Office of the
Privacy Commissioner
of Canada

Privacy Act

Annual Report to Parliament

2010-2011

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

Follow us on Twitter: @privacyprivee

Cat. No. IP50-2011E-PDF
ISBN 978-1-100-17831-8

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

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

November 2011

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 April 1, 2010 to March 31, 2011. This tabling is pursuant to section 38 of the *Privacy Act*.

Sincerely,

Original signed by

Jennifer Stoddart
Privacy Commissioner of Canada

Privacy Commissioner of Canada

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 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

November 2011

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 April 1, 2010 to March 31, 2011. This tabling is pursuant to section 38 of the *Privacy Act*.

Sincerely,

Original signed by

Jennifer Stoddart
Privacy Commissioner of Canada

TABLE OF CONTENTS

ABOUT THE *PRIVACY ACT*

The *Privacy Act*, which took effect in 1983, obliges approximately 250 federal government departments and agencies 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 organizations. 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

In the decade since 9/11, safety in the skies has come at a growing cost to privacy. In a wearisome modern ritual, we shed shoes and boots, and unzip our luggage to exhibit tiny toiletries in clear plastic bags. We "choose" whether to be patted down by a uniformed stranger, or to stand spread-eagled in a glass-enclosed scanner. We accept that our travel plans, passport numbers and other personal information are shared among airlines and governments.

We endure all this because we have no alternative if we wish to travel through Canadian airports. And, at the end of it all, we anticipate a significant payoff: a flight safe from terrorists and other threats.

From my perspective as Privacy Commissioner, however, that's not the whole story. In addition to providing physical security, the state also has an obligation to treat individuals with respect — to preserve their dignity and to safeguard their personal information.

This is not a mere frill or a "nice-to-have"; it is fundamental to the trust relationship that must exist between citizens and their government.

This annual report takes a good hard look at the federal government's stewardship of personal information — in the context of aviation security, law enforcement and day-to-day government operations.

While there is much to applaud, the record is not unblemished.

In an audit of airport security measures, for instance, we looked inside the private rooms where officers review images generated by full-body scanners and found a closed-circuit television camera and a cellphone. We did not find many such devices with recording capabilities — but nor did we find none, as the rules require.

We also found highly sensitive documents related to security incidents stored on open shelves and in boxes where passengers may be present.

TOO MUCH INFORMATION

But of even greater concern to us was that security authorities were collecting more personal information than permitted under their mandate — on incidents that were not threats to air safety and that, in some cases, were not even illegal.

A separate audit of the RCMP's control over its operational databases also raised concerns over the stewardship of personal information.

For example, when a person receives a pardon for a past crime, or is found to have been wrongfully convicted of an offence, the RCMP is supposed to block access to any information about the incident in its database. This hasn't been happening, so even though people have a right to get on with their lives, information about their past can continue to be shared.

Without question, the state needs personal information to govern. No government could avert a terrorist attack, fight crime, issue a passport or administer the tax system without data about individuals.

Modern information technology facilitates the process. Data can be collected more rapidly and in greater quantity than ever before. It can also be processed, manipulated, transformed, stored and disclosed more readily than ever before.

The stated objective of all this data management is better program delivery, strengthened public safety, and more effective governance and accountability.

But, as this report describes, so much personal information in the hands of government can also pose risks to the privacy of individuals.

PRIVACY RISKS

For instance, it is none of the state's business if a person travels in Canada with large sums of cash, yet such information is collected and shared among authorities. A wealthy traveller becomes a suspicious traveller.

A person's criminal conviction is overturned and the police record ought to be sealed. Instead, the same erroneous information that led to the wrongful conviction can continue to circulate, potentially crippling careers and even lives.

One vocal critic of the government discovers that his sensitive medical information is included in a ministerial briefing binder and shared widely among officials with no reason to know about it.

Too much information can also lead to data spills. A troubling finding in this report is that the most preventable privacy invasions are often the result of simple human error — like the psychiatric nurse at a federal correctional institution who forgot a patient's file on a city bus.

These are some of the reasons why the *Privacy Act* sets rules around the collection, use, storage, retention, safeguarding and disclosure of personal information. And this report is about the state's stewardship of personal information under the Act in 2010-2011. It describes what the government is doing right, what it's doing wrong, and how our Office worked to highlight opportunities for improvement.

Personal information is available today in unprecedented amounts, and the state's appetite for it is voracious. The technology used to manage the data is powerful, yet at the same time also vulnerable.

In this uniquely challenging context, the Government of Canada is obliged to handle the personal information of Canadians with an uncompromising level of care.

Not some of the time, or even most of the time, but all of the time.

Our Office will continue to ensure it lives up to its obligations — and to the trust and expectations of Canadians.

