suggests, a time of both hope and profound concern on the privacy front.

On the hopeful side, despite the numerous issues that have come to light over the past three decades, privacy remains a treasured value for the vast majority of Canadians. In fact, a 2011 poll commissioned by our Office showed two thirds of those surveyed agreed that protecting the personal information of Canadians will be one of the most important issues facing the country in the next ten years.

By acting in an ombudsman role, our Office has achieved positive results in specific cases such as the enhanced driver's licences, the Longitudinal Labour Force File and the protection of images captured by full-body airport scanners.

Despite some setbacks, the federal bureaucracy has generally become more attuned to privacy concerns.

Our Office is increasingly consulted in advance by government departments and agencies about the possible privacy implications of proposed initiatives,

including in the highly sensitive area of national security.

However, some areas of outstanding concern remain.

Some are summarized in Chapter 3, which recounts our audit and investigations of Veterans Affairs Canada and investigations involving the Correctional Service of Canada and the Canada Revenue Agency.

As well, some departments are still taking far too long to respond to legitimate requests from individuals about their personal information on file – in the most extreme cases it can take years for people to gain access.

Finally, despite the risk of underscoring the obvious, I must pick up the theme of many previous Commissioners' messages – the *Privacy Act* is badly outdated and requires an urgent overhaul to respond to the challenges of the digital era and the reality of huge government systems capable of a surveillance few could have envisaged in 1982.

Nonetheless, on this 30th anniversary, the Office of the Privacy Commissioner of Canada has much to be proud of.

Our greatest asset over the years has been the dedicated and talented people who have devoted themselves to ensuring that the privacy rights of Canadians are protected. We have always been a relatively small team, but we have accomplished a great deal.

Since opening our doors, we have responded to some 260,000 requests for information from Canadians. We have completed 37,600 investigations. We have reviewed over 500 Privacy Impact Assessments since 2002 (when PIAs were introduced). And we have carried out approximately 150 audits of federal government institutions.

Most importantly, we have worked to make a difference for Canadians.

Jennifer Stoddart
Privacy Commissioner of Canada

A Brief History:

FEDERAL PRIVACY LAW AND THE OFFICE OF THE PRIVACY COMMISSIONER OF CANADA

The Parliament of Canada enacted the federal *Privacy Act* in 1982. Prior to that time, data protection provisions were included in the *Canadian Human Rights Act*.

The Office of the Privacy Commissioner of Canada opened its doors on July 1, 1983 upon the coming into force of Canada's federal *Privacy Act*, which governs the personal information-handling practices of federal departments and agencies.

Over the three decades that have followed, we have adapted to a change in scope from purely public sector to private as well.

We have also gone from being heavily reliant solely upon investigations to focusing greater effort on public education to inform organizations on meeting their obligations through best practices and individuals on how to protect their privacy and assert their rights.

At the Office's inception, it shared corporate management expenses with the Office of the Information Commissioner. The two offices combined for a total of 59 full-time employees and an annual budget of just more than $2 million.

Beginning in 2001, the duties of our Office were extended to the private sector under the *Personal Information Protection and Electronic Documents Act* (PIPEDA). The legislation came into force in stages between 2001 and 2004.

By 2004, the Office no longer shared corporate management services and had an allocation for 100 full-time staff with a budget of just over $11.7 million per year.

In 2005, we received approval to stabilize funding for PIPEDA, as well as increased funding in support of our overall mandate. In subsequent years, we received additional funding for various initiatives such as the *Federal Accountability Act*, eliminating the backlog of investigations, expanding public outreach, establishing an internal audit function within the Office and also to support our new responsibilities under Canada's anti-spam legislation.

In recent years, we have enhanced our ability to address the fact that so many new and developing privacy issues are tied to information technology and the online world. It is critical that we have the right expertise and tools to evaluate the privacy impact of various technologies.

The online world is global and over the past years we have also found that cooperation with data protection authorities in other countries is essential to protect Canadians' privacy rights.

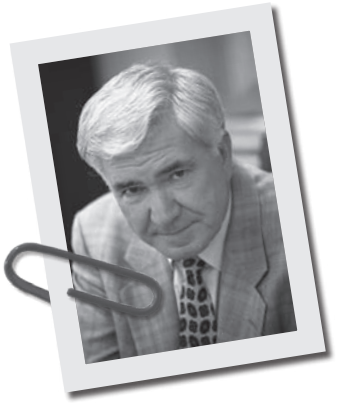
Today, the Office has the capacity for a full-time staff of 176 with annual expenditures of approximately $24.5 million. In response to the federal government's Deficit Reduction Action Plan, our Office proposed that we would find savings of five percent per year within our operations by fiscal year 2014-2015 while maintaining the best possible level of service for Canadians.

SELECTED QUOTES FROM PAST *PRIVACY ACT* ANNUAL REPORTS

John Grace
(Privacy Commissioner from 1983 to 1990)

Privacy protectors cannot be staled by custom or allowed to be complacent. The challenges to privacy are new, urgent, various and ingenious, brought about by technology that never sleeps and is rarely denied.
➤ **1984-1985**

Before countries earn the right to preach about protecting privacy values in the flow of personal information crossing borders, they need to have adequate data protection laws within their own jurisdictions.
➤ **1985-1986**



Bruce Phillips
(Privacy Commissioner
from 1991 to 2000)

There is no more fragile, yet important right, in today's complex society than the right to a reasonable expectation of privacy. It is not a right, which some cynics suggest, that only serves those with something to hide. Without a meaningful measure of privacy our fundamental freedoms of expression, belief and association risk becoming meaningless.
➤ **1990-1991**

The technology is evolving so fast that neither engineers nor policy makers have time to consider the social impacts. Each new development affects or overrides the privacy protections so laboriously erected to defend against the last one.
➤ **1991-1992**

The information society could just as well be characterized as the information jungle where the prevailing law is the survival of the fittest. The jungle is about to become much more lethal to our privacy with the introduction of infinitely larger systems of collecting, manipulating and distributing our personal histories to countless others.
➤ **1993-1994**

George Radwanski
(Privacy Commissioner
from 2000 to 2003)

We're all confronted now with the real possibility of having to go through life with someone looking over our shoulder, either metaphorically or quite literally. …(T)he evolution of fundamental rights such as privacy should teach us that their greatest value lies in their ability to ensure and protect us in times of the worst adversity.
➤ **2000-2001**

The more information government compiles about us, the more of it will be wrong. That's simply a fact of life.
➤ **2001-2002**

Robert Marleau
(Interim Privacy Commissioner in 2003)

People can have a private life even if much of their lives is spent in public view, as long as their activities cannot be linked to each other and to themselves. It is the ability to connect activities to each other and to an identifiable person that is at the heart of profiling and surveillance.
Lost privacy cannot be given back.
➤ **2002-2003**

Jennifer Stoddart
(Privacy Commissioner since 2003)

Our Office is not convinced that reducing the freedom of all individuals in society will prevent further threats to public safety by terrorists.
➤ **2003-2004**

Characterizing the current (Privacy) Act as dated in coping with today's realities is an understatement – the Act is tantamount to a cart horse struggling to keep up with technologies approaching warp speed.
➤ **2003-2004**

Canadians deserve real redress when things go wrong, not a Privacy Commissioner who has no power to even take a wrongful collection or a shameless disclosure of personal information to the Federal Court for a judgment and damages.
➤ **2004-2005**

There needs to be a greater acknowledgement of the fact that our privacy rights are fragile in the face of government. They falter each time we trade away the personal and private for promises of more safety, greater efficiency or faster service.
The Orwellian dystopia was predicated on a totalitarian society. In our democracy, benevolent intentions appear to be pushing us toward a surveillance society.
➤ **2007-2008**

Privacy by the Numbers

IN 2011-2012

INFORMATION REQUESTS

Linked to the *Privacy Act*	**1,310**
Linked to the *Personal Information Protection and Electronic Documents Act* (PIPEDA)	4,717
Not linked exclusively to either Act	3,086
Total	**9,113**

PRIVACY ACT COMPLAINTS*

Accepted	
Access	442
Time Limits	326
Privacy	218
Total accepted	**986**

Closed Through Early Resolution	
Access	95
Time Limits	66
Privacy	52
Total	**213**

Closed Through Investigation	
Access	340
Time Limits	256
Privacy	104
Total	**700**
Total closed	**913**

*For a description of each of these categories of complaints, please see Appendix 1.

PRIVACY IMPACT ASSESSMENT REVIEWS

Received	**58**
Reviewed as high risk	31
Reviewed as lower risk	26
Total reviewed	**57**

AUDITS

Public sector audits completed	1

POLICY AND PARLIAMENTARY AFFAIRS

Draft bills and legislation reviewed for privacy implications	16
Public-sector policies or initiatives reviewed for privacy implications	54
Policy guidance documents issued	8
Parliamentary committee appearances on public-sector matters	5
Submissions to Parliament	2
Other interactions with Parliamentarians or staff	53

COMMUNICATIONS ACTIVITIES *

Speeches and presentations	138
News releases and communications tools	34
Exhibits and other offsite promotional activities	42
Publications distributed	13,351
Visits to principal OPC website	1.77 million
Visits to OPC blogs and other websites	865,280
New subscriptions to e-newsletter	364
Total subscriptions to e-newsletter	1,365

*Combined public and private sectors

REQUESTS TO THE OPC UNDER THE *ACCESS TO INFORMATION ACT*

Requests received	**64**
Requests closed	58

REQUESTS TO THE OPC UNDER THE *PRIVACY ACT*

Requests received	**11**
Requests closed	10

CHAPTER 1

The Year in Review:

KEY ACCOMPLISHMENTS DURING 2011-2012

Here are highlights of the work we did over the past fiscal year to strengthen and safeguard the privacy rights of Canadians in their dealings with the Government of Canada. Details are provided in subsequent chapters.

PRIVACY COMPLIANCE AUDITS

During the year, we conducted an audit of Veterans Affairs Canada in order to assess compliance with the *Privacy Act*.

The audit found the Department has taken a number of encouraging steps and is determined to regain the confidence of its more than 200,000 clients after the highly publicized mishandling of one veteran's most sensitive personal details.

Our Office's 2010 investigation of that very high-profile case brought to light serious systemic issues and prompted the broader audit.

The audit, described in detail in Chapter 3, found that senior management at Veterans Affairs Canada is committed to ensuring that the personal information handling practices of the Department comply with the *Privacy Act,* and it has been actively involved in monitoring the efforts made to address the deficiencies highlighted in our investigation.

Key elements of a comprehensive privacy management program are now in place. As well, the Department is monitoring access to veterans' files, refining system access controls and increasing employee awareness. It has also developed new policies, procedures, processes and guidelines to respect veterans' privacy.

INFORMATION REQUESTS, COMPLAINTS AND DATA BREACHES

Our Information Centre is responsible for responding to requests from individuals and organizations about privacy rights and responsibilities – an extremely important service we offer to Canadians. In 2011-2012, we received over 9,000 requests and almost 15 percent of those related to federal public sector issues.

Meanwhile, there were significant increases in both the number of *Privacy Act* complaints accepted and closed. In 2011-2012, we accepted 986 complaints – an increase of almost 40 percent from the year previous. Meanwhile, we concluded 913 complaints – a 60 percent leap from a year earlier.

A significant proportion of the growth in complaints to our Office originated with four institutions: the Correctional Service of Canada, National Defence, the Royal Canadian Mounted Police (RCMP) and Veterans Affairs Canada. We explore the reasons for these increases in Chapters 3 and 4.

Our use of early resolution has been growing steadily over the last several years. Early resolution can be used to effectively and quickly address some complaints by using negotiation and conciliation. In 2011-2012 almost a quarter of our closed files involved the use of early resolution.

Federal institutions reported 80 data breaches involving personal information in 2011-2012, the highest number of breach reports we've received in recent years. It is unclear whether the increase reflects more diligent reporting or an actual increase in incidents.

PRIVACY IMPACT ASSESSMENTS

We reviewed 57 Privacy Impact Assessments (PIAs) in 2011-2012. Of these, 31 were reviewed in greater depth because of the significance of the privacy risks or the broader societal issues involved. Many of our PIA reviews and consultations with departments related to public safety initiatives.

Federal government institutions are required to undertake PIAs for activities and initiatives involving personal information, to demonstrate that privacy risks have been detected and either removed or mitigated. Our Office receives copies of these assessments; we may review and make comments on them if we feel it is necessary.

POLICY AND PARLIAMENTARY AFFAIRS

Parliament had a reduced sitting schedule in 2011 as a result of the federal election in May. During 2011-2012, officials from our Office appeared five times before parliamentary committees and provided two written submissions, which is somewhat less than in previous years.

A number of the legislative and international initiatives the government embarked upon raised potential concerns for privacy – for example, the "lawful access" legislation (Bill C-30), the Canada-US Perimeter Security Action Plan, and the *Safe Streets and Communities Act* (Bill C-10).

REACHING OUT TO FEDERAL INSTITUTIONS

Outreach is an important part of our interactions with federal government departments and agencies. Examples of our outreach during 2011-2012 included: hosting a third annual workshop for public servants on Privacy Impact Assessments, developing a video to help public servants to understand the PIA process; and helping to organize an event for federal Access to Information and Privacy professionals with our colleagues at the Office of the Information Commissioner of Canada.

ADVANCING KNOWLEDGE

The incredible pace of technological change makes our task of protecting the privacy rights of Canadians a constantly evolving challenge. It is essential that we take time to fully understand, and reflect upon changes that impact on privacy. Knowledge is what enables us to keep up with all this change.

At times, we commission research related to the public sector to support the work of our Office. In 2011-2012, this included work on themes such as privacy in the age of social media, surveillance and citizen journalism; the gathering of national security intelligence via the private sector; the proliferation of drones and the use of DNA for law enforcement purposes.

CHAPTER 2

The Integration of Privacy in Public Policy

A look at some of the positive developments for privacy protection within the federal government over the last 30 years.

HISTORICAL LOOK BACK

From its very beginning 30 years ago, the Office of the Privacy Commissioner of Canada has pursued the goal of nurturing a privacy-sensitive culture within the federal public service.

The ombudsman's model for our Office and the absence of enforcement powers have dictated a collaborative approach to safeguarding the sensitive personal information of Canadians constantly being gathered by federal institutions.

With the support of many dedicated public servants, we have seen privacy steadily being integrated into the development of public policy throughout the past three decades.

That integration has gone through a few distinct phases.

Often, during the first 20 years, privacy was incorporated *after* a government initiative had been already put into action. Typically, a public complaint or an audit by our Office shone a spotlight on a privacy-invasive initiative and policy changes followed.

That happened with questions in the 1991 census about religion and fertility, which some Canadians complained were intrusive and which were withdrawn from the 1996 census.

We also saw a failure to consider privacy at the front end of an initiative with the Longitudinal Labour Force Survey, under which the then Human

Resources Development Canada had quietly amassed files – some with 2,000 pieces of information – on 33.7 million Canadians (many of them deceased).

Two weeks after its existence was exposed in our 1999-2000 Annual Report, the Department shut down this "citizen profile in all but name."

A second phase of integrating privacy in policy development began in 2002, when Treasury Board introduced the pioneering Privacy Impact Assessment (PIA) Policy.

Instead of the costly and cumbersome repairing of privacy transgressions after the fact, Privacy Impact Assessments are geared at prevention.

The TBS Directive on Privacy Impact Assessment (which replaced the former Policy in 2010) requires most federal government institutions to examine the privacy effects of new or significantly altered programs or activities. Departments and agencies need to determine what personal information will be collected.

When we review Privacy Impact Assessments, we look to see that federal institutions have demonstrated that there is a pressing and substantial public goal rationally connected to any activities that infringe on privacy.

We also expect empirical evidence showing how the proposed collection and use of personal information actually meets the needs of that public goal.

If privacy risks are identified, the PIA should describe and quantify those risks and propose solutions to eliminate the risks or mitigate them to an acceptable level.

The Government of Canada is a world leader in requiring federal institutions to undertake PIAs. Similarly, our Office is often consulted by international organizations and data protection authorities on our own process, which has developed and evolved over the past decade, for reviewing those PIAs. While institutions are not obliged to heed our advice, we find that most consider our recommendations and work with us to resolve or mitigate privacy concerns.

What began as a trickle (six PIAs in 2001-2002) has quickly swollen to a steady stream of assessments, which our Office handles on a triage basis, focusing on the initiatives which we believe pose the greatest privacy risks.

Between 2002 and the end of the 2011-2012 fiscal year, our Office has received a cumulative total of 588 PIAs, with 2009-2010 being the high water year with 103.

One notable success of the PIA approach involved the use of enhanced driver's licences for land border crossings – a story told earlier in this report, in the Commissioner's Message.

Our work on many other files has also had positive, privacy-protective results. A few examples follow.

Privacy Impact Assessment Reviews: Making an Impact

Whole-body imaging at airports

Extensive consultations between our Office and the Canadian Air Transport Security Authority (CATSA) contributed to better privacy protections, including ensuring that millimeter-wave imagers were used only for secondary screening, and only as a voluntary option to a traveller undergoing a physical pat-down. (In some other jurisdictions, whole-body imaging is used for primary screening and is mandatory.) Scanned images are viewed in a separate area by an officer who cannot see the passenger. Follow-up checks by our Office have recommended better enforcement of these agreed-upon privacy safeguards.

Secure Certificate of Indian Status Card

First Nations citizens must have government-issued Indian status cards to claim entitlements under the *Indian Act*. A PIA submitted by Indian and Northern Affairs Canada in 2009 proposed that a new "secure" version of this card should also serve as a border-crossing document under stricter U.S. security rules.

This would have meant that all the application information for status cards would automatically be registered with Canadian border authorities, and potentially with U.S. border authorities. Instead, the Department accepted our recommendation to allow card holders the option of choosing border-crossing features, or having the status card issued without them, thus preserving their right to use a passport or enhanced drivers' licence instead, as do other Canadians at the border.

Automated licence plate recognition program in British Columbia

Active since 2007, the RCMP's automated licence plate recognition program in British Columbia uses video cameras on marked and unmarked police vehicles, combined with pattern identification software, to identify licence plates on parked and moving vehicles. More than 3.6 million plates were recognized in the first two and a half years of the program.

The plate numbers are cross-checked against databases containing lists of stolen vehicles, suspended drivers and uninsured vehicles. A "hit" or match triggers further investigation and police intervention; fewer than two percent of checks produce hits.

Our review of the PIA from the RCMP noted that the police were retaining the "non-hit" information. We saw that as ubiquitous surveillance of law-abiding Canadians who had committed no infraction. The RCMP agreed to stop retaining the "no-hit" information for the present.

Over the past few years, we have seen a promising new phase of policy integration unfolding.

We see a greater number of federal departments and agencies approaching our Office about initiatives or expanded activities even before they have prepared a PIA.

For example, the RCMP recently briefed us about a proposal to develop a centre to support investigations about missing persons and unidentified human remains.

In addition to a database accessible only to law enforcement agencies, the RCMP intends to create a public database with limited details about missing persons and unidentified remains.

Our Office reviewed with the RCMP concerns about data matching, limiting database access and the use of a public website to post details and solicit tips.

Such advance consultations span a wide range of programs – increased scrutiny of international students (Citizenship and Immigration Canada); developing international cyber security initiatives and protocols (Public Safety Canada); a cyber authentication renewal initiative, which includes using private-sector credentials to authenticate users of online government programs (Shared Services Canada); and a study of possible options for the 2016 census and beyond (Statistics Canada).

This dynamic integration of privacy in policy development has the potential to confer significant public benefits. It means that the public's privacy interests are taken into consideration at the earliest stages of developing policy for new programs. In turn, that should lead to speedier implementation of programs that are more privacy-aware.

Our process for reviewing PIAs is also evolving. Our Office is undertaking more site visits to supplement the paper-based review and is more frequently calling upon the expertise of our policy and technological specialists when reviewing PIAs. The help and collaboration of experts from other branches of our Office allows us to more effectively undertake complex and demanding examinations. In turn, our work on PIA files has helped to inform other branch activities, including parliamentary appearances, audits, inquiries, and complaint investigations.

Overall, PIAs provide our Office with an extremely valuable window through which we can view how initiatives are being rolled out across the entire federal government.

THE CURRENT YEAR

PRIVACY IMPACT ASSESSMENT REVIEWS

A thorough Privacy Impact Assessment can help ensure that the government collects only information to which it is legally entitled and which is necessary for a legitimate program, activity or initiative; that it properly protects the information; that it safeguards the information from inappropriate or illegal disclosures; and that it disposes of the information in a timely fashion when no longer needed.

We received 58 new PIAs during the past fiscal year.

Including some files submitted in the previous year, we reviewed 57 PIAs in 2011-2012. We sent out 31 detailed letters of recommendation for initiatives we felt were particularly intrusive, and an additional 26 letters with less detailed, high-level recommendations for initiatives which, in our view, posed lower privacy risks.

We also offered advice and recommendations at the request of government institutions on another 19 issues ranging from security clearance protocols to records storage and the use of personal information for social science research.

We welcome requests for these meetings and believe this consultative process is influential in helping to build data protection measures into government programs at the outset.

Here is a sample of these PIA reviews and consultations.

CITIZENSHIP AND IMMIGRATION CANADA
Visa Application Centre – Mexico

Citizenship and Immigration Canada consulted extensively with our Office on new requirements being introduced for temporary resident visa applicants, and on changes to the overseas application process. Staff at privately contracted visa application centres help individuals to fill in applications, provide information, verify that applications are complete and forward applications to Citizenship and Immigration for further processing and decision-making.

The way in which the Department establishes these overseas visa application centres is changing. Going forward, contracts with service providers will be managed by Citizenship and Immigration headquarters rather than by the Department's regional offices.

In some countries, applicants will be required to enroll their fingerprints at the visa application centre; these, along with a digital photograph, will be used to verify identity when the visa holder arrives at the Canadian port of entry.

We received a PIA for the Mexico Visa Application Centre in July 2011, and made recommendations

about the collection of sensitive personal information by private sector contractors, as well as recommendations about the necessity to safeguard key documents. We also made broad recommendations for particular care in the safeguarding of fingerprints, which will be required for visa applicants from some countries, which are yet to be determined, starting in 2013.

We also raised questions about access to individuals' personal information by the governments of the countries in which the centres are located. We have asked that our Office be informed when the Department decides which countries must submit fingerprints for visa applications. We also requested that the PIA be revised to reflect the need for additional safeguards for the protection of sensitive biometrics.

To ensure that the independent service providers adhere to the privacy protection clauses in their service agreements, we recommended that Citizenship and Immigration regularly audit visa application centres. Citizenship and Immigration has indicated that it will do so, and that agreements may be terminated if service providers don't measure up.

ROYAL CANADIAN MOUNTED POLICE
Video Surveillance, Parliament Hill, Phase II

We reviewed a preliminary PIA on the expansion of video surveillance activities on Parliament Hill, which is a joint project of the Royal Canadian Mounted Police (RCMP) and the security divisions of the Senate, House of Commons and Public Works and Government Services Canada.

Phase I of the video surveillance project was completed in 2003 with the installation of 50 cameras on the roofs of the Parliament buildings. Phase II contemplates the installation of an additional 134 video cameras over the next three years. The areas under camera surveillance include exterior perimeters of all buildings, pedestrian doors and assembly areas.

Some cameras will offer panoramic views and zoom capability and the video stream will be monitored 24/7.

We were concerned about the scope of the project and its potential impact on the privacy rights of Parliamentarians, Parliamentary staff, guests and visitors to Parliament Hill, and of those engaging in peaceful protests and assemblies. According to the preliminary PIA, a deliberate decision was made to not post signs notifying individuals of video surveillance on Parliament Hill.

That decision was of special concern to our Office. We referred the RCMP to our *Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities*, which state that the public should be notified by signage when surveillance cameras are in place.

We recommended that a full PIA be completed on the project, which will allow us to continuously assess future phases as they are implemented.

We also asked for a site visit to the video surveillance operations centre in order to observe collection, retention and disclosure practices. The RCMP responded positively, indicating they will share our concerns about signage with their partners in the project, and that a full PIA will be undertaken. A site visit was arranged, which added greatly to our knowledge and understanding of this project. We are in ongoing consultations with the RCMP, and will continue to follow this file closely.

National Victim Assistance Policy

The RCMP supplies police services under contract to all provinces and territories in Canada, except Quebec and Ontario. While the RCMP is subject to the *Privacy Act*, it also must respect provincial laws and policies where it operates.

One of the most interesting and challenging files during the past fiscal year involved the provision of personal information about victims of crime by RCMP members, working under contract to provincial governments, to provincially based victim services organizations without the consent of the victim – and, in some cases, when victims have specifically declined the service. This is known as "proactive referral."

While we recognize the importance of victims receiving the support and services to which they are entitled, we have several concerns about this practice when viewed through the lens of privacy.

We consulted closely with the RCMP and with provincial data protection commissioners during our review of this PIA, and a team from our Office visited victim services organizations in British Columbia. Our staff was impressed by the dedication of the victim services organizations to helping individuals whose lives have been affected by crime.

However, given the highly sensitive nature of the information being shared, and the applicability of the *Privacy Act* to the RCMP, we recommended that the RCMP reconsider the proactive referral policy. We also indicated that before personal information is shared with a third-party organization, the consent of the victim should be obtained.

When the victim does give consent, we recommended that the RCMP ensure victim services organizations have appropriate processes in place to guarantee the information received is protected and disposed of properly. We also recommended that the RCMP undertake regular audits to ensure these provisions are being met.

In addition, we suggested that the RCMP explore different and less privacy-intrusive methods of encouraging victims to give consent for referrals to victim services. This might include a targeted public outreach campaign in cooperation with provincial governments and provincial victim services organizations. We are continuing to consult with the RCMP on the issues raised by the PIA.

SHARED SERVICES CANADA
Access Key Service

We continued to review the Access Key Service, which is now under the responsibility of Shared Services Canada. The Access Key Service authenticates individuals and businesses in their online dealings with the Government of Canada.

We held numerous meetings with federal government institutions involved in this initiative, including Shared Services Canada and the Treasury Board Secretariat.

We have been assured that any federal government institution planning to offer online services or programs using the Access Key Service must first undertake a comprehensive risk assessment to ensure that the level of protection they will offer is commensurate with the risks and the sensitivity of the information involved in the online transaction.

We will continue to watch this file carefully as the government's online authentication renewal plan continues to evolve. The Access Key Service is to be phased out at the end of 2012, and will be replaced by a new Government of Canada branded credential. We will be reviewing a PIA for that initiative.

Credential Broker Service

In conjunction with the Access Key Service and as part of the federal government's Cyber Authentication Renewal Strategy, Shared Services Canada is introducing a new component of its service to authenticate Canadians when they use online government services.

The new Credential Broker Service, operating under contract to the government, will allow individuals to use online credentials issued by the private sector – such as electronic banking credentials – to sign onto Government of Canada services.

We have consulted closely with Shared Services Canada, the Treasury Board Secretariat and Public Works and Government Services Canada. We received a PIA on this initiative; however, it was lacking in required documentation and we asked that a revised PIA be submitted. Shared Services Canada agreed to do so. In the meantime, we continued our discussions, and have raised concerns related to the levels of authentication offered in the service and possible issues of accountability gaps if privacy breaches were to occur.

We have been reassured that appropriate mitigating measures are being built into the process and that privacy protective clauses are contained in the contracts between the federal government and the private-sector credential broker service.

CORRECTIONAL SERVICE OF CANADA
Disclosures for Health Research

The Correctional Service of Canada submitted a PIA about sharing the health information of inmates with Canadian academic institutions wishing to research the health of the federal offender population.

The PIA stated that this research is important to the safe transition of offenders into the community; to provide effective health services for First Nations, Métis, and Inuit offenders; and to improve mental health services. However, the file submitted to us lacked details on the actual research projects and did not include specifics of data-sharing agreements.

We had concerns about this vagueness, given the sensitivity of the information involved. We were also concerned that each unique research project may require different data elements and may create different technical risks.

We asked the Correctional Service of Canada to conduct separate PIAs for each data-sharing agreement. This will help ensure thorough analysis and mitigation of the specific and unique privacy risks that may be implicated in each research project.

We also asked that the agency carefully consider its proposed use of subsection 8(2(*j*)(i) of the *Privacy Act* for these disclosures. This section of the Act allows information to be disclosed for research purposes in an identifiable format only if the head of the institution is satisfied that the purpose for which the information is disclosed cannot reasonably be accomplished in any other manner. We are asking that the Correctional Service of Canada individually assess the merit of each research activity in order to make this determination.

CANADIAN AIR TRANSPORT SECURITY AUTHORITY Passenger Behaviour Observation Pilot Project

Another significant review was the analysis of the Passenger Behaviour Observation pilot project, which was launched by the Canadian Air Transport Security Authority (CATSA) in 2011. The field trial took place over a five month period from February to July 2011. This initiative involved specially trained officers who observed passengers awaiting clearance at the airport security checkpoint in order to look for suspicious behavior.

As we reported in our 2010-2011 Annual Report, our review of a PIA for Passenger Behaviour Observation raised concerns about the effectiveness of the initiative in identifying threats to aviation security. We noted the potential for inappropriate risk profiling, based on characteristics such as race, ethnicity, age or gender.

In addition to reviewing the PIA and consulting extensively with CATSA, we organized a site visit to see the project in action at the pilot site, Vancouver International Airport.

A PIA review officer and a technical analyst conducted a site visit in June 2011, and spoke at length with CATSA officials directly involved with the program at the airport.

The site visit added greatly to our knowledge of the initiative and helped us in our evaluation of the project's risks to the privacy and personal information of individuals.

We plan to increase our use of site visits in the future, as they have proven to be valuable adjuncts to the documents submitted to us for our review during the PIA process.

PARLIAMENTARY ACTIVITIES

Another way in which privacy can be integrated into policy development is through exchanges and interactions between our Office and Parliament.

Our discussions and submissions can lead to substantive changes that offer better protections for the privacy of Canadians. Of course, Parliament decides if and how our contributions can best be utilized.

National security and public safety issues, including lawful access legislation and border security, loomed large during the year.

The 2011 federal election meant fewer sitting days for Parliament during the past fiscal year and, as a result, fewer formal appearances before Members of Parliament and Senators than usual for our Office.

The Commissioner and other officials from our Office appeared five times and we made two written submissions. Among the issues discussed were:

- The *Safe Streets and Communities Act*;
- Privacy implications of potential changes to the immigration system; and
- Proposed changes to existing legislation covering money laundering and terrorist financing.

The following highlights some of our parliamentary work in 2011-2012:

Lawful Access

The interplay between privacy and security is a fundamental question to any open, democratic society. Our Office understands the need and the importance of integrating privacy protections into public safety measures.

The *Investigating and Preventing Criminal Electronic Communications Act* (Bill C-30), introduced in February 2012, is but the latest incarnation of a longstanding project by authorities to recast Canada's legal framework regulating use of electronic surveillance.

Our Office has had a lengthy history with this effort and our exchanges with government on it extend back as far as the mid-1990s.

Our Office understands the challenges faced by law enforcement and national security authorities in fighting online crime – especially in an era of evolving communications technologies.

However, legislation that seeks to recalibrate police powers online must demonstrably help protect the public, respect fundamental privacy principles established in Canadian law and be subject to proper

oversight. It is a standard of Canada's approach to surveillance that the invasiveness of a new police power or investigative method must be offset by similar levels of legal review, accountability and oversight.

Canadians care passionately about their right to privacy. Citizens from all walks of life, from every part of the country, irrespective of age and upbringing connect instinctively with this issue.

And so, when the government is proposing new methods of electronic surveillance – and contemplating the ideal balance between effective security and meaningful privacy – the views of citizens must be taken into account.

Since 2005, we have made our concerns public in parliamentary submissions and statements, responses to government consultations, communiqués issued with our provincial and territorial privacy counterparts, as well as in letters to responsible Ministers and lead departments. We have articulated these same concerns in speeches before professional associations, conference presentations, discussion papers and even classroom lectures.

In October 2011, we sent an open letter to the Minister of Public Safety to once again articulate our deep concerns prior to the reintroduction of legislation.

The proper treatment of personal information and the safeguarding of citizen's rights and freedoms in the context of national security are among the government's most pressing duties. Privacy protection is not an ancillary issue in this domain, but at the heart of the social freedoms that governments are bound to safeguard.

To date, Canadians have not been given sufficient justification for the proposed new powers when other, less intrusive alternatives could be explored. A focused, tailored approach is vital.

In February 2012, the federal government introduced the latest version of lawful access legislation, which proposes to expand the legal tools of the state to conduct surveillance and access private information.

For many years, our Office has been urging a cautious approach to creating an expanded surveillance regime that would have serious repercussions for privacy rights. We are not convinced that the latest bill takes the focused, tailored approach necessary to avoid the erosion of our free, open society.

We do recognize that the government, in that bill, reduced the number of data elements which could be accessed by authorities without a warrant or prior judicial authorization. There were also certain oversight provisions included in the latest version of the bill.

On balance, however, the legislation contains serious privacy concerns, similar to past versions.

In particular, we are concerned about access, without a warrant, to subscriber information behind an IP address. Since this broad power is not limited to

reasonable grounds to suspect criminal activity or to a criminal investigation, it could affect any law-abiding citizen.

The ongoing privacy issues that remain outstanding include:

- The scope of the new powers, which can be accessed by a wide range of provincial and federal authorities;
- Access to personal information without judicial authorization, including instances unrelated to crime or security issues;
- The lack of public reporting, which lessens accountability and complicates Parliamentary review; and
- The absence of dedicated review, to properly control and check on the use of new investigative tools.

We look forward to sharing our detailed views on this bill with Parliament when Bill C-30 is studied in Committee.

Canada-U.S. Perimeter Security Action Plan

Another important public safety issue was the Canada-U.S. perimeter security initiative, the stated goal of which is to increase security and ease trade along our shared border. While details continue to emerge month by month, our Office has strongly advocated that all initiatives flowing from the agreement must truly and properly integrate and respect the privacy rights and legal protections expected by Canadians.

Prime Minister Stephen Harper and U.S. President Barack Obama signed the *Beyond the Border Declaration* in February 2011. Our Office subsequently participated in the government's public consultation and submitted a series of recommendations touching on the privacy risks stemming from the various elements of the perimeter security model. These themes included: guiding privacy principles, health emergency plans, cyber security, biometrics, traveller monitoring, information sharing and border screening measures.

Submission by the Office of the Privacy Commissioner of Canada to the Government of Canada's Beyond the Border Working Group public consultation.

Following those discussions, the *Canada-US Perimeter Security Action Plan* was released in December 2011.