Privacy by the Numbers 2010-2011

INQUIRIES

Received	
Linked to the *Privacy Act*	**1,944**
Linked to the *Personal Information Protection and Electronic Documents Act* (PIPEDA)	4,789
Not linked exclusively to either Act	2,188
Total received	***8,921***

Closed	
Linked to the *Privacy Act*	**1,859**
Linked to the *Personal Information Protection and Electronic Documents Act* (PIPEDA)	4,762
Not linked exclusively to either Act	2,183
Total closed	***8,804***

PRIVACY ACT COMPLAINTS

Received	
Access	328
Time Limits	251
Privacy	129
Total received	***708***

Closed	
Through early resolution	
Access	30
Time Limits	6
Privacy	42
Total	**78**
Through investigation	
Access	182
Time Limits	251
Privacy	59
Total	**492**
Total closed	***570***

PRIVACY IMPACT ASSESSMENT REVIEWS

Received	52
Reviewed as high risk	19
Reviewed as lower risk	68
Total reviewed	***87***

AUDITS

Public-sector privacy audits	2

LEGAL ACTIVITY RELATED TO THE *PRIVACY ACT*

Legal opinions	16
Litigation — decisions rendered	0
Litigation — cases settled	2

POLICY AND PARLIAMENTARY AFFAIRS

Draft bills and legislation reviewed for privacy implications	19
Public-sector policies or initiatives reviewed for privacy implications	51
Policy guidance documents issued	16
Parliamentary committee appearances on public-sector matters	14
Other interactions with Parliamentarians or staff	34

OTHER OPC ACTIVITIES

Public sector	
Visits by external stakeholders	32
Public events	2
Combined public and private sectors	
Speeches and presentations	112
News releases and communications tools	57
Exhibits and other offsite promotional activities	20
Publications distributed	34,007
Visits to principal OPC website	2.22 million
Visits to OPC blogs and other websites	1.01 million
New subscriptions to e-newsletter	321
Total subscriptions to e-newsletter	1,013

ACCESS TO INFORMATION ACT

Requests received	63
Requests closed	64

PRIVACY ACT

Requests received	105
Requests closed	106

CHAPTER 1

The Year in Review

Key Accomplishments in 2010-2011

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.

For details on any of these activities, please refer to the associated section numbers of this report, listed at the right.

Privacy Compliance Audits	
We conducted two audits during the year to test for compliance with the *Privacy Act*.	
One examined whether the Canadian Air Transport Security Authority (CATSA) and the thousands of airport screeners it hires under contract respect the privacy of the travelling public and are good stewards of their personal information. It found that, while elements of a privacy management framework are in place, some significant gaps remain in practice. Of greatest concern is that the agency collects personal information beyond its statutory authority. For example, CATSA officers sometimes alert police when they encounter a traveller on a domestic flight carrying large sums of cash. It is legal to transport money within Canada, and, in any case, the matter is unrelated to aviation safety and therefore lies outside the agency's mandate.	**2.1**

We also found issues around the safekeeping of sensitive documents. For instance, incident reports turned up on open shelving units, on the floor and even in a room where passengers are taken for further screening. Moreover, despite being strictly prohibited, the audit discovered a cell phone and a closed-circuit TV camera in the rooms where officers view the images generated by full-body scanners. These issues were addressed promptly when brought to the attention of CATSA authorities.	**2.1**
Our other audit looked at the RCMP's management of operational databases that are widely shared with other police services and government institutions. One of the best known is CPIC, the Canadian Police Information Centre, which holds more than 10 million records and is accessed by approximately 80,000 law enforcement officers in more than 3,000 police departments, RCMP detachments, and federal and provincial agencies. While the RCMP has policies and procedures in place to safeguard this sensitive information, we also found some troubling gaps. For instance, with respect to a database called the Police Reporting and Occurrence System (PROS), the RCMP has no process to withhold access to any information that relates to an offence for which a pardon has been granted or — worse — that resulted in a wrongful conviction. The RCMP committed to addressing all of our concerns.	**2.2**
We also followed up on three audits that we conducted in 2008 and 2009. We were advised by the responsible departments that 32 of the 34 recommendations we had made in those audits had been implemented, either entirely or to a substantial degree.	**4.4**
One follow-up inquiry focused on the RCMP's exempt databanks, which store personal data that is not subject to the access provisions of the *Privacy Act*. We were pleased to learn that the force had followed our recommendations to sift through the data, and purge any that should not be there. Indeed, by March 2011, all but 190 of the 5,288 files that had been in the RCMP's national security exempt databank in March 2008 had been removed. Similarly, more than 58,000 criminal intelligence files were weeded out.	**2.5**

Inquiries, Complaints and Data Breaches	
Our inquiries unit responded to 1,859 calls and letters related directly to the *Privacy Act* in 2010-2011, a 30-percent decline from the year before. We fielded a further 2,183 inquiries where the applicable privacy law could not be determined, or that pertained to neither of the two statutes. Since the number of visits to our Office website continues to rise — up since 2007-2008 by 31 percent, to 2.2 million visitors in 2010-2011 — we surmise that more people are going online to find answers to their privacy-related questions.	**5.1.1**
We continued this year to focus on early-resolution strategies, under which complaints are resolved without formal investigations. In all, 78 of the 570 complaints we closed last year were resolved in this way. This represented 14 percent of our caseload, up from six percent the year before. This has had a beneficial impact on the timeliness of our service. Early resolution cases were closed in an average of 3.6 months last year, bringing our overall treatment times down to 7.2 months, on average, from 12.9 months in 2009-2010.	**5.1.2**
Of the 492 complaints that proceeded to full investigations in 2010-2011, the vast majority related to problems that people had in gaining access to their personal information in the hands of government (182), or to the time it took for the government to respond to their access requests (251). Nearly 80 percent of the time-limits complaints we investigated were lodged against the Correctional Service of Canada (150), the Canada Revenue Agency (24) or the Department of National Defence (23). We issued formal findings in 443 of our investigations, with the others being discontinued (41) or settled during the course of the investigation (8). In 63 percent of those findings we sided with the complainant, most often because the institution had not given the complainant timely access to his or her personal information. Where we did not substantiate a complaint, it was typically because the institution had properly applied one or more of the exemptions that allow it to withhold personal information under the *Privacy Act*.	**5.1.4**