This served to set the stage for our Office and our provincial and territorial colleagues to release a joint resolution on the initiative. The document stresses the importance of privacy protection in the new security initiatives and intelligence-sharing channels flowing from the governments' Action Plan.

In our recommendations to the federal government, we have stressed that:

- Any initiatives under the plan that involve the collection of personal information should also include appropriate redress and remedy mechanisms to review files for accuracy, correct inaccuracies and restrict disclosures to other countries;
- Parliament, provincial privacy commissioners and civil society should be engaged as initiatives under the plan take shape;
- Information about Canadians should be stored in Canada whenever feasible, or at least be subject to Canadian protection; and
- Any use of new surveillance technologies within Canada such as unmanned aerial vehicles must be subject to appropriate controls set out in a proper regulatory framework.

Our Office has already made provisions for the added review function and activities we anticipate in connection with the initiative's various new programs – reviewing Privacy Impact Assessments, offering comment on regulatory revisions and providing information to Parliamentarians on new legislative proposals and privacy issues flowing from the joint US-Canada security effort.

Safe Streets and Communities Act

The *Safe Streets and Communities Act* reintroduced a number of measures aimed at increasing penalties for certain crimes that had previously been included in nine bills debated by Parliament during a previous session, but not passed.

We advised Parliamentarians that the legal changes proposed in this omnibus legislation would have significant and lasting effects on privacy rights for many Canadians.

These effects are not limited to individuals convicted of criminal offences. For instance, people working at, or visiting a correctional institution, or married to or visiting certain imprisoned individuals could find their personal information collected more readily and shared more broadly among government agencies.

Our Office offered recommendations to mitigate potential violations of privacy and minimize unnecessary collection of the personal information of law-abiding Canadians. We cautioned government to establish robust controls and limits to narrow the collection, use, disclosure and retention of personal information to only that which is appropriate and necessary.

None of our recommendations were incorporated and the legislation received Royal Assent on March 13, 2012.

Money Laundering and Terrorist Financing

The Commissioner appeared before the Senate Standing Committee on Banking, Trade and Commerce on March 1, 2012, during its review of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*.

During her testimony, she shared her concerns about a possible expansion of Canada's anti-money laundering and anti-terrorist financing regime without evidence that further changes were needed to address domestic problems.

Canada already has an expansive regime that, as we found in our 2009 audit, leads to the over-reporting of vast amounts of personal information about Canadians while failing to provide conclusive evidence about its effectiveness and its impact on Canadians.

Audit of the Financial Transactions and Reports Analysis Centre of Canada (2009)

The Commissioner recommended that the Senators fully assess the effectiveness of the regime and explore whether other measures could be more demonstrably efficient and less privacy-intrusive in combating money laundering and terrorist financing.

If the federal government is convinced that additional changes are absolutely necessary for law enforcement and national security purposes, the Commissioner underscored the importance of the government providing public justifications for these changes, supported by data and evidence. In 2012-2013 we plan to table our second audit of the Financial Transaction and Report Analysis Centre of Canada.

Security of Canada's Immigration System

The Commons Standing Committee on Citizenship and Immigration agreed in December 2012 to study the security of Canada's immigration system. Specifically, the Committee examined what gaps exist and the actions the federal government had taken or planned to take to enhance that security.

Appearing before the Committee on February 16, 2012, the Commissioner stressed that the *Privacy Act* imposes obligations when the federal government collects personal information. Federal agencies must ensure certain safeguards, limit secondary use, and list their data holdings publicly, whatever the citizenship of the individuals involved.

The Commissioner also told Committee members that if the federal government made any legislative or regulatory changes to the immigration system, she would expect detailed PIAs from the appropriate institution.

Finally, she emphasized the necessary tension between the scrutiny of visitors and Canada's global commitment to rights and freedoms. These values are embedded in the privacy obligations of government when it processes the personal information of

individuals, either as they visit our country or take their first steps toward citizenship.

Census

Following the abolition of the Long Form Census, Statistics Canada consulted extensively with our Office on its Report on 2016 Census Options: Proposed Content Determination Framework and Methodology Options.

Statistics Canada explored methodological options for conducting the Census of Population in 2016 and beyond. These options, based on international practices, include the traditional census methodology currently used in Canada, the use of administrative records and surveys to supplement the short-form census and a census based on the creation of a Central Population Register using a universal PIN.

In our response, we indicated we could not support the use of a universal and mandatory PIN and a Central Population Register as a viable option. We also expressed strong reservations when it comes to the use of additional administrative data records for census purposes.

We continue to work with Statistics Canada.

CHAPTER 3

Challenges for Information Management

Three decades after the Privacy Act *was passed, there remains room for substantial improvement in terms of how some federal government departments address the protection of personal information.*

While there have been some very positive developments for privacy in the federal government over the past 30 years, some challenges remain.

This chapter describes some of the areas where there remains room for improvement.

Two themes are interwoven throughout the case studies that follow:

First, the need for improved anticipation of potential problems involving the management of personal information; and, second, the need for better training in how to reduce those risk areas.

For example, better training should have led correctional officers to question the propriety of posting inmate medical appointments in plain view at a federal penitentiary. Who amongst us wants our co-workers (or fellow inmates, as the case may be) to know, not only when we're seeing the doctor, but even the purpose of the visit? Similarly, a lack of awareness of procedures led officials to, not once, but twice, wrongly reveal the severity of a disability suffered by a member of the Canadian Forces to people who had neither the need, nor the right to know.

However, clear direction from the top and a well-conceived training and communication plan can make a huge improvement in privacy awareness and in the management of personal information.

Our exhaustive audit of Veterans Affairs Canada paints an encouraging picture of a Department

determined to regain the confidence of its more than 200,000 clients after the highly publicized mishandling of one veteran's most sensitive personal details.

This chapter also shines a spotlight on two other departments which have consistently been on our Office's Top Five list for complaints over the last decade – the Correctional Service of Canada, which is in a league of its own in terms of the volume of complaints to our Office, and the Canada Revenue Agency.

There are intrinsic reasons why certain federal institutions are liable to continue to generate a substantial number of *Privacy Act* complaints. They hold a huge volume of personal information, much of it highly sensitive.

However, there are also ongoing privacy concerns related to those two institutions. In some cases, a genuinely *proactive* approach could lead to stronger privacy management and thus, fewer complaints.

Data breaches remain another source of continuing concern. The number of breaches reported to our Office last fiscal year hit an all-time high.

As examples demonstrate, many of those breaches could have been avoided by the exercise of some common sense. And others could have been averted if people had followed existing rules.

Finally, endlessly delaying access to personal information is no different than refusing access outright. That was the intended message when Parliament included a maximum time limit of two months for responses to requests made under the *Privacy Act*.

Yet this deadline is too often missed. In some cases, delays have even stretched into years.

AN AUDIT OF VETERANS AFFAIRS CANADA

Background

In October 2010, the Commissioner released the results of an investigation into a complaint alleging that Veterans Affairs Canada mishandled an individual's personal information.

The investigation brought to light serious systemic issues, prompting our Office to launch the audit of Veterans Affairs.

The investigation found that the veteran's sensitive medical and personal information was shared – seemingly with no controls – among departmental officials who had no legitimate need to see it. This personal information subsequently made its way into ministerial briefing notes about the veteran's advocacy activities.

The investigation confirmed that two ministerial briefing notes about the complainant contained

personal information that went far beyond what was necessary for the stated purpose of the briefings. This included sensitive medical information as well as details about how the complainant interacted with the Department as a client and an advocate for veterans.

The Commissioner concluded that the Department was not compliant with the *Privacy Act* and lacked adequate controls to safeguard the personal information of veterans.

The Commissioner recommended that Veterans Affairs:

- Develop an enhanced privacy policy framework to regulate access to personal information within the Department;
- Revise information management practices and policies to ensure that personal information is shared within the Department on a need-to-know basis;
- Ensure that consent for the transfer of personal information has been obtained and that the information shared is limited to that which is necessary; and
- Provide training to employees on how to handle personal information.

In response to the Commissioner's report, and at the request of the then Minister of Veterans Affairs, the Department developed a 10-point Privacy Action Plan to address these recommendations.

As part of this plan, the Department:

- Implemented a privacy governance structure;
- Developed policies, procedures, processes and guidelines for managing veterans' personal information;
- Established mandatory privacy training for employees; and
- Instituted monitoring of the Client Service Delivery Network, the primary electronic repository for veterans' personal information.

About Veterans Affairs Canada

Veterans Affairs Canada provides programs and services to more than 200,000 clients, including veterans from the Second World War and Korean War as well as former and serving members of the Canadian Forces and eligible family members. The Department also administers disability pensions and health care benefits for certain serving and former members of the Royal Canadian Mounted Police.

With approximately 3,900 employees, Veterans Affairs operates three regional offices and 35 service points across Canada. The Department has also established 24 integrated personnel support centres with the Department of National Defence.

More information is available at www.veterans.gc.ca.

What We Examined

We reviewed the Department's personal information management policies, procedures and processes, program records, guidelines, Privacy Impact Assessments, security reviews, training materials, information-sharing agreements and contracts with third-party service providers.

We also examined the controls in place to protect personal information stored in electronic and hard copy format. In addition, we looked at a sampling of veterans' files.

The objective was to assess whether the Department has implemented adequate controls to protect the personal information of veterans, and whether its policies, procedures and processes for managing such information comply with the fair information practices embodied in sections 4 through 8 of the *Privacy Act*.

The audit did not include a review of the Department's management of personal information about its employees or contract personnel or the programs administered for the RCMP. Nor did we examine the personal information handling practices of the Veterans Review and Appeal Board, the Office of the Veterans Ombudsman, the Bureau of Pension Advocates, Ste. Anne's Hospital or the Department's third-party service providers.

Why This Issue is Important

The Department offers a wide range of programs and services to veterans, their dependents and survivors. This requires the collection and use of sensitive personal information and the maintenance of a large repository of that information.

The data holdings are not only voluminous, they are also highly sensitive. In addition to biographical data (names, dates of birth, marital status, etc.), veterans' files may contain military service records, employment and educational histories, financial and medical information.

The unauthorized use and disclosure of personal information could have a significant impact for veterans, their dependents and survivors. This could include financial loss resulting from identity theft or fraud, humiliation or damage to reputations, or risk to personal safety.

Veterans Affairs Canada has a legal obligation to ensure that policies, procedures and controls are in place to protect personal information collected under its mandate. This is essential in order for the Department to maintain the confidence of veterans in its ability to preserve the confidentiality of information entrusted to it.

What We Found

Senior management at Veterans Affairs Canada has expressed a commitment to ensure that the personal information handling practices of the Department comply with the *Privacy Act,* and it has been actively involved in monitoring the efforts made to address the deficiencies highlighted by the Privacy Commissioner in October 2010.

Key elements of a comprehensive privacy management program are in place.

An internal governance structure has been formalized to foster a culture of privacy throughout the organization, and to provide a coordinated and consistent approach to managing privacy in day-to-day operations. Information management and privacy experts have been engaged to examine and identify opportunities for improving the Department's personal information management practices.

As well, investments have been made in monitoring access to veterans' files, refining system access controls, increasing employee awareness, and developing new policies, procedures, processes and guidelines to respect veterans' privacy.

Our 2010 investigation report centred on two ministerial briefing notes containing personal information beyond what was necessary for the stated purpose of the briefings.

Veteran Affairs Canada: Audit Report of the Privacy Commissioner of Canada

Within a month, the Department established guidelines for preparing briefing notes and other documents for internal use, as part of its Privacy Action Plan.

The guidelines emphasize that briefing material should contain only personal information that is absolutely necessary to meet the objective of the briefing. Employees are also instructed to consider whether this objective can be achieved without including personal identifiers, such as the names of veterans.

Employees involved in drafting client-specific briefing notes and background reports received training on the new guidelines. The Department also established centralized work units to process ministerial briefing documents.

As part of our audit, we reviewed a sample of 88 client-specific ministerial briefing documents that were prepared between April 2011 and March 2012.

We found that virtually all of them adhered to the need-to-know principle – the personal information revealed was limited to that necessary to fulfill the purpose of the briefing.

While two briefing documents contained information that extended beyond what was strictly required, it should be noted that those particular documents were prepared before a quality assurance process was set up in the fall of 2011.

Fair Information Practices

Fundamental to privacy protection is the principle that personal information should be collected only if there is a legitimate and authorized need directly related to an operating program or activity. We found that the Department's collection activities are relevant and are not excessive, and that veterans' personal information is used for authorized purposes.

However, there is room for improvement in how the Department manages veterans' consent. Generally, the Department obtains consent before releasing a veteran's personal information to a third party (e.g. external service provider, family member, etc.). But we observed consent forms that did not specify the third party or the information the Department was authorized to release. Further, we noted disclosures had been made and the corresponding consent was not included in the file.

Similarly, we found that details surrounding consent were not always entered in the Client Service Delivery Network, the primary electronic repository for veterans' records. A concerted effort is needed to ensure consent is consistently and sufficiently recorded on file. Otherwise, there is a risk that the Department may mistakenly disclose veterans' personal information.

We recommended that Veterans Affairs Canada ensure that veterans' consent is consistently recorded on file, and is easily accessible for verification. We also recommended that the Department establish mechanisms to provide assurance that consent is accurately reflected in the Client Service Delivery Network.

The Department has established schedules that set out how long personal information may be retained before it is destroyed. We found that an extremely large number of paper files have been kept beyond their retention period.

Prior to 2008, the files of all veterans were deemed to have historical value and, as such, were retained indefinitely. In 2008, however, the Librarian and Archivist of Canada changed the designation of some of those files to non-archival, with a retention of seven years after the death of the veteran.

As a result, the Department is in the process of reviewing the contents of more than two million paper files to determine which records may now be destroyed.

Further, the Client Service Delivery Network lacks the technical capability to dispose of records, meaning that information is kept indefinitely in that database.

We recommended that Veterans Affairs Canada implement systems to ensure electronic and paper records are disposed of upon the expiration of their established retention periods.

Safeguarding Veterans' Personal Information

Ensuring that access to personal information is restricted to those with a legitimate need is a key safeguard in privacy protection. The results of our 2010 investigation prompted Veterans Affairs to undertake a review of employee access rights to the Client Service Delivery Network.

All positions were examined as part of the exercise. Managers were required to submit the rationale for each access level deemed essential for employees to perform their duties. The submissions were reviewed by a Departmental committee and either accepted or rejected, often after questioning the rationale provided.

As a result of this review, system access privileges were removed for approximately 500 employees. Moreover, access levels were reduced for 95 percent of the remaining positions.

However, we noted that Veterans Affairs uses a manual process to establish and maintain access levels – an approach which risks inappropriate levels of access for some employees.

We recommended that to mitigate the risk of employees having access to veterans' information that they do not need, the Department should automate access controls based on roles, not individuals, for the Client Service Delivery Network.

The Department has contracted a third party, Medavie Blue Cross, to manage the processing of veterans' health care claims and certain services. As part of the arrangement, Medavie implemented the Federal Health Claims Processing System, which it owns and operates.

Although processes and procedures are in place to manage access to the system by Veterans Affairs employees, the Department has not conducted a review to ensure its employees' access privileges are in keeping with the need–to-know principle. Our sampling of 26 user accounts found that more than a third had access to information not required for their defined roles.

We recommended that Veterans Affairs Canada review employees' access to the Federal Health Claims Processing System to ensure user privileges are in keeping with the need-to-know principle. We also indicated that the Department would benefit from automating role-based access within the system.

With the exception of two regional offices and one district office, the Department has outsourced the disposal of veterans' paper records to private shredding companies. Approximately one-third of the arrangements are not governed by written contracts with terms and conditions that satisfy Treasury Board security requirements.

There is also an absence of systematic monitoring to verify that records are destroyed in a secure manner. Of the 25 sites where records are shredded on-

site, 10 reported that the process is not monitored. We also confirmed that the Department does not systematically monitor contractors' off-site disposal practices through periodic inspections.

We recommended that Veterans Affairs Canada ensure that written contracts are established for all outsourced disposal of personal information, under conditions that meet Treasury Board requirements. We also recommended that the Department monitor the on-site disposal of records and implement a protocol for monitoring contractors' off-site destruction practices.

Privacy Management and Accountability

A comprehensive approach to privacy breach reporting can assist departments to better manage privacy risks, allowing them to adjust their policies, processes and practices based on lessons learned. In March 2011, Veterans Affairs established a protocol to address privacy breaches with four steps: (1) breach containment and preliminary assessment; (2) evaluation of the risks associated with the breach; (3) notification; and (4) prevention.

Although the Department's protocol provides a framework for doing so, we found evidence of privacy breaches that were not reported to head office and/or the Access to Information and Privacy Coordinator.

We recommended that Veterans Affairs reinforce the requirement for employees and contract staff to report all known or suspected privacy breaches.

In October 2010, Veterans Affairs launched a mandatory privacy awareness program for all employees.

The program is supplemented by privacy-related bulletins and other resources that are accessible on the Department's intranet site. While the various training initiatives have been successful in underscoring the importance of maintaining client confidentiality, employees would benefit from an enhanced awareness of core privacy principles.

Conclusion

The Department has sent a clear signal that privacy is vital to its operations and it has dedicated significant resources to improving the way it manages the personal information of veterans. With committed leadership, structures and control mechanisms in place, the Department is well positioned to move from reacting to privacy issues to proactively addressing them.

Veterans Affairs Canada has responded positively to our findings and will be implementing all of the recommendations in this audit.

VETERANS AFFAIRS CANADA INVESTIGATIONS

In comparison to other departments, Veterans Affairs Canada has not historically been the subject of a large number of complaints. (Our Office has closed a total of 157 complaint files involving Veterans Affairs since 1983.)

However, the high public profile of the issues we investigated in 2010 likely led to an increase in requests for personal information files by other veterans, which, in turn, triggered a surge in complaints to our Office.

In 2011-2012, we accepted 39 new complaints against Veterans Affairs Canada – an increase from 15 complaints in the previous fiscal year.

Perhaps not surprisingly, this surge included numerous complaints about time limits – 18 of the 39 – and, in turn, those can primarily be traced to a few requestors seeking large numbers of records.

The encouraging news is that seven of the 39 complaints were resolved through our early resolution process.

This included a case where our investigation determined that medical records sought by a complainant had been transferred to the federal archives from a former veterans' hospital and subsequently destroyed.

Complaints related to access also increased in the fiscal year, to nine from five previously. Formal privacy complaints – which include collection, retention and disposal, and use and disclosure types of complaints – remained constant at 10.

The findings of the investigations summarized below confirmed some of the concerns we identified in the 2010 investigation that led to our decision to audit Veterans Affairs Canada.

Veterans Affairs Withholds Father's Pension File from Family

The adult children of a veteran who had passed away applied for the documents in his pension file held by Veterans Affairs Canada. The Department refused to release the documents on the grounds that the *Pension Act* obliged it to protect personal information for 20 years after death and also that the adult children were not eligible to receive any of the veteran's pension benefits.

Through a lawyer, the children complained to our Office that the documents were necessary for the administration of their father's estate. In particular, they stated that the pension entitlement had not been fully paid and the pension claim may have been processed in bad faith by Veterans Affairs.

Our Office concluded that it was not reasonable for Veterans Affairs to dictate to an estate what information it requires in order to administer an estate. Under the *Privacy Act*'s Regulations, the

complainants are entitled to the pensioner's personal file to carry out the administration of the estate.

We upheld the complaint as **well founded**.

After the findings were communicated to Veterans Affairs, the Department informed us that it had released the veteran's pension file to his survivors.

Copying Google Result is Collecting Personal Information

In June 2010, an individual contacted officials at Veterans Affairs and the National Capital Commission to obtain information about the Aboriginal War Veterans Monument, which had been unveiled in Ottawa in 2001.

Subsequently, the individual complained that his personal email address had been disclosed to new recipients added to the email thread.

One of those new recipients, a Veterans Affairs official, put the individual's email address into a Google search to see if it was publicly available. That search turned up a Google group discussion page, where the individual had posted personal information about his education and his views on open government. His email address was "masked" by Google on that page – which means that users must enter special characters on the page in order to "unlock" and view the complete email address. This is defined by Google as "email masking", intended to prevent automated computer programs from harvesting full email addresses for spamming purposes.

Nonetheless, the Veterans Affairs official responded to the individual: "Your email is public domain. Like mine," and emailed that message, along with the webpage URL, to the entire email thread.

The individual complained to our Office that his personal information had been improperly collected.

Under section 4 of the *Privacy Act*, personal information collected by a government institution must relate directly to an operating program or activity of the institution. Our Office concluded that Veterans Affairs did not have a demonstrable need to collect the URL linking to the personal information posted by the complainant on the Google group discussion page.

Veterans Affairs contended that the public availability of information on the Internet is incompatible with a claim of privacy.

However, concerning personal information that is publicly available, the *Privacy Act* draws a distinction between its use and disclosure – which is not protected – and its collection, which still must relate directly to an operating program or activity.

Accordingly, the collection of the complainant's URL violated the *Privacy Act* and the complaint was **well founded**.

The Department apologized to the individual by letter and took steps to ensure that the email was deleted from its computer systems.

Veterans Affairs Improperly Reveals Severity of Disability – Twice

A serving member of the Canadian Forces who was receiving a disability pension required immediate medical treatment and transportation in 2009. Responding to the crisis, an official at the Department of National Defence asked Veterans Affairs Canada for help.

Veterans Affairs is responsible for disability pension payments, while National Defence provides health benefits to Canadian Forces members.

A Veterans Affairs employee responded with an email containing medical details and also the exact percentage of the disability pension awarded the veteran.

The Forces member complained to our Office that the disability pension percentage was disclosed to National Defence without his consent and contrary to the formal arrangements for sharing personal information between the two departments.

The same individual had made a similar complaint in 2008 about the sharing of the disability pension percentage with National Defence. That complaint had been concluded as well founded.

An investigation by our Office established that an agreement between the two departments limits the sharing of personal information about disability pensions to five specific pieces of information, not including the percentage which indicates the severity of the affliction.

We also found no evidence that the disclosure of the complainant's disability pension percentage was in any way useful or necessary to facilitate his treatment.

Veterans Affairs submitted that its disclosure was made under the "public interest" provisions of the *Privacy Act* (subsections 8(2)(*m*)(i) and 8(2)(*m*)(ii)).

However, our investigation found no evidence that the disclosure of the complainant's disability pension percentage was done deliberately, as would have been expected to warrant claiming the "public interest" exemption.

Instead, the disclosure apparently occurred because an email chain among Veterans Affairs officials was forwarded to a Department of National Defence official without deleting sensitive personal information that National Defence had no apparent need to know.

We upheld the complaint as **well founded**.

We recommended that Veterans Affairs review and comply with its own existing policies and procedures concerning the sharing of personal information with the Department of National Defence. We also recommended that Veterans Affairs disseminate

those policies and procedures to its employees and provide training about appropriate practices for handling information with the Department of National Defence.

Both recommendations were accepted and implemented. As well, Veterans Affairs Canada re-examined its arrangement with National Defence concerning the disclosure of personal information.

This incident occurred in 2009, prior to the launch of Veterans Affairs Canada's 10-point action plan to address privacy concerns.

CORRECTIONAL SERVICE OF CANADA INVESTIGATIONS

For the 10th consecutive year, the Correctional Service of Canada accounted for the largest number of complaints received by our Office – and again for the 10th consecutive year, by a wide margin over the second-place institution.

In 2011-2012, we accepted 326 complaints against the Correctional Service of Canada, an increase of 18 percent from last year's 276 complaints received.

Since our first Annual Report in 1983-1984, we have investigated over 11,000 complaints against the Correctional Service of Canada.

Some key drivers for this persistently high number of complaints seem obvious. Incarcerated in the country's 57 federal penitentiaries are more than 13,000 offenders overseen by more than 7,000 correctional officers. In a prison environment, information is currency.

However, the picture is not quite as bleak as the total figures might suggest.

Time limit cases (127) accounted for more than a third of the total complaints accepted, yet this was 32 fewer than the previous fiscal year. This suggests that the Correctional Service of Canada is succeeding in reducing the sources of delays within their system for processing *Privacy Act* requests.

Approximately one-quarter of time limit complaints were resolved through our early resolution process.

Early resolution also succeeded in more than one-third of the complaints about gaining access to personal information and almost 40 percent of the complaints about privacy, predominately the use and disclosure of personal information.

Overall, 106 of the total 326 complaints were handled by early resolution, compared to only 19 in the previous fiscal year.

The 33 remaining privacy complaints, however, represented a 175 percent increase from the 12 which were not completed through early resolution in 2010-2011.

However, that number was greatly inflated because of 16 complaints over the same issue at one institution; and a further eight complaints at another penitentiary. In both cases, investigations are continuing.

The following two cases reflect the variety and complexity of Correctional Service of Canada complaints:

Drug Scan, Child Access Linked in Inappropriate Disclosure

This case involves a complaint from a woman who tested positive for traces of an illicit drug during ion scans carried out when she visited an inmate in a federal penitentiary.

The woman's ex-husband was a Correctional Service of Canada employee. His lawyer informed the woman that – in light of several positive drug tests – her ex-husband would no longer allow access to their children "due to his concerns over their safety and well-being."

The woman complained to the acting warden about the apparent inappropriate disclosure of her personal information. Several months later, the inmate she had visited was informed by the acting warden that two Correctional Service of Canada employees had inappropriately accessed his personal information in key databanks.

The woman and the inmate believed that the ex-husband had obtained the drug scan information through this inappropriate access.

Correctional Service of Canada officials determined that the ex-husband had not taken part in the database intrusion, nor was there any evidence that the culpable employees had passed information to him. However, the Department didn't try to discover how the ex-husband had learned of the drug incidents.

Our investigation determined that the existence of drug traces on the woman had indeed been disclosed to her ex-husband by other Correctional Service of Canada employees. We were unable to discover who had disclosed that personal information, or where the information came from.

We upheld the complaint as **well founded** and also concluded that the Correctional Service of Canada had failed to adequately deal with the core disclosure issue.

Inmate Medical Details Openly Displayed

An inmate at a federal penitentiary complained that the Correctional Service of Canada had contravened the *Privacy Act* by openly posting details of medical appointments at the institution. He said his name, appointment time and partial standard offender

number had been disclosed at least three times to the general penitentiary population.

The inmate also said that names, medical appointment times, complete offender numbers and other medical information were similarly disclosed for other inmates on several occasions.

The Correctional Service of Canada acknowledged that the *Privacy Act* had been breached by the postings and said it would notify each inmate of medical appointments rather than post a list.

However, penitentiary officials did not accept our recommendation that only partial offender numbers be used on the lists which employees use for the individual notification.

We upheld the complaint as **well founded**.

CANADA REVENUE AGENCY INVESTIGATIONS

Only once in the last 10 years has the Canada Revenue Agency not featured in the Top Five list of institutions about which our Office has received complaints under the *Privacy Act*.

Since our first Annual Report in 1983-1984, we have investigated approximately 4,000 such complaints against the agency.

And, again, the reasons for the consistently high number of complaints are not difficult to imagine.

Most people will reveal a lot of other personal information more readily than they will lay bare their finances. If individuals have even the slightest inkling that the Canada Revenue Agency has not been scrupulous in handling data about what they earn, what deductions they claim and what level of tax they pay, they are likely to raise a red flag.

The 65 complaints accepted during 2011-2012 constituted a 23 percent increase from the 53 of a year earlier. However, 15 of the complaints in this fiscal year were handled quickly through early resolution, in contrast to only one in 2010-2011. Half of those early resolutions came in the privacy category, which meant that formal complaint investigations in that crucial category rose only slightly, from seven in the previous fiscal year to 11 in the current reporting period.

In recent years, our Office has identified several ongoing privacy risks at the Canada Revenue Agency relating to inadequate controls surrounding employee access to taxpayers' electronic information. These risks, which relate directly to a series of reported privacy complaints, have prompted our Office to launch an audit of the Agency. The audit will be conducted in the 2012-2013 fiscal year.

The investigations summarized below as well as a breach incident at the Canada Revenue Agency described on page 50 illustrate some of the concerns we have identified.

A Year to Confirm Ex-Husband Got Former Wife's Tax Information

Through an access to information request to the Canada Revenue Agency, a woman learned that her tax information had been accessed by a Canada Revenue Agency employee who is the common-law spouse of her ex-husband. The ex-husband then used that information to seek an amendment to a child support arrangement.

The woman lodged a *Privacy Act* complaint with the Canada Revenue Agency. An investigation by the Agency confirmed the complainant's tax information had been inappropriately accessed by an employee, who passed the information along to the ex-husband.

The Canada Revenue Agency investigation took 13 months. A letter informing the complainant of the results of the internal investigation was drafted, but never sent. The lengthy delay prompted the woman to make a complaint to our Office.

Our investigation concluded that the Canada Revenue Agency has a rigorous and comprehensive discipline policy to address employee misconduct. But for such policies to be effective, allegations of employee misconduct must be addressed more quickly and efficiently.

We also highlighted the need for enhanced privacy training and to ensure that employees with access to personal tax information are fully informed of their obligations in terms of protecting the privacy of Canadian taxpayers.

We upheld the complaint as **well founded**. Our recommendation was accepted and implemented.

Canada Revenue Agency gave personal information to a third party without consent

A woman applying for an adjustment had not updated her family name in the Canada Revenue Agency's system. An Agency employee conducted a search in order to find the applicant in the system to follow up on her request for an adjustment. The employee failed to verify whether the address matched the information appearing on the request and on the supporting documents. As a result, the woman's niece received a letter addressed to her containing her own Social Insurance Number, but with information concerning the complainant. The complainant and her husband's niece both have the same family name and first name, although the spelling of the given name is slightly different.

Our Office found that this was the result of a human error because the procedure in place had not been followed to the letter. The complaint was **well founded**.

Following this incident, the Agency admitted its error and put in place measures to prevent this type of incident from recurring in the future.

TIME DELAYS – ACCESSING PERSONAL INFORMATION

Too many federal government departments and agencies are consistently slow in dealing with requests from Canadians to access their personal information.

Year after year, our Office has investigated departments for complaints about flouting *Privacy Act* provisions mandating substantive answers within a maximum time limit of two months.

From 19 institutions in 2010-2011, the number of tardy departments and agencies climbed to 27 in this reporting period. Indeed, for the first time ever, the total number of time delay complaints exceeded 300.

Some time limit cases are truly alarming, including four that were finally closed in the past fiscal year after delays of 24 months (both Public Works and Government Services Canada and Canada Border Services Agency); 19 months (Correctional Service of Canada) and 17 months (Department of Justice).

In two cases involving the Correctional Service of Canada, so much time elapsed after access requests were filed that we initiated an application before the Federal Court. Shortly after the application was filed, the Correctional Service of Canada provided a satisfactory response to the two individuals and we discontinued both matters. (See Chapter 4 – Judicial Proceedings for further details.)

As a result of our long-standing concerns about this issue, the Assistant Privacy Commissioner informed 23 departments that, starting in September 2011, a new clock would be ticking.

We will put departments on notice when we accept a time delay complaint. Within a maximum of four months, they must provide a commitment date or a work plan for the production of the requested personal information.

If they don't, our Office may issue a formal finding that the institution has been deemed to have refused to give access, otherwise known as "deemed denial."

That clears the way for the individual or the Privacy Commissioner herself to refer the matter to the Federal Court for review.

Not only is justice delayed, justice denied; so too is delay in access to personal information.

DATA BREACH REPORTS

In the past fiscal year, the number of data breaches reported to us by federal institutions reached 80, the highest number in recent years, and a 25 percent increase over the previous year.

Any loss or unauthorized disclosure of personal information constitutes a data breach. In some cases, the affected individuals didn't know about the breach; in other cases people were notified about the breach or found out somehow. Some filed complaints with our Office.

FEDERAL PUBLIC SECTOR DATA BREACHES REPORTED TO THE OPC

2007-2008	44
2008-2009	26
2009-2010	38
2010-2011	64
2011-2012	80

Given that the reporting of data breaches is voluntary, it is impossible to say categorically whether the current increase reflects more diligent reporting or an actual increase in breaches.

The federal government has guidelines encouraging federal government institutions to report all significant data breaches to our Office in a timely fashion.

Breach Reporting Guidelines

The Treasury Board Secretariat strongly recommends that institutions notify our Office of any data breach that:

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

Notification of the breach and any mitigating measures should occur as soon as possible after the institution becomes aware of the breach, preferably within days.

The guidelines acknowledge that there "may be some very minor incidents" that institutions may choose to manage internally with the individuals concerned, without notifying our Office.

On the basis of the two most recent fiscal years, Human Resources and Skills Development Canada appears to be exercising considerable diligence in notifying our Office.

The Department reported 19 data breaches for 2011-2012, almost one-quarter of the total flagged to our Office. In 2010-2011, it accounted for one-third of all breaches reported. However, we were encouraged by the Department's diligence in responding to breaches.

Of the 80 data breach notifications we received, four involved the theft of information, including corporate and personal tax documents taken in a break-in of the car of a Canada Revenue Agency employee. Nine other breaches were blamed on the loss of documents, including two passports at Canadian embassies abroad.

Thirteen breaches arose from unauthorized access to personal information or, in one case, the unauthorized sharing of documents.

Once again, the largest category of data breaches – and the one proving most resistant to eradication – was accidental disclosure, with 54 breaches predominately caused by human error.

These two data breaches stood out:

ATIP Officials Weren't Advised of Incident Involving Taxpayer Data

At the request of an employee involved in a labour dispute, the Canada Revenue Agency provided her in March 2006 with 16 CDs that contained copies of all the files on the "home", or H drive, of her office computer. The employee believed the files included an email which would be of benefit in the dispute. She locked the CDs in a secure cabinet at home.

At the labour hearing in September 2008, the Canada Revenue Agency learned that the CDs contained not only the employee's personal files, but also Agency information – 76 documents with more than 42,000 instances of taxpayer information, including names, Social Insurance Numbers, addresses and financial data.

The contents of all but two of the CDs had been copied to a work laptop computer of the employee's boyfriend in order to search for the email. During a Canada Revenue Agency investigation, the boyfriend said he deleted all the copied information.

When the incident was discovered, the Agency conducted a security review and determined that no taxpayer information was improperly disclosed. Therefore, the Agency's officials responsible for privacy were not notified of the incident.

The Canada Revenue Agency has now taken steps to ensure that in any case where personal information is compromised the Access to Information and Privacy officials will be notified. It will then be their responsibility to notify our Office.

"Phishing" Shuts Down Federal Job Bank for Two Weeks

Job Bank is a free employment service provided to Canadian employers and job-seekers by Human Resources and Skills Development Canada.

In early February 2012, Job Bank officials detected a limited but serious security issue and shut the site down to make important security upgrades.