Of the 570 complaints we closed in all, 101 related to concerns about the collection, use, disclosure, retention or disposal of personal information. The circumstances ranged from the egregious to the banal.	**5.1.4**
One noteworthy case involved Veterans Affairs Canada, where we learned that a large quantity of the complainant's sensitive personal information, including medical information, had found its way into briefing notes prepared for the then-Minister of Veterans Affairs. In advance of the complainant's participation in a Parliament Hill press conference, for instance, the Minister was briefed about the complainant's medical history, recommended treatment plan, and the level of veteran's benefits he received. The personal information was, moreover, widely shared among Departmental officials who would normally need little or no access to the man's medical information in order to fulfill their duties. We upheld the complaint as well founded. As the investigation revealed serious systemic issues, we decided to launch a full audit of the Department in 2011-2012.	**3.1**
Other privacy violations were far less glaring, but no doubt still troubling for the individuals involved. We found several instances in which the personal information of Canadians was mishandled by public employees — left exposed in public places, abandoned on a bus, or shipped through a prison's internal mail system without benefit of an envelope.	**4.1.1** **4.1.2** **4.1.4**
We also raised questions about the way Canada Post gauges the validity of requests for special paid leave to care for an ailing relative. We concluded that the organization asks for more information than necessary, including some about third parties.	**2.4.1**
In addition to complaints from individuals, we received 64 reports from departments and agencies, detailing instances in which they had inappropriately disclosed the personal information of Canadians. Institutions are required by Treasury Board policy to report such data breaches to our Office in a timely manner, and more reports than ever reached us during the past fiscal year.	**4.2**

Here again we found that many of the incidents were caused by sloppiness — binders left on public transit and airplanes, typos on address labels, and documents faxed to the wrong office. As in every other year, we once again discovered that the processing of requests under the *Access to Information Act* and the *Privacy Act* can lead to the inadvertent release of personal information that should have been protected.	**4.2**
In one unusual incident, Human Resources and Skills Development Canada noted that its brand new online portal for Service Canada had a technical glitch that enabled users to view financial and other personal information of previous visitors to the site. An internal investigation concluded that only 75 of the 85,000 people who had used the site on its first day of operation had been affected by the technical failure. The probe traced the problem to a feature of the underlying architecture, called Access Key, and disabled the feature. The Department continued to work with Bell Canada, which provides the Access Key service for the government, to find a permanent and reliable technical solution.	**4.2.6**
We also report this year on the disclosures that were made under section 8(2)(m) of the *Privacy Act*, which allows government departments and agencies to disclose personal information if it is clearly in the greater public interest, or clearly in the interests of the individual concerned. In all there were 80 such disclosures, the vast majority of them by the Department of Foreign Affairs, the Correctional Service of Canada and the RCMP. Typical examples included advising a community before an offender is released from prison, informing provincial health officials when airline passengers may have been exposed to a traveller with tuberculosis, or passing along warnings about professionals with disciplinary or other problems.	**4.5**

Privacy Impact Assessment Reviews	
We reviewed 87 Privacy Impact Assessments in 2010-2011, 19 of them in greater depth because of the significance of the privacy risk or the broader human rights or societal issues involved. Departments and agencies are required to submit such assessments to our Office to demonstrate that they have considered the privacy ramifications of proposed programs or activities, and planned for ways to mitigate intrusive impacts.	**2.3**
One of our reviews examined a plan by the Canadian Air Transport Security Authority to observe passengers in the airport pre-boarding areas for suspicious behaviour. We expressed several concerns, including the potential for inappropriate risk profiling based on characteristics such as race, ethnicity, age or gender.	**2.3.2**
Another Privacy Impact Assessment we reviewed was submitted by Citizenship and Immigration Canada and related to the use of biometrics to identify all non-Canadians entering Canada. We made a number of recommendations to better safeguard the data and ensure it is shared with other nations only under the most stringently controlled circumstances.	**2.3.3**
We also continued to review a series of Privacy Impact Assessments related to a large-scale and evolving project that enables the sharing of investigative information collected by the RCMP and provincial, territorial, aboriginal and municipal police forces — amongst themselves and with federal government departments. The data-sharing structure is called the National Integrated Interagency Information System, or N-III. Some of the information that can be accessed through this structure may be subjective, or indicate no wrongdoing at all. We noted that, if it is used without the appropriate context and safeguards, the information could result in detrimental outcomes for innocent individuals. We recommended safeguards and controls for this information sharing, as well as greater transparency and accountability.	**4.3**

Policy and Parliamentary Affairs	
We made 15 appearances before Parliamentary committees over the past fiscal year, and all but one of them dealt with public-sector issues. We weighed in on matters such as open government, child sexual exploitation and the long-form census. We outlined the priorities of the Office as Commissioner Stoddart's leadership as Commissioner was renewed for another three years. Aviation security was an area of particular and ongoing concern, in light of legislative measures such as the Advance Passenger Information/Passenger Name Record program, the Passenger Protect Program, and America's Secure Flight Program. These measures have resulted in the creation of massive government databases, the use of secretive no-fly lists, the increased scrutiny of travellers and airport workers, and greater information sharing with foreign governments. During our Parliamentary committee appearance on aviation security, we underscored the importance of transparency, minimizing data collection, setting limited retention periods, and establishing robust and accessible redress mechanisms.	3.5 5.2
Another ongoing concern related to lawful access legislation, in which the government looks for ways to strengthen the capacity of police and security agencies to gain access to data associated with citizens' electronic communications. Commissioner Stoddart joined with provincial and territorial counterparts to write to the Deputy Minister of Public Safety Canada, outlining the privacy risks that they see emerging from the government's intention to amend the legal regime governing the use of electronic search, seizure and surveillance.	2.6.2

Supporting Public Servants	
Canadians count on the government to handle their personal information with the utmost care and professionalism. But government isn't a single monolithic entity; it's tens of thousands of individuals who generally try their best to live up to the requirements of the *Privacy Act*.	5.3

Recognizing the challenge for public servants operating under extraordinary pressure to collect and manipulate data, we sought in 2010-2011 to provide practical assistance through workshops, seminars and other outreach activities. In March, for instance, we hosted our inaugural Privacy Practices Forum, an opportunity for civil servants to learn and share knowledge about ways to advance privacy in their respective departments.	**5.3**
We also invested a great deal of effort over the past year in helping institutions adapt to a new government Directive on the completion of Privacy Impact Assessments. We held a second annual workshop to guide more than 100 participants in the preparation of solid Privacy Impact Assessments. During the workshop, we launched a detailed guidance document that sets out what we expect from such assessments. Entitled *Expectations: A Guide for Submitting Privacy Impact Assessments to the Office of the Privacy Commissioner of Canada*, the document was distributed across the public service and is available on our website.	**5.3.1**
Our Office also drew on the advice of a wide spectrum of experts in both privacy and security to develop a reference document to help policymakers, practitioners and citizens integrate privacy protections with new public safety and national security objectives. Entitled *A Matter of Trust: Integrating Privacy and Public Safety in the 21st Century,* the document provides important context, as well as step-by-step guidance on achieving the appropriate balance.	**2.6.1**
Another area where we offered our guidance related to the increasing use of biometric information, such as fingerprints and facial images. Biometric systems can contribute to highly reliable and robust identification systems, but can also raise significant privacy challenges, including the covert collection of biometric characteristics, cross-matching, and the unwanted disclosure of secondary information embedded in an individual's biometric information.	**2.7**

To help institutions weigh the pros and cons, our Office prepared a detailed primer called *Data at Your Fingertips: Biometrics and the Challenges to Privacy*. It introduces a method for determining the appropriateness of biometrics for different applications, and makes recommendations for privacy-sensitive designs.

2.7

Advancing Knowledge

The *Privacy Act* affords us no explicit public education mandate, but that doesn't stop us from reaching out to the people we serve to help them better understand their privacy rights and how to protect their personal information.

In the past year, for instance, we participated in 20 exhibits and other offsite promotional activities, distributed 34,000 publications, delivered 112 speeches, and hosted 32 stakeholder visits. Our websites and Office blogs remain popular vehicles for the dissemination of information, with 3.23 million distinct visits over the past fiscal year.

Privacy by the Numbers

We are also working hard to advance the state of knowledge about privacy and the emerging threats to personal information.

Toward that end we commissioned research on such matters as key issues of concern for officials in access-to-information and privacy branches of federal institutions; privacy and data-collection laws and practices in developing countries; and the privacy impact of new technologies for authenticating identity in online payment systems.

5.5.1

CHAPTER 2

Data Diet

Can the State Curb its Appetite for Information about its Citizens?

Asked in 1924 why he felt compelled to scale Mount Everest, British climber George Mallory is famously reported to have quipped: "Because it's there."

The same logic appears to be driving many organizations the world over as they rush to scoop up veritable mountains of personal information. Information is power, so wouldn't it be a shame to leave any byte unclaimed? Data, it seems, is good; more of it still better.

The Government of Canada, already the nation's single biggest repository of personal information, is not immune to this impulse. Personal data is the oxygen that the state needs to govern. Without it there can be neither revenues nor entitlements; no peace, order or good government.

And yet, there are limits. Sections 4 to 6 of the *Privacy Act* specify the terms under which federal departments and agencies may collect, retain and dispose of personal information.

In general, the government can only collect personal information if it relates directly to an operating program or activity. Wherever possible, the data should be collected from the individual to whom it relates. With some specific exceptions, the individual should be informed about the purpose of the collection.

Once the information was used for its intended purpose, there are limits to how long it can be retained, and rules for how it must be disposed of.

MINIMIZING COLLECTION

Without a doubt, the digital era has made it far easier for organizations to collect everything, rather than to sift, sort, and jettison what's no longer needed.

But ease and convenience are no justification for the excessive collection or retention of personal information. Indeed, the statutory limitations set out in the *Privacy Act* have both a practical and a philosophical rationale.

Curbing the volume of personal data in the hands of government lessens the chances of accidental disclosures, and of errors or omissions that can lead to wrongheaded decisions, often with dire consequences for the affected individual.

Moreover, people have a fundamental right to live their lives in peace and anonymity, free from the prying eyes of the state. This is the foundation for the trust that must exist between citizens and their government, an expression of the social contract that defines an enlightened nation.

This chapter explores what we learned in 2010-2011 about the government's stewardship of personal information, including its collection, retention, secure storage and disposal. It includes the following sections:

2.1 Audit of the Canadian Air Transport Security Authority

Every year, tens of millions of travellers pass through Canadian airports. As a condition for boarding a flight, they and their baggage must undergo some form of security screening measures.

It is widely accepted that screening contributes to passenger safety, and our Office does not dispute this. We do, however, believe that security and privacy are not opposing values; an increase in one does not necessitate a loss of the other.

On the contrary: We take the view that a strong framework of control over the management of the personal information of passengers will mitigate privacy risks while, at the same time, also strengthening aviation security.