A third party had posed as a legitimate employer and posted fake job ads in order to obtain the banking information of job applicants, an electronic masquerading known as "phishing."

Five employer accounts were affected out of more than 135,000 in the system. In each instance, Job Bank promptly removed the job ads and notified affected employers, our Office and the Canada Revenue Agency.

Job Bank reopened after a two-week shutdown with new security features comprising a new login system and more comprehensive monitoring procedures for employers. For job-seekers, Job Bank has added warnings on the website about potential phishing schemes, including information about the actual incident.

In addition, job-seekers are asked to contact Job Bank immediately if they encounter a questionable job ad or an employer seeking personal or banking information. Job-seekers and employers are also directed to contact local police or the Canadian Anti-Fraud Centre if they believe they have been a victim of phishing.

Job Bank was working with IT experts to let job-seekers create strong passwords to protect their accounts, while also mitigating the risk of their accounts being compromised. This is part of a second stage of security enhancements added and was scheduled to be implemented in the summer of 2012.

CHAPTER 4

The OPC in Action -

STRENGTHENING THE PRIVACY RIGHTS OF CANADIANS

Any dispute between citizens and the state is, by definition, a lopsided battle. For starters, citizens usually have to figure out what particular arm of the multi-limbed federal government they should be dealing with.

When it comes to privacy issues, the place where individuals can seek assistance is the Office of the Privacy Commissioner of Canada.

OUR "FRONT OFFICE" WORK

INFORMATION REQUESTS

Over the past couple of years we have implemented major changes to our Offices in order to better serve Canadians. We have created an Information Centre in order to engage Canadians and provide them with useful information as quickly as possible, which, in some cases can be effective in resolving issues immediately without resorting to our formal complaints process.

Our Information Centre responds to requests for information from the public and organizations regarding privacy rights and responsibilities. In 2011-2012, we received over 9,000 such requests.

Just over half of those calls related to private sector issues.

Less than 15 percent of information requests were linked to the *Privacy Act*. Those requests related to a huge variety of issues, but some of the more common questions related to how individuals can access their personal information held by government departments; how our Office's complaint process operates; and about whether certain information must be disclosed to federal departments and agencies.

A significant number of the requests we received (roughly one third) related to privacy problems over which we do not have jurisdiction. In those cases,

we offer assistance by referring individuals to other organizations or by suggesting strategies for resolving issues or tracking down information.

INTAKE

As part of our efforts to improve front-end service, in 2011-2012 we created a dedicated Intake Unit to analyze, triage and register complaints to our Office.

All written complaints about privacy matters are forwarded to this Unit.

The Intake Unit reviews the complaint, and, if necessary, follows up with the complainant to clarify our understanding of the complaint and to gather any additional information necessary to begin an investigation.

Our Intake team has been increasingly successful with its efforts to satisfactorily address some issues immediately, eliminating the need for a potential complainant to submit a complaint to our Office.

EARLY RESOLUTION

Early resolution can address some complaints more efficiently by relying on negotiation and conciliation.

It often involves sharing information with both sides to clear up a simple misunderstanding. For example, complainants may not know about exemptions that the department withholding personal information is permitted to apply under the *Privacy Act*. Once they

Examples of Early Resolution Cases in 2011-2012

Transport Canada
When a man registered a sailboat with Transport Canada, he was assured the information was confidential. Two years later, he received a form from the Ontario government asking about the boat's purchase price and date of purchase in order to assess taxes. He complained that this was a breach of his right to privacy.

However, the Transport Canada licence registration form includes a printed disclaimer that the information may be disclosed in certain specific circumstances, including to an agency enforcing "the requirement to pay provincial sales tax."

Given this information, the complainant agreed the file could be closed.

RCMP
After being charged under the *Motor Vehicle Act*, the complainant requested all information pertaining to his charge, including notes of the charging constable, audio recordings of communication between that officer and the RCMP detachment, as well as the officer's vehicle camera film of the incident.

The RCMP responded to the complainant's request by stating that the requested information was exempted under section 22(1)(*a*)(ii) of the *Privacy Act* and would not be released. Under that section, the RCMP does not have to show that releasing information could cause harm, as with some other exemptions in the *Privacy Act*.

Since the RCMP demonstrated that it had met the criteria for this exempting provision, there was little our Office could do to pressure the organization to release the requested information.

It should be noted, however, that once a criminal investigation has been through the court system, the RCMP will often release such information, providing it does not reveal investigative techniques or the personal information of other individuals.

understand the law, some complainants are satisfied and the matter is considered resolved.

Similarly, potential complainants will usually accept that proceeding with a formal investigation would lead to a finding of not well founded when we explain that departments were found to have complied with the Act in previous investigations involving similar issues.

When it succeeds, early resolution is the best possible outcome for both sides.

Individuals get the answers they were seeking quickly. The government institution avoids a drawn-out process.

The success of early resolution has been growing steadily over the last several years.

In the past fiscal year, we closed more than one fifth of all complaints received through early resolution. The number of early resolution successes was almost three times more than the previous year (213 in 2011-2012, compared to 78 in 2010-2011.)

COMPLAINTS

After six consecutive years of declining numbers of complaints, 2011-2012 saw a 39 percent increase over the previous fiscal year, with the total of 986 complaints accepted – almost back to the record level of 2005-2006.

There are 10 different reasons why an individual might lodge a complaint under the *Privacy Act* and they fall into three distinct categories – Access, Privacy and Time Limits. These categories are described in Appendix 1.

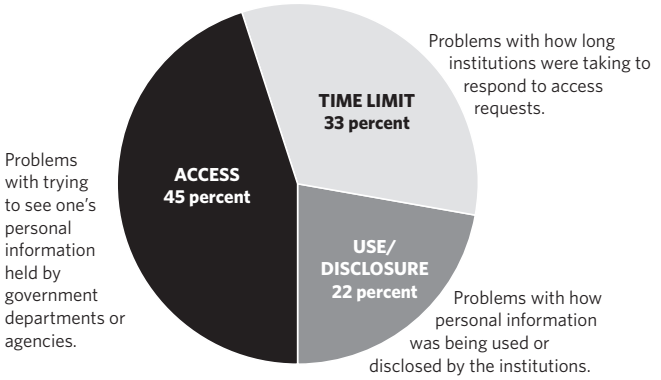
We saw a rise in all three of the categories, however, the jump in denial of access complaints was particularly strong.

This increase is likely a result of more Canadians exercising their right to access their personal information. We believe that greater media attention to privacy issues has enhanced awareness of access rights.

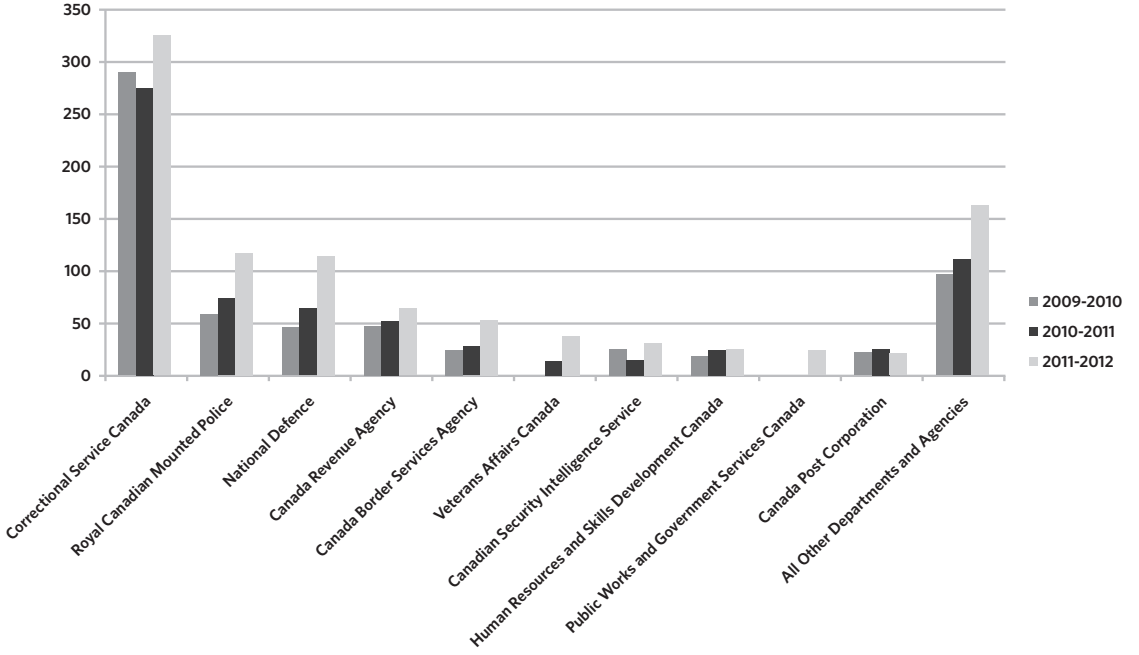
In turn, the increased number of requests for access has led to increased processing delays and therefore a rise in complaints to our Office about timeliness.

A number of federal institutions have experienced an increase in access requests, however, the resources to handle those requests have remained the same or have decreased.

COMPLAINTS ACCEPTED BY CATEGORY



TOP 10 INSTITUTIONS BY COMPLAINTS RECEIVED IN 2011-2012 (Three-year history)



Nearly 60 percent of the increase in complaints to our Office originated with just four institutions: the Correctional Service of Canada (50 complaints more); National Defence (50 more); RCMP (42 more); and Veterans Affairs Canada (24 more).

Throughout the past decade, the Correctional Service of Canada, National Defence and the RCMP have repeatedly appeared among the Top Five list of complaints to our Office.

Chapter 3 includes an analysis of complaints to the Correctional Service of Canada and Veterans Affairs Canada.

Here are some observations on the other two institutions.

DEPARTMENT OF NATIONAL DEFENCE

The 115 complaints accepted about the Department of National Defence in this fiscal year amounted to a nearly 80 percent rise from the 65 complaints in the previous period.

The overwhelming bulk of that increase came in the form of time limit complaints, which quadrupled from 19 to 76.

In most cases, such significant jumps reflect a mismatch between the increasing volume of requests and the resources made available to deal with them. Complaints to our Office about access actually dropped for National Defence, and most of those that could not be resolved through the early resolution process concerned denial of access complaints from departmental employees or Canadian Forces members.

RCMP

Time limit problems also drove up the total complaints accepted about the RCMP, with that category increasing by a factor of three. Complaints about use and disclosure of personal information similarly burgeoned, leading to an overall rise from 75 complaints received in 2010-2011 to 117 in 2011-2012.

Worth noting, however, is that 13 of the 32 complaints in the use and disclosure category were handled through early resolution.

The following is an example of one of the use and disclosure complaints against the RCMP that we investigated.

RCMP Names Murder Suspect at Community Meeting

The head of a community group invited an RCMP staff sergeant to discuss a decade-old murder case at a meeting and to specifically address why the name of a member of the community kept coming up in talk about the murder.

The sergeant said he would discuss that particular man only if he were present. The head of the group assured him this would not be a problem. The talked-about man had been

present at a recent group meeting, where it had been agreed to invite the RCMP to discuss the cold case investigation.

The sergeant had no contact with the man until both attended the meeting. During a discussion about the cold case, the sergeant said the man was a "person of interest" and had declined to submit to a polygraph test.

The man commented that he had Charter rights. Another member attacked him for not co-operating.

The man complained to our Office that the RCMP sergeant inappropriately disclosed the fact he was a suspect in the murder investigation at the meeting. He said he had been advised that he would be discussed at the meeting, but had not been advised of the subject matter.

The evidence indicates that the sergeant presumed that the complainant had consented to the discussion, because of the complainant's attendance at the meeting and assurances from representatives of the group that the complainant was aware of, and had not objected to, the proposed discussion.

While it is commendable that the sergeant was being responsive to the interests of the community, the onus was on the RCMP to actively obtain consent, rather than presuming it. The onus was *not* on the complainant to object to a disclosure of his personal information. We upheld the complaint as **well founded**.

OTHER INVESTIGATIONS OF INTEREST

While Chapter 3 presented examples of cases from three institutions, other federal departments and agencies also generated investigations of interest.

The following is a snapshot of some of the other investigations completed in 2011-2012.

Mystery of How Newspaper Identified Boat Refugee

On October 17, 2009, a ship called the *Ocean Lady* arrived at Victoria, B.C. carrying 76 refugee passengers. Five days later, a news story in the *National Post* reported that one of the passengers was a 26-year-old fugitive sought by the International Criminal Police Organization (INTERPOL) on a terrorism offence.

On behalf of a non-profit organization, a complainant alleged that personal information about that refugee had been disclosed to a *Post* reporter. She named four federal institutions as potentially culpable – the Canada Border Services Agency, the Canadian Security Intelligence Service, Citizenship and Immigration Canada and the Royal Canadian Mounted Police.

Our investigation confirmed that the individual in question was a wanted fugitive on INTERPOL's website. The publicly available INTERPOL notice included the individual's full name, sex, date of birth, place of birth, nationality and language spoken, the colour of his eyes and hair, and his photo.

Because of journalistic confidentiality, our investigation was unable to confirm how the *National Post* reporter obtained the information for the article.

In the absence of this information, there was no factual evidence to support the allegation that any of the four institutions named in the complaint disclosed personal information about the passenger to the reporter.

Accordingly, we found the complaint was **not well founded**.

However, our Office took the opportunity to remind each department that the personal information of refugees and refugee claimants may have greater than usual sensitivity, considering the potential for harm to the safety and security of individuals seeking protection under Canada's refugee program.

Canada Post Sharing Personal Information with Credit Bureau

Protecting against identity theft has complicated what was once a relatively simple matter – changing your mailing address with the post office – especially when Canadians want the convenience of doing this online.

The online process takes seven steps, and a man complained that the final stage consisted of Canada Post checking his credit rating.

Our investigation established that Canada Post has a legitimate need to confirm the identity of individuals requesting a change of address. Misdirection of personal mail is a common tactic in identity theft.

To verify identity in online requests, Canada Post has contracted with Equifax, best known as a credit-rating agency.
Personal information provided online to Canada Post by a requestor is sent electronically to Equifax.

The online requestor is also transferred seamlessly to Equifax's identity verification website and asked questions about outstanding loans and other financial dealings listed with the credit-rating agency.

If the individual correctly answers these "out-of-wallet" questions, Equifax advises Canada Post that their identity has been successfully verified. Canada Post then processes the payment for the change-of-address transaction and the individual's address change will be activated. Equifax assured us that any information provided by the individual during this identity verification process will be kept entirely separate from the information it collects and maintains in the individual's credit file for credit reporting purposes.

As a result of our investigation, we were satisfied that Canada Post has the statutory authority to collect the personal information used in this online process. Further, we were satisfied that Canada Post does not conduct a credit verification of individuals wishing to change their address online. Consequently, there has been no violation of the *Privacy Act* in that regard. We found the complaint was **not well founded**.

Nevertheless, our Office was concerned that individuals were not adequately informed that their personal information was being shared with Equifax. Therefore, we recommended that Canada Post clearly state on its website that an individual's personal information will be disclosed to Equifax and also that it list the personal information that will or may be disclosed. As well, we recommended that Canada Post clarify its identification requirements for online applications. Canada Post implemented our recommendations.

Mix-up by Immigration Officials Discloses Personal Information

A Canadian woman wanted to hire a Bangladeshi man as a live-in caregiver for her child. The man applied for a work permit at the Canadian High Commission in Dhaka and supplied all the necessary documents.

To strengthen the man's application, the woman asked her MP to send a letter of support to the High Commission. She also asked the MP to attach to his letter copies of personal documents such as her passport and federal income tax assessment, which included her date of birth, Social Insurance Number and other personal information.

The MP's office forwarded all this information to officials of Citizenship and Immigration Canada at the Canadian High Commission in Dhaka.

The man's application for a work permit was refused. Following standard practice, the Immigration official returned to the man the entire contents of his file, which included not only his documents, but also the woman's personal documents sent by the MP's office.

According to the woman, the man then shared her personal information with family and friends. She was concerned that this disclosure could result in identity theft or jeopardize her safety if she travelled to Bangladesh. She complained to our Office.

Citizenship and Immigration acknowledged that it did not have the complainant's consent and that her personal information should not have been disclosed to the man. At our request, officials apologized to the complainant in a letter.

We upheld the complaint as **well founded**.

This is not the first time a breach of this nature has occurred at a Canadian High Commission.

We recommended that all High Commissions create a stamp that says "Destroy/Do Not Return to Applicant" to distinguish documents from sources other than a visa applicant. The Dhaka mission has already done so.

INVESTIGATIONS AND DISPOSITIONS – BY THE NUMBERS

Elsewhere in this report, we have devoted a considerable amount of words to describing complaint investigations. Here we concentrate on the numbers big picture. Readers who want detailed statistics can also consult the tables in Appendix 3.

Our Office accepted and closed almost the same number of complaints in 2011-2012 – 986 in the "in tray," 913 in the "out tray."

The 913 complaints concluded represent a 60 percent increase from the 570 concluded in the previous reporting period. This includes 213 complaints closed through the use of early resolution, nearly a quarter of the total.

As discussed earlier in this report, our Office has put a greater emphasis on the use of early resolution techniques in recent years.

Three-quarters of our not well founded cases involved access issues. In general, these are cases where individuals had challenged an institution's refusal to provide access to their personal information. However, we found that appropriate exemptions had been applied.