That is the context in which we examined whether the Canadian Air Transport Security Authority (CATSA), the federal organization charged with screening passengers and luggage, complies with the information-handling requirements of the *Privacy Act*.

About the Canadian Air Transport Security Authority

Established as a Crown corporation in April 2002 in response to the Sept. 11, 2001 terrorist attacks on the United States, CATSA's mandate is to screen passengers, flight crews, baggage handlers and maintenance staff for prohibited items.

CATSA reports that as of March 31, 2010 it had 530 employees and 6,790 contract personnel serving as screening officers. In an average year, they screen 48 million passengers and 62 million pieces of luggage at 89 Canadian airports.[1]

WHAT WE FOUND

2.1.1 FULL-BODY SCANNERS

Full-body image scanners, present in many Canadian airports, detect concealed explosives or weapons through a traveller's clothing.

CATSA has implemented a strong framework to protect passengers' privacy. It includes controls to ensure that an image cannot be linked to a name or any other identifiable information about the passenger. Scanned images are sent electronically to a remote viewing room to ensure that the screening officer cannot view or identify the passenger.

---

[1] Canadian Air Transport Security Authority. (2010). *Stepping Forward: Annual Report 2010*. Retrieved from http://www.catsa.gc.ca/File/Library/87/English/AnnualReport2010.pdf

The images, moreover, cannot be retained or printed, and are permanently deleted once the passenger has been screened.

We did, however, find that procedures to protect privacy are not consistently followed. For example, the image-viewing officer is supposed to ensure that images are cleared from the screen before anyone enters or leaves the room. We observed instances where this did not happen.

We also witnessed an official inside the image-viewing room with a cellphone, which is strictly prohibited because such devices often have video-recording capabilities.

Further, we located a closed-circuit television camera in the ceiling above the viewing room at one airport. The camera was disabled after we brought the matter to CATSA's attention.

Given the privacy concerns surrounding the use of full-body imaging technology, we recommended that CATSA ensure that privacy safeguards are understood, enforced, and subject to ongoing compliance monitoring. We also recommended a physical inspection of all viewing rooms and the disabling of any closed-circuit television cameras.

2.1.2 COLLECTION OF PERSONAL INFORMATION

CATSA's governing regulations and related orders require the organization to notify authorities if its screening activities detect a threat to aviation safety. It therefore quite properly collects the personal information of travellers found to be carrying a concealed weapon, explosive, incendiary device or other threat to aviation security, so that the incident can be reported to the appropriate authorities.

Potentially illicit activities

There are also occasions when a search for aviation threats inadvertently turns up evidence of other activities, such as an apparent attempt to import narcotics or to export large sums of money. While the smuggling of drugs or money is illegal, it is not a direct threat to aviation safety.

In such circumstances, CATSA's practice is to detain the suspect and to alert the appropriate police or other law enforcement authorities.

However, we also determined that once local law-enforcement authorities have been called, CATSA's involvement in the incident ends. Thus, CATSA's practice of writing up incident reports on illicit activities that pose no direct threat to aviation safety is inappropriate.

Accordingly, we recommended that the organization restrict its collection of personal information to aviation security incidents.

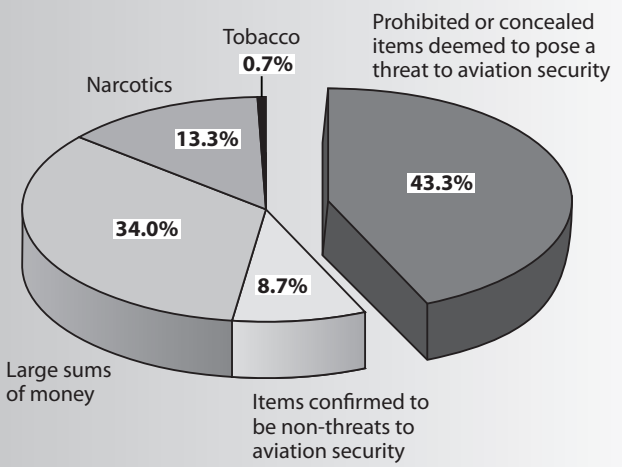
Domestic transport of cash

We also found that CATSA collects personal information about domestic travellers carrying large sums of cash, and passes this along to police once the passenger has left the screening area.

It is not an offence to travel within Canada with large amounts of money. By permitting the individual to proceed through screening, it is evident that the cash does not constitute a threat to aviation security, which places it outside CATSA's mandate.

We were told that CATSA has more than 10,400 incident reports on file. We extracted an exploratory sample of 150 reports for examination. As shown in the chart, approximately 57 percent of the reports concerned matters unrelated to aviation security.

BREAKDOWN OF SAMPLE INCIDENT REPORTS BY TYPE



On the basis of our analysis, we concluded that CATSA is collecting personal information beyond its legislative mandate. Mindful of the size of our audit sample, however, we cannot determine the extent to which CATSA's information holdings contain reports that should not be there.

We recommended that CATSA implement measures to ensure it collects only personal information that is directly related to aviation security.

2.1.3 ELECTRONIC BOARDING PASS AUTHENTICATION SYSTEM

As part of its pre-boarding activities, CATSA must verify the authenticity of boarding passes. A Boarding Pass Security System was introduced in 2009 to facilitate this process. It captures information printed on the boarding pass, as well as other data, in a special bar code.

While there may be a need to temporarily display the contents of the boarding pass bar code so that the screening officer can match the information with what is printed on the boarding pass, we questioned the necessity of collecting and retaining personally identifiable information in the system's database.

Indeed, while the system was implemented to detect fraudulent boarding passes, CATSA is using the data (specifically passenger names) for other purposes. These include responding to passenger claims and complaints, as well as security incidents and breaches (for example if a person enters a restricted area without having been screened).

As a general rule, passengers' personal information should not be collected on the basis that it may have some future use. CATSA was able to demonstrate that the collection of personal information derived from a boarding pass and bar code is necessary to fulfill its aviation security mandate. However, passengers are not informed that the data was being retained for 30 days, or that the information may be shared with CATSA's foreign counterparts to address matters relating to aviation security.

We urged CATSA to more clearly inform passengers of the purposes for which the data is collected, the uses that are made of it, with whom and under what circumstances the information may be shared, and how long it is kept.

2.1.4 DISCLOSURE OF PERSONAL INFORMATION

Disclosure to authorities

CATSA is obliged to report aviation security incidents to specific authorities, including the Minister of Transport, the Canada Border Services Agency (CBSA), or the appropriate air carrier, police service or airport authority.

CATSA is not empowered to search for contraband. However, it will contact authorities when illegal narcotics or large sums of money are discovered during the screening process, and share the passenger's name, flight information and a description of the alleged contraband.

We considered whether CATSA has the authority to contact the police or the CBSA about incidents that are unrelated to aviation security. For the purposes of the *Privacy Act*, the authority rests on whether such disclosures can be considered "a use consistent with the purpose" for which the information was obtained.

Under its mandate, CATSA obtains personal information for the purpose of screening individuals and their baggage for prohibited items and threats to aviation security. At times, officers stumble upon other kinds of illicit items, such as street drugs or smuggled money.

Determining whether disclosing information about such discoveries to the police or other authorities is a consistent use under the Act turns on whether individuals can reasonably expect CATSA to notify somebody when, in the course of carrying out their mandated duties, officers stumble upon illicit items outside of this mandate.

In our view, it is reasonable for an individual to expect that CATSA would notify the appropriate authorities when apparently illegal items are inadvertently discovered. While individuals are only consenting to a search of their person and baggage for threats to aviation safety, it would be unreasonable to expect that clear evidence of other illegal items would be ignored.

Indeed, passing such information to police ties directly to the original purpose for which the information was obtained — for public safety and compliance with the law in the context of aviation security. By contrast, as explained in section 2.1.2, it is not an offence to travel within Canada with large amounts of cash. Therefore, there is no reason why CATSA would need to alert authorities if it finds such cash during its screening activities.

To bring its disclosure practices into compliance with the* Privacy Act*, we recommended that CATSA stop notifying police when it discovers a large sum of money in the baggage of a person travelling domestically.

Disclosure to air carriers

Aside from informing police about incidents unrelated to aviation security, we also found that CATSA conveys personal information to airline carriers. This may not always be appropriate.

For instance, while it may be appropriate to notify an airline if a passenger will be delayed at the security checkpoint, there is no need to disclose specifics, such as contraband having turned up in the individual's baggage.

We called on CATSA to ensure that all disclosures to airline carriers are limited to that which is necessary in the circumstances of each case.

2.1.5 INFORMATION PROTECTION AT AIRPORTS

CATSA has outsourced passenger screening to 11 private-sector companies. Each contract includes a confidentiality agreement, which establishes the contractor's obligations for safeguarding passenger information.

During our site visits to airports, however, we found deficiencies in this regard. We observed incident reports on open shelving units, on the floor, and in cabinets that did not meet required security specifications. At one airport we found reports stored in boxes in a room used to conduct private searches on passengers.

The confidentiality agreement requires screening contractors to protect records in accordance with CATSA's Document Protection Procedures, which outline the storage and transmission requirements for information designated either 'protected' or 'secret'.

The agreement states that CATSA will identify all information falling within either of the two categories. CATSA had not, however, done so at the time of our audit, which could have contributed to some of the storage deficiencies we observed.

We recommended that CATSA apply a security designation to personal information that is commensurate with the sensitivity of the information. Screening contractors should implement physical security measures that comply with Treasury Board standards.

We also found that CATSA does not systematically inspect or audit contractors' handling of passenger information. The organization has been guided by the assumption that screening contractors are managing information appropriately, but with no assurance that this is so.

In the absence of an effective monitoring regime, contractors may circumvent their privacy obligations without consequence.

We recommended that CATSA ensure that screening contractors' management of passengers' personal information is subject to regular inspection and audit.

2.1.6 RETENTION AND DISPOSAL OF PERSONAL INFORMATION BY CATSA

In the event of a security incident or breach, CATSA typically collects the passenger's name, flight information, address, phone number and a summary of the event. The report is faxed to CATSA's Security Operations Centre in Ottawa and then entered into the Call and Incident Data Collection System, the electronic repository for security incident reports.

Federal institutions are required by law to develop retention and disposal schedules to manage their records. These schedules establish how long records will be kept before they are destroyed or transferred to the control of Library and Archives Canada. A records retention and disposal schedule is important from a privacy perspective because holding on to records for too long may result in prejudice against the individual concerned.

We found that CATSA had not developed a retention and disposal schedule for personal information under its control. As a result, security incident reports were held at CATSA's head office indefinitely.