The number of well founded cases we see in the public sector is significantly higher than in the private sector. The vast majority (88 percent) of the well-founded cases under the *Privacy Act* in 2011-2012 involved time limits complaints – cases where an institution failed to respond to access requests within legislative timeframes.

DISPOSITIONS*	# of Cases	Percentage
Not well founded	248	27 %
Well founded	247	27 %
Early resolution	213	23 %
Discontinued	96	11 %
Settled	63	7 %
Well founded resolved	32	4 %
Resolved	14	2 %
TOTAL	**913**	

* Definitions of dispositions are provided in Appendix 1. For a more detailed breakdown, please see the table Disposition by Complaint Type in Appendix 3.

The average treatment time to complete exclusively formal investigations dropped slightly from 8.0 months in 2010-2011 to 7.6 months.

Our refining of the early resolution approach has produced a steady decline in the average time to complete cases overall. Our combined treatment times for both formal investigations and early resolution categories have dropped as follows; 19.5 months in 2008-2009, 12.9 months in 2009-2010, 7.2 months in 2010-2011 and 5.8 months this past fiscal year.

It should also be noted that, previously, our Office calculated treatment times from the date complaints were received, even though some lacked essential information and required clarification before work could start.

Starting in 2011, complaints are considered "accepted" only after the contents are complete. We feel that the changed definition allows for a more accurate picture of treatment times.

This means that the complaint numbers compared between the current fiscal year and previous years weren't compiled on exactly the same basis.

For percentage changes, this makes little significant difference. For comparative purposes, if this year's treatment times were calculated the same way as last year, our average treatment time in 2011-2012 would have been 6.2 months, down from 7.2 months in 2010-2011.

The Top 10 Institutions accounted for 84 percent of all complaints accepted during 2011-2012, a proportion virtually unchanged from the previous two fiscal years.

However, the departments that made the Top 10 list did change compared to a year earlier:

- Canadian Security Intelligence Service jumped to 7th place from 9th.
- Canada Post dropped from 6th place to 10th place.
- Veterans Affairs Canada rose to 6th place.
- Public Works and Government Services Canada is new on this year's list, in the 9th spot.
- Citizenship and Immigration Canada dropped off the list this year, compared to its 8th position in 2010-2011.

TOP 10 INSTITUTIONS BY COMPLAINTS ACCEPTED IN 2011-2012

Institution	2011-2012
Correctional Service of Canada	**326**
Royal Canadian Mounted Police	**117**
National Defence	**115**
Canada Revenue Agency	**65**
Canada Border Services Agency	**55**
Veterans Affairs Canada	**39**
Canadian Security Intelligence Service	**32**
Human Resources and Skills Development Canada	**26**
Public Works and Government Services Canada	**25**
Canada Post Corporation	**22**
All other departments and agencies	**164**

REACHING OUT TO FEDERAL INSTITUTIONS

Outreach to federal institutions is an important component of our public sector work. Each year, we discuss issues related to the protection of personal information with as many as possible of the 250 federal institutions that fall under the authority of the *Privacy Act*.

Help with Privacy Impact Assessments

More than 100 privacy and data protection officials from 38 different federal institutions attended the third annual Privacy Impact Assessment (PIA) workshop in January, which we co-hosted with the Treasury Board Secretariat.

Officials from the Treasury Board Secretariat and our Office explained our roles in relation to Privacy Impact Assessments and the Directive on Privacy Impact Assessment. We also outlined our respective expectations about PIA content.

In addition, our Office presented an assessment by our Technology Analysis Branch of the leading security risks that could result in privacy breaches for government institutions, and discussed how PIAs can be used to effectively gauge and manage these risks.

Our Office has been pleased by the number of federal managers and employees who wish to attend presentations to hear our guidance on preparing PIAs. Our Expectations document, which provides extensive advice on preparing PIAs, has also proved to be very popular.

As a result, we have produced a short video to be added to our website in the next fiscal year so that anyone interested in hearing our advice can view the video at any time.

Expectations: A Guide for Submitting Privacy Impact Assessments to the Office of the Privacy Commissioner of Canada

ATIP Outreach

Our Office, along with the Office of the Information Commissioner of Canada, organized an event for federal Access to Information and Privacy professionals – an "ATIP Community Breakfast" – in June 2011.

The event, attended by over 100 ATIP professionals from various departments, supported our efforts to better understand the challenges and emerging privacy issues that federal departments and agencies face. It also offered the opportunity for the ATIP community to come together to share experiences and exchange ideas and to meet with both the Privacy Commissioner and the Assistant Privacy Commissioner.

We believe the event helped us to continue to strengthen our relationship with the ATIP community and to improve the services we deliver jointly to Canadians.

As part of an ongoing effort to modernize our *Privacy Act* investigation process, at the time of writing this report we were meeting with a number of ATIP offices to present them with our modernization priorities and listen to their thoughts on how we could make our processes more efficient. Our primary aim is to streamline our investigative process and resolve complaints more quickly.

Speeches and Presentations

The Commissioner, Assistant Commissioner and other officials from our Office made a number of speeches on public sector issues throughout the year. For example, the Commissioner presented at a special data privacy event at Canada Post and we also spoke at events for public servants organized by the Canada Border Services Agency, the Immigration and Refugee Board of Canada and the Treasury Board. As well, we took part in conferences such as the APEX Symposium and the National Human Rights Conference organized by the national association of federal, provincial and territorial human rights agencies. In October 2011, we also co-sponsored an international conference with the Université de Montréal on integrating privacy into public safety measures. Both the Commissioner and Assistant Commissioner participated. The Commissioner chaired a panel on cyber surveillance and cyber terrorism and the Assistant Commissioner gave a presentation on the Canadian experience of integrating privacy into public safety measures.

A Matter of Trust: Integrating Privacy and Public Safety in the 21st Century

Data Privacy Day 2012

On January 28, 2012, Canada, along with many countries around the world, celebrated Data Privacy Day. Recognized by privacy professionals, corporations, government officials, academics and students around the world, Data Privacy Day highlights the impact that technology is having on our privacy rights and underlines the importance of valuing and protecting personal information.

Our Office used this occasion to highlight the importance of privacy and to heighten awareness about various privacy issues in both the private and public sectors.

In the public sector, we sent all federal Access to Information and Privacy coordinators an email that included information about Data Privacy Day, our planned activities and links to our online resources, which included web graphics and printable posters.

We also shared our Data Privacy Day materials with the federal Security Training, Education and Awareness Working Group, and a number of other interested government departments, including Canada Revenue Agency, Human Resources and Skills Development Canada, Health Canada and Public Safety Canada.

During the week of Data Privacy Day, we hosted a Canada School of Public Service Armchair Discussion about Privacy Impact Assessments and

the importance of privacy awareness in the public service.

2012 Privacy Calendar

This year, our Office once again produced and distributed a privacy calendar featuring cartoons illustrating key privacy issues, as well as useful tips and links to related information. As part of our outreach work with the public sector, we sent the 2012 privacy calendar to all federal Access to Information and Privacy coordinators.

Human Resources Tips

Employee information – be it in either the public sector or the private sector – is often highly sensitive and needs to be handled with care. In 2011-2012, we developed a tip sheet, *Ten things HR professionals need to know about privacy,* in order to help organizations ensure that all employees' information is treated with integrity and professionalism.

Ten things HR professionals need to know about privacy

ACTION BEFORE THE COURTS

The Privacy Commissioner may be involved in a review before the Federal Court pursuant to section 42 of the *Privacy Act*, by applying to appear before the Federal Court in cases where a federal institution has denied an individual access to his or her personal information. As well, the Commissioner may occasionally be the subject of an application for judicial review.

Our Office may also seek to become involved as an intervener in other matters before the courts or other tribunals. We may seek leave to intervene in order to clarify issues around the interpretation of particular provisions of the *Privacy Act*, or in order to offer a court or tribunal our perspective on other legal issues involving privacy and/or the protection of personal information (for example, the extent of the application of the open courts principle to administrative tribunals.)

Here are summaries of cases in which we were involved during 2011-2012.

In keeping with the spirit of our mandate, we do not publish the names of plaintiffs. The file numbers of the proceedings and the names of respondent institutions are, however, provided.

Privacy Commissioner of Canada v. *Correctional Services Canada*
Court File No. T-1218-11 (FC) and T-1219-11 (FC)

Two individuals filed access requests to the Correctional Service of Canada and both received letters back requesting a 30-day extension to the original 30-day deadline to provide access. However, neither individual received access after this time period had elapsed; each subsequently filed a complaint with our Office.

In both cases, we contacted the Correctional Service of Canada to request the documents and to attempt to establish a work plan so the agency could deliver them in a timely fashion. The Correctional Service of Canada did not comply with either of these requests.

Given the time that had elapsed since the complainants filed their respective access requests, the Assistant Commissioner deemed that access had been denied under the Act, and determined that both complaints were well founded.

On July 22, 2011, the Commissioner initiated an application before the Federal Court under subsection 42(*a*) of the *Privacy Act* regarding the Correctional Service of Canada's refusal to disclose the personal information requested by the two individuals.

Shortly after the application was filed, the Correctional Service of Canada provided a satisfactory response to the complainants with respect to their access requests, and the Commissioner discontinued both matters.

These cases coincided with our Office's issuance of guidance to federal institutions regarding deemed denials of access under the Act, given that a substantial majority of the complaints we receive come from individuals alleging that a federal institution unjustly denied them timely access to their personal information.

X. v. *Hon. Peter Gordon Mackay et al. and Privacy Commissioner of Canada and Attorney General of Canada*
Court File No. A-274-11 (FCA)

In 2006 and 2007, an individual made three separate access complaints against the Department of National Defence, Citizenship and Immigration Canada and the Canadian Security Intelligence Service.

Our Office found the complaints to be not well founded as we were satisfied that the responses and exemptions applied by each of the respondent government institutions under the *Privacy Act* were appropriate.

The individual brought an application under section 41 of the *Privacy Act*. The application was subsequently dismissed by the Federal Court and the applicant appealed to the Federal Court of Appeal. Our Office was erroneously named as a Respondent to the appeal procedure by the applicant. We filed a motion and were granted an order to have the Commissioner removed as a named Respondent in this appeal on September 2, 2011.

X. v. *The Privacy Commissioner of Canada & Minister of Public Works and Government Services Canada*
Court File No. T-425-12 (FC)

A former candidate for a position within the public service was in the process of filing a grievance for alleged improprieties during the course of the employment competition process.

To this end, she sought access to her personal information held by the Department of Public Works and Government Services Canada. She subsequently filed a complaint with our Office, alleging that the access was incomplete. Our investigation did not reveal any evidence that documents had been inappropriately withheld from the disclosure package, and found the matter to be not well founded.

On February 24, 2012, the complainant, as a self-represented litigant, filed an application for a *de novo* hearing under section 41 of the *Privacy Act*. She was seeking access to personal information allegedly withheld by Public Works and Government Services Canada.

However, she listed the Privacy Commissioner of Canada in addition to the Minister of Public Works and Government Services Canada, as respondents. Given that the application was filed under section 41 of the *Privacy Act*, that it concerned the Department's alleged refusal to provide the complainant access to her personal information, and that the relief sought by the complainant was exclusively against the Department, our Office filed a motion seeking to remove the Commissioner as a named respondent.

On April 19, 2012, the Court released its decision and ordered that our Office be removed as a respondent to the Application and that the style of cause be amended accordingly.

X. v. *Privacy Commissioner of Canada*
Court File No. T-555-10 (FC), 11-A-14 (FCA) and A-451-11 (FCA)

We reported on this matter in last year's Annual Report. This was an application for judicial review against the Commissioner, in which the applicant seeks an order compelling our Office to reinvestigate a complaint the applicant filed against the Social Sciences and Humanities Research Council regarding a denial of access to his personal information under the *Privacy Act*.

The Federal Court dismissed the application on November 7, 2011, awarding $5,000 in costs to our Office. On December 1st, 2011, the applicant served our Office with a Notice of Appeal of the decision. At the time of writing this report, the appeal was pending before the Federal Court of Appeal.

The applicant has also made a series of parallel access complaints in various provinces and with the Office of the Information Commissioner of Canada. He has brought a second judicial review against our Office. (See T-272-12 below.)

X. v. *Privacy Commissioner of Canada*
Court File No. T-272-12 (FC)

This is a separate judicial review proceeding initiated by the applicant in the matters noted in the preceding paragraph. The applicant seeks judicial review of another report of findings issued by our Office, and other various reliefs. This matter is still pending before the Federal Court.

ADVANCING KNOWLEDGE

To keep pace with the rapidly changing field of threats to personal information, our Office variously sponsors workshops, commissions studies and sponsors research. Examples of such initiatives from the past fiscal year include:

Privacy in the age of social media, surveillance and citizen journalism

The past decade has witnessed an ever-increasing surveillance of public spaces. Whether from individuals or institutions, in the hands of police or protestors, miniaturization, mobile devices and new media now mean that while we may stand in public space, our presence is duly registered, recorded and increasingly reproducible for whatever reason.

To help inform discussion of this trend, our Office commissioned two independent papers from Jesse Hirsh, an Internet strategist, researcher, and broadcaster, and Kent Glowinski, an Ontario lawyer with expertise in privacy issues surrounding social media.

Their research considered how the emergence of new kinds of citizen journalism and mobile camera technologies can lead to new potential breaches of privacy.

The authors observe that citizens increasingly are playing an active role in identifying and implicating others in bad behaviour and criminal activity using mobile devices and shaming by social media. This trend is coupled with the growing interest of law enforcement in actively monitoring and engaging with social media.

The devices that ordinary Canadians use and depend upon, the nature of the interactive media they consume, the smart technologies they incorporate into their daily lives – all of these have converged as tools capable of capturing our every move.

The authors reflect on this new social reality and consider the implications for privacy in the age of social

media, where a moment of bad judgment, indiscretion or mistake is often captured – and not easily forgotten.

We expect to post these papers to our website in the next fiscal year.

Research in surveillance studies, ten years after 9/11

In conjunction with academics from four universities, our Office co-sponsored a research workshop, "The Expanding Surveillance Net: Ten Years after 9/11," hosted by the New Transparency Project at Queen's University.

The workshop presentations and discussions touched on themes exploring the social, political, legal and ethical implications of increased government and private sector surveillance in the wake of 9/11. Selected papers from the workshop will appear in a special issue of the *Canadian Journal of Law & Society*.

Research on electronic communications interception and privacy

University of Toronto Professor Wesley Wark received funding under our Office's Contributions Program to examine Canada's gathering of intelligence for national security purposes via the private sector.

The study included an examination of recent developments in this area, covering topics such as the collection of electronic communications by the Communications Security Establishment, Canada's recently released Cyber Security Strategy, enhanced intelligence-sharing proposals in the Canada-U.S. Perimeter Security Plan, and the draft "lawful access" legislation.

Professor Wark made suggestions on how the right policy framework can accommodate both privacy protection and the ramping up of electronic communications interception – a feature of the post 9/11 age of intelligence.

This paper is available on the University of Ottawa Centre for International Policy Studies site at (http://cips.uottawa.ca/wp-content/uploads/2012/04/WARK_WorkingPaper_April2012.pdf.

Research on drones

The proliferation of drones in the domestic skies is an emerging issue that requires careful consideration from a privacy perspective.

In light of this trend, we commissioned research from Angela Gendron, a Senior Fellow at the Canadian Centre of Intelligence and Security Studies at the Norman Paterson School of International Affairs at Carleton University.

Her research was conducted for internal purposes to help us understand the industry and examine some of the potential privacy issues.

Ms. Gendron shared her research perspectives on recent developments and debates in the use of unmanned aerial systems surveillance, the legal and

privacy implications of their use, and the challenges for oversight.

As well, she considered the economic and security factors driving the proliferation of drones in domestic skies and the private and social implications that accompany their covert capability to conduct overhead surveillance.

International comparison of the use of DNA for law enforcement

We commissioned a research paper by health law specialist Amy Conroy to examine the privacy risks inherent in the collection, use, and retention of genetic information within the context of criminal investigations.

Her research considered the privacy protections under Canadian laws compared to other jurisdictions, specifically the United States, United Kingdom, Australia, and the Netherlands. She found that jurisdictions are increasingly sharing DNA stored on their national data banks with foreign police authorities for the purposes of combating crime on a global scale.

However, little information is available about the agreements under which DNA sharing takes place, suggesting a need for greater transparency.

FOLLOW-UPS ON PREVIOUS AUDITS

The *Privacy Act* gives the Commissioner discretion to carry out audits of the relevant privacy practices of federal departments and agencies. If an audit finds shortcomings, the Commissioner can recommend remedial actions to the institution. The audit findings and recommendations may be published in an Annual Report or in special reports to Parliament.

The Act provides no further enforcement powers. Accordingly, about two years after the publication of an audit, we follow up to determine whether the audited organization has addressed our recommendations, or is following through on any commitments.

This year we did so for our audits of both Transport Canada's Passenger Protect Program and of departmental Annual Privacy Reports.

We were pleased to note that, of the six recommendations related to those two audits that were accepted, all have been fully or substantially implemented.

Passenger Protect Program

The Program

The Passenger Protect Program is better known to Canadians as the "no-fly list." This passenger

screening tool, operating since June 2007, aims to prevent people named on a "specified persons list" from boarding domestic or international flights leaving or bound for Canadian airports.

The program is secretive, using very sensitive personal information without the knowledge of the persons concerned to identify individuals Transport Canada considers an immediate threat to aviation security. The repercussions of being denied boarding on an aircraft can be profound in terms of privacy and other human rights, such as freedom of association and expression and the right to mobility. Not only can an individual's reputation suffer but also his or her ability to earn a living.