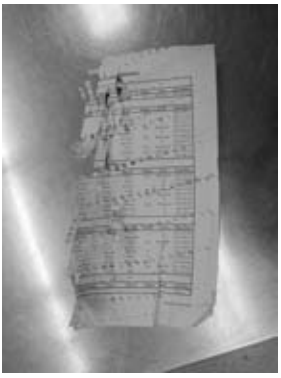
We recommended that CATSA permanently delete all electronic and hard copy records that it does not have the authority to collect. These would, for instance, relate to the incidental discovery of contraband, items that were wrongly identified as threats to aviation security, and large sums of money carried by passengers.

CATSA should also establish a records retention and disposal schedule for personal information collected under its aviation security mandate.

2.1.7 RETENTION AND DISPOSAL OF PERSONAL INFORMATION BY CONTRACTORS

CATSA's contracts with screening providers are silent on disposal requirements, leaving it up to screening contractors to develop and manage the process. We learned that incident reports are typically held for one year, then destroyed in on-site shredders or by private-sector shredding companies.

We collected a sample of shredded material at one of the airports that handled its own document shredding. We found the papers were not destroyed according to the standard set by Treasury Board. While there is insufficient evidence to suggest a systemic problem, it does underscore the importance of monitoring disposal practices.



Sample of document still legible after shredding

However, we found that CATSA has no audit protocol under which it can monitor records destruction by off-site shredding services. Consequently, there is no assurance that individuals who handle the personal information of passengers are screened to the appropriate security level, that incident reports are destroyed in a way that they cannot be reconstructed, and that records are disposed of in a timely fashion that mitigates the risk of unauthorized access.

We recommended that CATSA ensure that all contracts for the disposal of personal information comply with Treasury Board requirements and implement a protocol for monitoring off-site destruction practices.

2.1.8 OTHER SAFEGUARDS ARE IN PLACE

Our audit revealed that other important safeguards are in place to protect personal information. Notably:

- CATSA's head office is controlled by various measures, including security guards, closed-circuit television cameras and an intrusion detection alarm system. Electronic access control cards, biometric identifiers and security cabinets restrict access to the premises and records. We found no evidence to suggest that personal information could be compromised through inadequate physical security controls.

- CATSA operates a private network that connects its head office, airports and data centres. We reviewed the network architecture and found adequate measures to protect personal information. These included firewalls, intrusion detection and prevention technologies, automated software patch management, and access controls. Threat and risk assessments have been completed and annual penetration tests are performed to identify and remedy potential weaknesses.

- We found that data extracted from a boarding pass bar code is transmitted by a secure network to a local server, and then to a central database. CATSA has implemented controls to protect data in transmission. Moreover, personal information stored in the database is encrypted.

- Third-party service agreements include sound privacy provisions. For instance, personal information must be stored in Canada; security and physical measures must accord with Government of Canada security standards; information cannot be used for secondary purposes; and any individual with access to the database must have a secret security clearance.

- CATSA has installed closed-circuit television to observe and record passengers from the time they enter the screening waiting line until they have been processed by screening officers. We found that there are appropriate controls over access to, use, retention and disclosure of the video footage. Indeed, CATSA told us it will not release a copy of the footage unless compelled to by a warrant or court order.

2.1.9 TRANSPARENCY

Federal institutions are obliged to describe their personal information holdings in *Info Source*, an index published by the Treasury Board Secretariat. However, we found that the current edition of *Info Source* is silent on CATSA's collection of passenger information.

We also found a lack of transparency about the use of closed-circuit television in passenger screening areas. Only four of the eight airports we visited had signage visible to passengers, and it only stated that the area *may* be monitored. We confirmed that the cameras continuously record passenger movement.

We also observed that passengers were not always informed of their options when subjected to a physical search.

Passengers referred for supplementary screening have the option of a full-body image scan, a physical pat down in public view, or a physical pat down in a private area such as a partitioned stall or separate room. However, in observations at five airports, we found that travellers were typically asked to choose between a full-body scan and a pat down in public view; the option of a hand search in private was seldom offered.

***We recommended that CATSA describe all categories of personal information under its control in the next edition of* Info Source.**

In the spirit of transparency, the organization should also ensure that passengers are advised that they are being monitored by closed-circuit television and that there are three options for secondary physical searches.

2.2 Audit of Selected RCMP Operational Databases

2.2.1 OVERVIEW

Canada's law enforcement and criminal justice community relies on an extensive network of database systems to help enforce laws, prevent and investigate crime, and maintain peace, order and security.

For the purposes of our audit we looked at two of several databases that the Royal Canadian Mounted Police (RCMP) uses for its policing and crime-prevention operations. Both share information with a broad range of public safety partners.

- The ***Canadian Police Information Centre*** (CPIC) offers computerized storage and retrieval of information on crimes and criminals. CPIC holds more than 10 million records that relate, for example, to driver's licences and vehicle plates, stolen vehicles and boats, warrants for arrest, missing persons and property, criminal history records, fingerprints, firearms registration, and missing children.

  More than 80,000 law enforcement officers in more than 3,000 police departments, RCMP detachments and federal and provincial agencies can connect to the central computer system through CPIC. Courts, parole boards and government departments and agencies, such as the Correctional Service of Canada, the Canada Border Services Agency, Canada Revenue Agency and Passport Canada, also use CPIC.

  About the Mounties

  With approximately 30,000 employees, the RCMP enforces federal laws across Canada and provides investigative and operational support services to more than 500 Canadian law enforcement and criminal justice agencies. It also provides policing services in all provinces except Ontario and Quebec, as well as in the three northern territories and nearly 200 municipalities.

  Information contained in CPIC is shared internationally via INTERPOL, and with American law enforcement agencies such as U.S. Customs and Border Protection.