The Audit

Our audit, completed in November 2009, found that the collection and use of information within this program was done in accordance with the *Privacy Act* and the *Aeronautics Act*.

However, we also found that:

- The Deputy Minister of Transport Canada was not provided with complete information when deciding to add names to or remove names from the specified persons list;
- The information technology system used to disclose to air carriers information on the specified persons list had not been certified and accredited to meet government security standards;
- There were no requirements that air carriers report security breaches involving personal information to Transport Canada; and
- Transport Canada had not extended its oversight activities to verify that airlines are complying with requirements of the federal identity screening regulations related to the handling and safeguarding of specified persons list information.

Audit of the Passenger Protect ProgramTransport Canada (2009)

The Follow-up

Transport Canada indicated that procedural changes were implemented even before the completion of the audit to ensure that the Deputy Minister received all necessary information to make an informed decision. Effective February 2011, responsibility for this program was transferred to Public Safety Canada.

Transport Canada also indicated that, to ensure personal information in this system is adequately safeguarded, it updated its threat-and-risk assessment. As well, its security regulatory advisory system is now accredited as meeting government standards.

While Transport Canada did not fully accept our recommendation in 2009 that air carriers be required to report security breaches involving personal information, Public Safety Canada and Transport Canada both indicated

that they are pursuing a review of the regulations to address this issue.

Finally, Transport Canada indicated that its oversight of airline activities ensures that airlines comply with requirements for the handling and safeguarding of personal information on the specified persons list.

Departmental Annual Privacy Reports

In November 2009, we issued our audit findings related to federal institutions' Annual Privacy Reports. These reports provide a picture of how, in delivering programs, organizations manage and protect the personal information of Canadians under the *Privacy Act*. We examined the extent to which 33 federal departments were complying with the Treasury Board Secretariat's reporting requirements for these Annual Reports to Parliament.

Audit of the Federal Annual Privacy Reports (2009)

We found that, although the majority of these institutions complied with most, if not all, of the Treasury Board Secretariat's mandatory reporting requirements; many reports failed to provide anything beyond a basic level of information. They did not provide a clear picture about the organization's privacy practices, or its approach to managing the risks associated with the personal information it collects.

The Treasury Board Secretariat has indicated to us that it ensures that all mandatory reporting requirements are met by departments and any deficiencies noted are communicated to them.

We had also recommended that departments report privacy breaches, as well as steps taken to avoid future breaches in their Annual Privacy Reports. Although the Treasury Board Secretariat does not require departments to report breaches in their Annual Privacy Reports, we were pleased that, in 2010, the Secretariat issued a Directive on Privacy Practices.

The directive requires heads of government institutions to implement a plan that ensures that, in the event of a breach: affected individuals are notified; procedures are followed; privacy risks identified through the investigation are mitigated and corrective actions are implemented.

PUBLIC INTEREST DISCLOSURES UNDER SECTION 8(2)(*M*) OF THE *PRIVACY ACT*

Section 8(2)(*m*) of the *Privacy Act* allows an institution to disclose personal information without the consent of the individual concerned where, in the opinion of the institution head:

- The public interest in disclosure clearly outweighs any resulting invasion of privacy; or

- The disclosure would clearly benefit the individual to whom the information relates.

Institutions intending to make a public interest disclosure are required to notify our Office in writing, prior to the disclosure if possible or immediately afterwards.

Our Office reviews the disclosures and may express any concerns with the proposed disclosures or recommend that the individual whose personal information is being disclosed be notified of the disclosure if the institution has not already done so.

If the department declines to notify the individual, the Privacy Commissioner is empowered to do so.

However, the decision to release personal information in the public interest rests solely with the head of the institution and the Commissioner has no authority to prevent it.

During 2011-2012, we handled 107 disclosure notifications under section 8(2)(*m*), up significantly from the 80 dealt with the year previous. The 2011-2012 files included:

Department of Foreign Affairs and International Trade

The Department of Foreign Affairs and International Trade made 31 disclosures, once again more than any other any institution. Twenty-six of those concerned providing contact information to provincial health authorities for individuals who may have been exposed to tuberculosis infection from another passenger on a flight.

The other five related to providing police with contact information for the next of kin of individuals either missing or deceased.

Canada Border Services Agency

The Canada Border Services Agency notified our Office of 21 public interest disclosures in the past fiscal year, of which 20 concerned the removal from Canada of individuals on the "Wanted by the CBSA" list.

The other notification involved the disclosure of an address to a children's aid society in order to confirm the well-being of a minor who had been removed from Canada with her mother.

Royal Canadian Mounted Police

The Royal Canadian Mounted Police notified our Office of 21 public interest disclosures.

Almost two-thirds of those dealt with individuals being released into the community after serving sentences for assault, sexual assault or possession of child pornography and who were considered at high risk to reoffend.

Five other cases concerned information related to sexual offenses being disclosed to local police detachments for further investigation.

Another disclosure provided contact information for individuals who had undergone a specific surgery in the 1980s so they could ask their doctors about further follow-up.

The last two disclosures involved notifying the public of potential violence between two gangs and notifying a provincial College of Physicians and Surgeons of a doctor's consumption of non-prescribed drugs.

Correctional Service of Canada

The Correctional Service of Canada made nine disclosures to either inform victims before an inmate was transferred to another penitentiary or to inform family members about the circumstances surrounding the death of an inmate.

CHAPTER 5

The Year Ahead

The closing words in last year's Annual Report were a warning that privacy is far too crucial a concern for our society and our democratic values to let government dominate the debate.

We're repeating the same thought at the start of this chapter.

As a nation, we need to continue asking fundamental questions about privacy – and that discussion requires the full involvement of Canadians.

On the horizon at the time of writing this report are a plethora of federal government plans and proposals which carry profound implications for safeguarding the personal information of Canadians. Yet their very number and complexity could discourage many people from getting involved in the large-scale process of coming to public judgment that is essential in a democracy.

In 2012-2013, we anticipate that new surveillance initiatives and security measures will figure prominently in discussions of privacy protection focused within the public sector.

PERIMETER SECURITY

Canada and the United States have embarked on an ambitious agenda for examining how their shared border is managed and the extent to which goods and people entering the two countries are monitored and tracked.

The Canada-U.S. Perimeter Security and Economic Competiveness Action Plan, released in late 2011, sets out 32 separate initiatives that will take years to come to fruition. Taken together, these represent a major shift in how security, intelligence sharing, law enforcement and customs inspection are carried out in the two countries.

Development of joint Canada-US Privacy Principles, which would guide implementation of all programs and initiatives flowing from the Action Plan, is a critical step in our view. We have argued this foundation needs to address issues of openness,

transparency, retention, redress, accuracy and access. In short, all the Fair Information Principles should be accounted for, to provide a strong basis for protecting the privacy rights of all Canadians.

Our Office and our provincial and territorial counterparts have already underlined the fact that many of the planned initiatives carry privacy risks.

Our Office will be devoting considerable attention to the review and analysis of these commitments in the coming year, through media outreach, support of parliamentary deliberations and studies, and the Privacy Impact Assessment process.

Expanded Surveillance

Meanwhile, there are also proposals to expand government surveillance and monitoring. In some cases, these are based on new technologies, such as aerial drones or rapidly evolving facial recognition software.

In other cases, the increased surveillance and monitoring would come through new investigative powers for gathering online information, tracking the location of electronic devices and identifying users of Internet services.

Citizens from all walks of life, from every part of the country, connect instinctively with this issue. When government proposes new methods of electronic surveillance – and seeks to recast privacy protections in the law in favor of greater investigative powers – the views of Canadian citizens must be taken into account. Canadian legislation, under the Canadian Charter of Rights and Freedoms and the *Privacy Act*, imposes clear limits on obtaining personal information.

In particular, personal information can only be collected by a government institution when it relates directly to an operating program or activity of that institution, and cannot be compelled by law enforcement without a warrant unless it is an emergency. Our Office remains concerned about the broad nature of current legislative proposals for lawful access, and we believe there are options for limiting its use to cases where it is justifiable and proportional.

Further Initiatives

In addition, reforms to immigration legislation are also expected to generate a number of PIAs with changes to the application processes and as applicant information is shared and tracked more widely.

We have already had a number of consultations on information-sharing arrangements now under development, and expect to receive more than a dozen PIAs related to collection, use, and exchange of personal information – including fingerprints – for bilateral immigration and border control.

The federal government's plans to begin to share services between departments, meanwhile, will present our Office with potential challenges on many fronts. We will remind government that appropriate consideration needs to be given to privacy when consolidating IT infrastructures, data centres and email services. Privacy issues will need to be carefully considered as

the potential outsourcing of some services to non-government service providers is examined.

In all these matters, the policy, legal and technical questions are complex; the potential implications for privacy in Canada profound.

The position of our Office has been, and will continue to be, that while new issues for law enforcement may be emerging from online environments, Canadian legal standards and our intrinsic expectations of privacy as citizens deserve to be upheld and protected.

As a nation we need to continue asking fundamental questions about privacy. Why is it so important? What would our society look like without it?

These questions must be asked with the full involvement of Canadians, rather than abandoning the debate to the public sector by default.

So we will continue to engage and educate citizens across Canada on privacy issues, protection of personal information and their rights of access – through public events, timely research, open discussions and seminars, as well as through new media channels online.

Our Office has another weighty responsibility in the coming 12 months. Like athletes facing a major competition, we need to raise our game to meet these emerging challenges.

For that reason we have already started to enhance the Office's technological support capacity by expanding both our team of technologists and their state-of-the-art testing laboratory.

In the next fiscal year, we expect to launch a new online complaint form, which will facilitate the submission of complaints.

We have also embarked on a modernization project intended to simplify the *Privacy Act* complaints investigation process and to shorten the time needed to resolve complaints.

Shortening resolution times is vital if the Office is going to be able to deal with the anticipated rise in privacy challenges while resources remain flat-lined for the next two fiscal years. (And that's a best-case economic scenario since a forced move to new offices in 2013 will bring significant additional costs, for which we are seeking supplementary funding.)

Canada Revenue Agency Audit

Our Office has identified a number of ongoing privacy risks at the Canada Revenue Agency and has selected that organization for an audit under Section 37 of the *Privacy Act*.

The Agency's repository of over 30 million taxpayer files and hundreds of millions of related records is one of the largest such holdings in the country. These documents contain highly sensitive financial, employment, family and health information. This vast

databank of personal information is accessible to over 20,000 full-time employees and several thousand casual employees hired each year during tax season.

A number of privacy breaches involving employees inappropriately accessing taxpayer information, have been reported to our Office in recent years and there is a potential risk that a future breach could affect thousands of Canadians – and also undermine public trust in the Agency.

At the time of writing this report, the audit had commenced and our Office was in the process of identifying areas for examination.

Conclusion

Finally, as the *Privacy Act* enters its fourth decade we hearken back to these words from Commissioner John Grace, in our Office's first Annual Report:

> *Societies which treat privacy with contempt and use personal information as a cheap commodity will sooner or later hold the same attitudes towards their citizens. Privacy, therefore, is not simply a precious and often irreplaceable human resource; respect for privacy is the acknowledgment of respect for human dignity and the individuality of man.*

Thirty years on, those words remain as true – and undoubtedly even more important – than when they were written.

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.

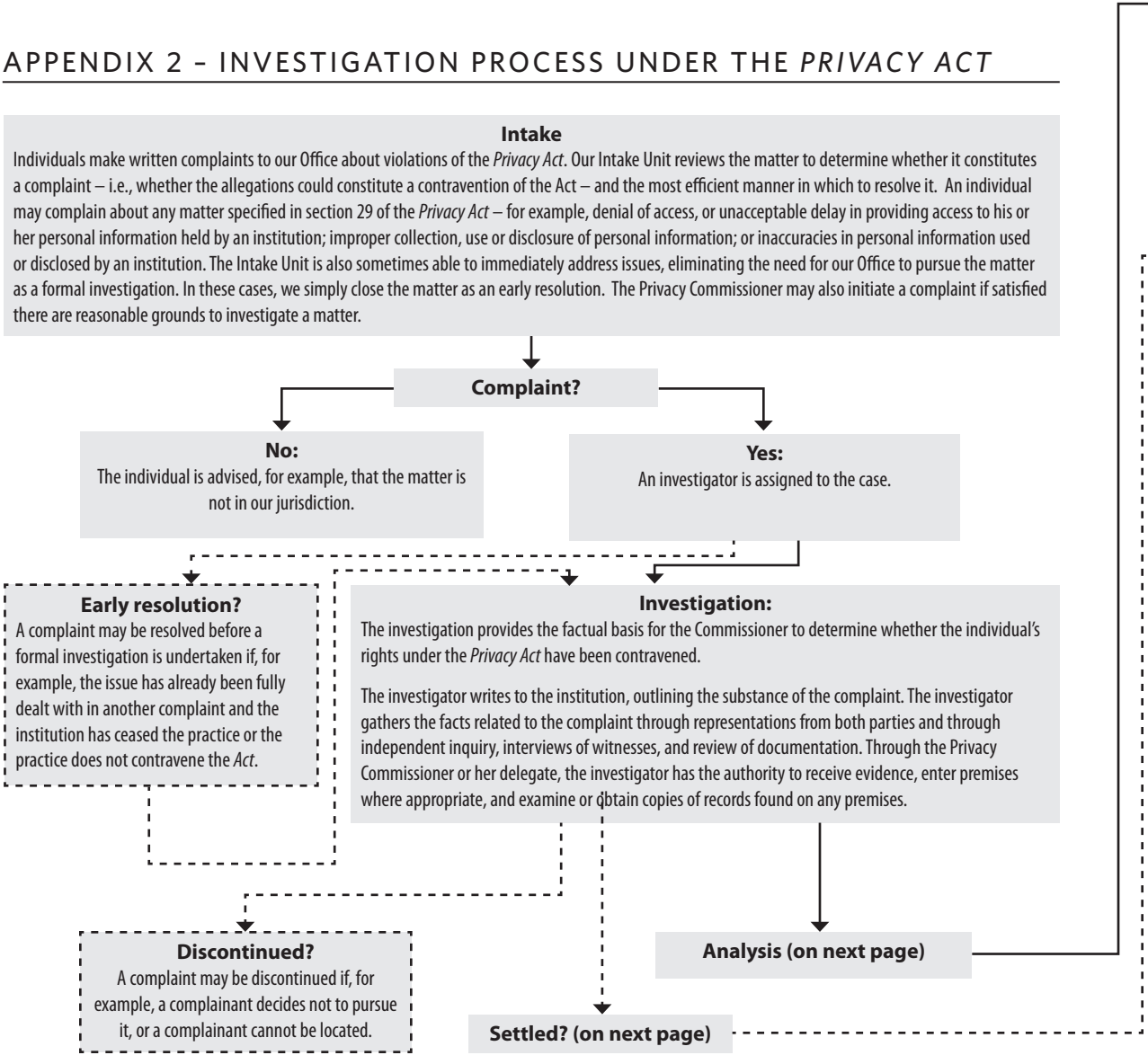
2. Other Dispositions

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 – COMPLAINTS AND INVESTIGATIONS UNDER THE *PRIVACY ACT*, APRIL 1, 2011 TO – MARCH 31, 2012

COMPLAINTS ACCEPTED BY COMPLAINT TYPE

COMPLAINT TYPE	Early Resolution	Formal Complaints	Total	Percentage
Access	129	299	428	43.41%
Correction / Notation	11	1	12	1.22%
Language	1	0	1	0.10%
Fees	0	1	1	0.10%
Time Limits	94	227	321	32.56%
Correction – Time Limits	0	1	1	0.10%
Extension Notice	1	3	4	0.41%
Collection	16	18	34	3.45%
Retention and Disposal	3	5	8	0.81%
Use and Disclosure	60	116	176	17.85%
TOTAL ACCEPTED	**315**	**671**	**986**	

- As in 2010-2011, the most common category of complaints to our Office in 2011-2012 related to difficulties people were encountering in gaining access to their personal information in the hands of government departments or agencies. These access complaints accounted for a combined total of 442, or 45 percent of all complaints accepted. This number was up by 34 percent from 2010-2011, when we reported 328 such complaints.

- The second-most common reason for people to file complaints with our Office related to the length of time institutions were taking to respond to access requests. We received 326 time limit complaints, about one-third of the complaints we accepted. This is also an increase of 30 percent from last year's 251 time limit complaints accepted.

- Privacy complaints, which include problems related to the collection, use, disclosure, retention or disposal of personal information, comprised a total of 218 complaints, representing 22 percent of the total complaints accepted. This is a substantial jump (69 percent) over the 129 privacy type complaints received in 2010-2011.

TOP 10 INSTITUTIONS BY COMPLAINTS ACCEPTED

	ACCESS			TIME LIMITS			PRIVACY			
	Early Resolution	Formal Complaints	TOTAL	Early Resolution	Formal Complaints	TOTAL	Early Resolution	Formal Complaints	TOTAL	TOTAL
Correctional Service of Canada	53	92	145	32	95	127	21	33	54	326
Royal Canadian Mounted Police	36	24	60	12	13	25	13	19	32	117
National Defence	8	22	30	30	46	76	3	6	9	115
Canada Revenue Agency	5	19	24	3	20	23	7	11	18	65
Canada Border Services Agency	5	34	39	2	6	8	2	6	8	55
Veterans Affairs Canada	4	5	9	1	17	18	2	10	12	39
Canadian Security Intelligence Service	3	27	30	1	0	1	0	1	1	32
Human Resources and Skills Development Canada	5	8	13	4	2	6	2	5	7	26
Public Works And Government Services Canada	2	12	14	2	2	4	1	6	7	25
Canada Post Corporation	5	5	10	0	2	2	8	2	10	22
All Other Federal Departments and Agencies	15	53	68	8	28	36	20	40	60	164
TOTAL	**141**	**301**	**442**	**95**	**231**	**326**	**79**	**139**	**218**	**986**

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. This may, in turn, lead to complaints about the institution's collection, use, disclosure, retention or disposal of personal information, or the manner in which it provides access to that information.

See page 62 for a discussion of the year-over-year changes in the Top 10 list.

TOP 10 INSTITUTIONS BY COMPLAINTS ACCEPTED IN 2011-2012
(Three-year history)

ORGANIZATION	2009-2010	2010-2011	2011-2012
Correctional Service of Canada	290	276	**326**
Royal Canadian Mounted Police	60	75	**117**
National Defence	47	65	**115**
Canada Revenue Agency	49	53	**65**
Canada Border Services Agency	26	29	**55**
Veterans Affairs Canada	2	15	**39**
Canadian Security Intelligence Service	26	16	**32**
Human Resources and Skills Development Canada	20	25	**26**
Public Works And Government Services Canada	7	8	**25**
Canada Post Corporation	23	27	**22**
All Other Departments and Agencies	98	111	**164**

COMPLAINTS ACCEPTED BY INSTITUTION

ORGANIZATION	Early Resolution	Formal Complaints	TOTAL
Aboriginal Affairs and Northern Development Canada	1	10	11
Canada Border Services Agency	9	46	55
Canada Post Corporation	13	9	22
Canada Revenue Agency	15	50	65
Canadian Air Transport Security Authority	1	0	1
Canadian Broadcasting Corporation	0	2	2
Canadian Cultural Property Export Review Board	0	1	1
Canadian Food Inspection Agency	0	3	3
Canadian Forces Grievance Board	1	6	7
Canadian Heritage	0	3	3
Canadian Security Intelligence Service	4	28	32
Canadian Space Agency	0	4	4
Citizenship and Immigration Canada	4	18	22
Commission for Public Complaints Against the RCMP	0	2	2
Correctional Service of Canada	106	220	326
Environment Canada	0	1	1
Fisheries and Oceans Canada	1	4	5
Foreign Affairs and International Trade Canada	0	5	5
Health Canada	2	2	4
Human Resources and Skills Development Canada	11	15	26
Immigration and Refugee Board	2	2	4
Industry Canada	2	1	3
Justice Canada	3	6	9
Library and Archives Canada	0	1	1
Military Police Complaints Commission	1	0	1
National Arts Centre	1	0	1
National Capital Commission	1	0	1
National Defence	41	74	115

COMPLAINTS ACCEPTED BY INSTITUTION (cont.)

ORGANIZATION	Early Resolution	Formal Complaints	TOTAL
National Energy Board	0	2	2
National Gallery of Canada	0	2	2
National Research Council Canada	0	1	1
Natural Resources Canada	1	5	6
Office of the Chief Electoral Officer of Canada	1	1	2
Parole Board of Canada	1	1	2
Passport Canada	2	13	15
Privy Council Office	0	1	1
Public Health Agency of Canada	1	5	6
Public Prosecution Service of Canada	1	4	5
Public Safety Canada	1	1	2
Public Service Commission of Canada	2	0	2
Public Service Labour Relations Board	2	1	3
Public Works And Government Services Canada	5	20	25
Royal Canadian Mounted Police	61	56	117
Security Intelligence Review Committee	0	1	1
Social Science and Humanities Research Council	0	2	2
Statistics Canada	6	2	8
Transport Canada	2	4	6
Treasury Board of Canada Secretariat	3	2	5
Veterans Affairs Canada	7	32	39
Veterans Review and Appeal Board	0	1	1
VIA Rail Canada	0	1	1
	315	**671**	**986**

COMPLAINTS ACCEPTED BY PROVINCE/TERRITORY

PROVINCE/TERRITORY	Early Resolution	Formal Complaints	Total	Percentage
Ontario	121	277	398	40.37%
Quebec	52	164	216	21.91%
British Columbia	75	92	167	16.94%
Alberta	33	62	95	9.63%
Saskatchewan	10	20	30	3.04%
Manitoba	7	20	27	2.74%
Nova Scotia	9	12	21	2.13%
New Brunswick	5	7	12	1.22%
International*	0	9	9	0.91%
Newfoundland and Labrador	0	5	5	0.51%
None provided	1	1	2	0.20%
Northwest Territories	1	0	1	0.10%
Nunavut	0	1	1	0.10%
Prince Edward Island	1	0	1	0.10%
Yukon Territories	0	1	1	0.10%
TOTAL	**315**	**671**	**986**	

* The right of access to personal information applies to Canadian citizens, permanent residents, inmates of Canadian penitentiaries, and any other individuals "present in Canada." These individuals have the corresponding right to complain to our Office concerning a denial of access. Canadians living abroad have the same rights of access and complaint as those living in Canada, and nine people chose to exercise those rights in 2011-2012. The privacy protections contained in sections 4 to 8 of the *Privacy Act*, related to the collection, use, disclosure, retention and disposal 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.

Ontario, home to a significant proportion of the Canadian population, still holds first place for highest number of complaints. The number of complaints originating in Ontario increased from 213 in 2010-2011, to 398 in 2011-2012 (a jump of 87 percent), and this represents 40 percent of all complaints accepted by our Office during 2011-2012. The increase can be attributed to multiple complaints by the same complainant in many cases.

We also saw a decline in complaints from Newfoundland and Labrador, from 24 to 5 year-over-year.

We also noticed an increase of international complaints, with 9 such complaints in 2011-2012, compared to just 2 the year previous.

DISPOSITION BY COMPLAINT TYPE

COMPLAINT TYPE	Investigative Findings				Other Dispositions			TOTAL
	Well Founded	Well Founded–Resolved	Not Well Founded	Resolved	Discontinued	Early Resolution	Settled During Investigation	
Access	3	26	185	12	65	83	44	418
Correction / Notation	0	2	0	1	1	11	1	16
Language	0	0	0	0	0	1	0	1
Fees	0	0	0	0	0	0	0	0
ACCESS TOTAL	**3**	**28**	**185**	**13**	**66**	**95**	**45**	**435**
Time Limits	216	0	21	0	11	65	3	316
Correction – Time Limits	1	0	0	0	1	0	0	2
Extension Notice	0	0	3	0	0	1	0	4
TIME LIMITS TOTAL	**217**	**0**	**24**	**0**	**12**	**66**	**3**	**322**
Collection	1	2	7	0	0	16	2	28
Use and Disclosure	26	2	28	1	18	32	11	118
Retention and Disposal	0	0	4	0	0	4	2	10
PRIVACY TOTAL	**27**	**4**	**39**	**1**	**18**	**52**	**15**	**156**
TOTAL CLOSED	**247**	**32**	**248**	**14**	**96**	**213**	**63**	**913**

We accepted almost the same number of complaints that we concluded in 2011-2012 – 986 accepted, and 913 concluded.

The 913 complaints closed in 2011-2012 represented an increase of 60 percent from 2010-2011, when we closed 570 complaints.

The figure of 913 closed complaints includes 213 complaints closed through the use of early resolution (23 percent of complaints closed).

Access: Complaints about access to personal information were the most common category of files we closed last year – a total of 435 complaints, comprising 48 percent of all the complaints closed. Almost half of the total number of cases closed (43 percent) were concluded as not well founded. Of the remaining cases investigated, 28 were concluded as well-founded, resolved; another 13 were investigated and found to have merit, but were resolved through negotiation rather than a formal finding; and 3 cases were upheld as well founded. Of the remaining 206 cases in which other dispositions were rendered, 95 cases were resolved through the early resolution process, 66 cases were discontinued and the remaining 45 cases were settled during the investigation.

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 322, or 35 percent of our caseload. Most complainants only come to us after the statutory deadline for their complaint has passed, and therefore 217 (or 67 percent) of those complaints were well founded.

Privacy: Cases involving the collection, use, disclosure, retention or disposal of personal information combined to account for 156, or 17 percent, of all complaints we closed in 2011-2012. Our investigations found that 27 of the complaints were well founded, and 39 were not well founded. Of note, we were successful in resolving early one third of these cases (52). The vast majority of all privacy complaints related to the improper use or disclosure of personal information.

DISPOSITION OF TIME LIMITS COMPLAINTS BY INSTITUTION

ORGANIZATION	Well founded	Well founded-Resolved	Not Well founded	Resolved	Discontinued	Early Resolution	Settled during Investigation	TOTAL
Aboriginal Affairs and Northern Development Canada	3	0	0	0	0	0	0	3
Canada Border Services Agency	7	0	1	0	0	1	0	9
Canada Post Corporation	2	0	2	0	0	0	0	4
Canada Revenue Agency	14	0	0	0	4	3	0	21
Canadian Forces Grievance Board	0	0	0	0	0	1	0	1
Canadian Heritage	1	0	0	0	0	0	0	1
Canadian Human Rights Tribunal	0	0	2	0	0	0	0	2
Canadian International Development Agency	1	0	0	0	0	0	0	1
Canadian Security Intelligence Service	1	0	0	0	0	1	0	2
Citizenship and Immigration Canada	4	0	1	0	1	3	0	9
Commission for Public Complaints Against the RCMP	1	0	0	0	0	0	0	1
Correctional Service of Canada	118	0	12	0	4	23	2	159
Fisheries and Oceans Canada	1	0	0	0	0	0	0	1
Foreign Affairs and International Trade Canada	3	0	0	0	0	0	0	3

DISPOSITION OF TIME LIMITS COMPLAINTS BY INSTITUTION (cont.)

ORGANIZATION	Well founded	Well founded-Resolved	Not Well founded	Resolved	Discontinued	Early Resolution	Settled during Investigation	TOTAL
Health Canada	4	0	0	0	0	1	0	5
Human Resources and Skills Development Canada	2	0	0	0	0	3	0	5
Justice Canada	1	0	0	0	0	0	0	1
National Defence	33	0	0	0	1	19	0	53
National Energy Board	1	0	0	0	0	0	0	1
Natural Resources Canada	1	0	1	0	0	0	0	2
Privy Council Office	1	0	0	0	0	0	0	1
Public Prosecution Service of Canada	0	0	0	0	0	1	0	1
Public Works And Government Services Canada	2	0	0	0	0	2	0	4
Royal Canadian Mounted Police	7	0	3	0	2	7	1	20
Transport Canada	3	0	0	0	0	0	0	3
Treasury Board of Canada Secretariat	0	0	2	0	0	0	0	2
Veterans Affairs Canada	6	0	0	0	0	1	0	7
TOTAL	**217**	**0**	**24**	**0**	**12**	**66**	**3**	**322**

DISPOSITION OF ACCESS AND PRIVACY COMPLAINTS BY INSTITUTION

ORGANIZATION	Well founded	Well founded-Resolved	Not Well founded	Resolved	Discontinued	Early Resolution	Settled during Investigation	TOTAL
Aboriginal Affairs and Northern Development Canada	2	1	0	0	0	1	0	4
Business Development Bank of Canada	0	0	0	0	1	0	0	1
Canada Border Services Agency	3	1	19	0	11	4	3	41
Canada Post Corporation	1	1	6	1	0	8	3	20
Canada Revenue Agency	3	1	17	0	12	9	3	45
Canadian Air Transport Security Authority	0	0	0	0	0	1	0	1
Canadian Broadcasting Corporation	0	1	0	0	1	0	0	2
Canadian Food Inspection Agency	0	0	1	0	2	0	0	3
Canadian Forces Grievance Board	0	0	0	0	0	0	5	5
Canadian Heritage	0	0	0	0	1	0	0	1
Canadian Human Rights Tribunal	1	0	0	0	0	0	0	1
Canadian Radio-Television and Telecommunications Commission	0	0	0	0	0	1	0	1
Canadian Security Intelligence Service	0	0	25	0	1	2	0	28
Canadian Space Agency	0	0	1	0	0	0	0	1
Citizenship and Immigration Canada	1	2	7	1	1	0	1	13
Commission for Public Complaints Against the RCMP	0	0	0	0	0	0	1	1
Correctional Service of Canada	3	9	50	1	22	32	28	145
Financial Transactions and Reports Analysis Centre of Canada	0	0	2	0	0	0	0	2
Fisheries and Oceans Canada	0	0	2	0	2	1	0	5
Foreign Affairs and International Trade Canada	0	0	2	1	0	0	2	5
Health Canada	0	0	2	0	1	0	0	3

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

ORGANIZATION	Well founded	Well founded-Resolved	Not Well founded	Resolved	Discontinued	Early Resolution	Settled during Investigation	TOTAL
Human Resources and Skills Development Canada	2	2	9	0	3	7	1	24
Immigration and Refugee Board	1	0	0	0	1	1	1	4
Industry Canada	1	0	0	1	0	1	0	3
Justice Canada	2	0	4	1	1	1	0	9
Library and Archives Canada	0	0	1	0	0	0	0	1
Military Police Complaints Commission	0	0	0	0	0	1	0	1
National Arts Centre	0	0	0	0	0	1	0	1
National Capital Commission	0	0	0	0	1	0	0	1
National Defence	2	7	17	2	7	8	5	48
Natural Resources Canada	0	0	0	0	2	1	0	3
Office of the Chief Electoral Officer of Canada	0	0	1	0	0	1	0	2
Office of the Information Commissioner of Canada	1	0	0	0	1	0	1	3
Parole Board of Canada	0	0	2	0	0	1	0	3
Passport Canada	0	0	0	0	1	2	1	4
Public Health Agency of Canada	0	0	0	0	1	0	0	1
Public Safety Canada	0	0	2	0	0	1	0	3
Public Service Commission Canada	0	0	0	0	0	1	0	1
Public Service Labour Relations Board	1	0	0	0	0	2	0	3
Public Works And Government Services Canada	0	0	5	1	0	3	0	9
Royal Canadian Mounted Police	2	5	39	4	6	40	3	99

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

ORGANIZATION	Well founded	Well founded-Resolved	Not Well founded	Resolved	Discontinued	Early Resolution	Settled during Investigation	TOTAL
Social Science and Humanities Research Council	0	0	1	1	0	0	0	2
Statistics Canada	0	0	1	0	0	5	1	7
Transport Canada	0	2	3	0	0	2	0	7
Treasury Board of Canada Secretariat	0	0	0	0	0	3	0	3
Veterans Affairs Canada	4	0	3	0	5	6	0	18
Veterans Review and Appeal Board	0	0	0	0	0	0	1	1
VIA Rail Canada	0	0	1	0	0	0	0	1
Western Economic Diversification Canada	0	0	1	0	0	0	0	1
TOTAL	**30**	**32**	**224**	**14**	**84**	**147**	**60**	**591**

TREATMENT TIMES

EARLY RESOLUTION CASES BY COMPLAINT TYPE

COMPLAINT TYPE	# of Cases	Avg Treatment Time (Months)
Access	83	2.19
Time Limits	65	1.35
Use and Disclosure	32	2.38
Collection	16	1.94
Correction – Notation	11	0.73
Retention and Disposal	4	3.50
Extension Notice	1	2.00
Language	1	1.00
TOTAL	**213**	**1.89**

Note on Treatment Times: In past Annual Reports, we reported on complaints based on the *complaint received date* – the actual date a complaint was received by the OPC. However, this led to artificially high treatment times for some cases in which we didn't receive sufficient information required to begin an investigation. In 2011, we modified our intake process and revised the treatment time definition. It is now based on the time between when a complaint is accepted to when a finding is made or the case is otherwise disposed of. As a result, we now report based on the *complaint acceptance date* – when our Office receives enough information to make a complaint complete and clear enough to investigate.

TREATMENT TIMES

FORMAL INVESTIGATIONS BY COMPLAINT TYPE

COMPLAINT TYPE	# of Cases	Average Treatment Time (Months)
Access	335	8.16
Time Limits	251	4.41
Use and Disclosure	86	8.24
Collection	12	10.00
Retention and Disposal	6	11.00
Correction / Notation	5	12.80
Extension Notice	3	3.00
Correction – Time Limits	2	3.00
TOTAL	**700**	**7.58**

TREATMENT TIMES

ALL CLOSED FILES BY DISPOSITON

DISPOSITION	# of Cases	Avg Treatment Time (Months)
Not well-founded	248	8.55
Well-founded	247	5.24
Early Resolution	213	1.93
Discontinued	96	7.39
Settled	63	4.86
Well-founded resolved	32	10.45
Resolved	14	11.57
TOTAL	**913**	**5.76**

Treatment times are measured from the date a complaint is *accepted* to when a finding is made or the case is otherwise disposed of. As noted earlier, this definition is a change from previous years.

The average treatment time to complete investigations *and* early resolution cases (total 913**)** dropped last year to 5.8 months. In 2010-2011, the average treatment time was 7.2 months to conclude 570 cases.

Both our emphasis on early-resolution strategies and the elimination of a backlog of complaints have enabled us to reduce the average treatment times for all complaints significantly in recent years.

Our average treatment time for formal investigations (not including early resolution cases) has fallen to 7.6 months (700 complaints) in 2011-2012, compared to 8.0 months (492 complaints) in 2010-2011.