  Even the Insurance Bureau of Canada, the national industry association for the property and casualty insurance market, has access to CPIC.

  CPIC processed more than 200 million queries through 40,000 access points in 2009.

- The ***Police Reporting and Occurrence System*** (PROS) is the RCMP's operational records management system. Introduced in 2003, PROS is used by the RCMP and 23 police partner agencies, typically those with fewer than 300 officers that do not have their own electronic records management system.

  PROS contains information on any individual who has come into contact with police, whether as a suspect, victim, witness or offender, from initial occurrence to the final disposition of the case. About 1.6 million occurrence files are processed every year.

Under powers vested in our Office through the *Privacy Act*, we audited the RCMP's compliance with the Act's requirements on the collection, protection, retention and disposal of personal information in CPIC and PROS.

In particular, we examined:

- the RCMP's policies and procedures governing access to and use of CPIC
- policies and procedures related to the removal of personal information contained in PROS that is no longer required
- the RCMP's practices for reviewing compliance with the terms and conditions of use for both CPIC and PROS and
- the management of user access to PROS.

How the systems are used

An RCMP officer stops a car for speeding. She then uses her in-car computer to run a query in CPIC to see whether the detained vehicle is stolen or whether there are outstanding warrants on the driver. The officer might then search PROS, in case the vehicle or driver has been involved in prior incidents. An occurrence record is created in PROS to record the event. The record is subsequently updated as the case develops.

We did not examine how the personal information contained in these databases is actually used. Nor did we look at the data-protection safeguards applied by municipal, provincial, territorial and international partners who have access to the data through formal information-sharing arrangements.

2.2.2 WHY THIS ISSUE IS IMPORTANT

Both CPIC and PROS contain extensive amounts of sensitive personal information that, if improperly used or disclosed, could have significant impacts on the reputation, employability and personal safety of affected individuals. A security breach could also compromise ongoing police investigations.

The RCMP reports annually on security breaches of the CPIC system. Some of these breaches have involved unauthorized access to, or inappropriate use of, the personal information of others.

The RCMP has also found that certain police agencies contravened CPIC policy by disseminating to employers the details of convictions, discharges or pardons of a prospective employee, without the informed consent of the individual.

The RCMP is responsible for the storage, retrieval and communication of shared operational police information on behalf of accredited criminal justice and other partner agencies. It has an obligation to protect the privacy of individuals with respect to the personal information in its care.

2.2.3 WHAT WE FOUND

Canadian Police Information Centre (CPIC)

- **Policies and procedures**

The RCMP has policies and procedures in place to govern access to and use of data in the CPIC database in a way that protects the personal information of Canadians. Among other things, the risk-mitigation strategy for information technology requires agencies to implement strong identification and authentication protocols to ensure that all users are legitimate.

However, we found that one-third of agencies had constraints on their technical infrastructure that impeded them from putting such protocols in place.

We also looked at the Memoranda of Understanding (MOUs) that the RCMP uses to set out the terms under which agencies may use the CPIC database. MOUs were in place with agencies that had limited law-enforcement powers, or roles that are complementary to law enforcement.

However, at the time of our audit, MOUs had yet to be signed with approximately 25 percent of police agencies that had previously been granted access on the basis of their core policing role.

We recommended that the Canadian Police Information Centre set clear timeframes to establish MOUs containing privacy provisions with any entities where such agreements do not already exist.

- **Breaches**

Our audit established that privacy breaches have occurred but are relatively rare. Mechanisms are in place to investigate them and to act on the results of those investigations.

Many of the breaches involved people querying CPIC for personal reasons. The RCMP also recently discovered that certain police agencies were passing criminal record information from the CPIC system to employers. The data related to convictions, discharges or pardons, and was disseminated without the informed consent of the prospective employee.

Depending on their severity, data breaches can lead to a directive from the RCMP, a change in CPIC policy, a reprimand, a suspension, or a dismissal.

Police Reporting and Occurrence System (PROS)

- **Information purging**

Legislation requires that all records created in PROS be purged when the retention period for each category of information has expired. Unless records are purged, they remain readily accessible.

Prior to deletion, records are evaluated to determine whether they should be archived with Library and Archives Canada. We found that the PROS database was designed to automatically purge occurrences once they reach their disposition date, unless they have archival value.

But while the functionality to purge exists, we found that the RCMP has disabled it in order to extract some statistical information.

An organization that retains personal information longer than required is in contravention of the* Privacy Act. *We therefore recommended that the RCMP purge the data necessary to bring it into compliance with the Act.

The RCMP responded that it assigned staff to develop a statistical solution and, once implemented, the appropriate data will be purged as required by legislation.

While examining purging procedures mandated by law, we also found that the RCMP had not yet implemented processes to remove access to records related either to pardoned offences or wrongful convictions. In the event of a pardon or a wrongful conviction, the related records are supposed to be sequestered and should no longer be accessible in PROS.

It is important to Canadians who have received a pardon that the information not be inappropriately disclosed so they can enjoy the same opportunities to get a job, travel, study and volunteer as any other Canadian. The *Canadian Human Rights Act* prohibits discrimination based on a pardoned criminal record. Such freedom from discrimination is doubly important if a person has been wrongfully convicted.

To mitigate the risk of an unlawful or inappropriate disclosure, we recommended that the RCMP implement processes to remove access to records in the PROS database that relate to pardoned offences and wrongful convictions.

- **User access and activity**

RCMP policy requires that a user's access to PROS be revoked when access is no longer required for the user's job function, or if the user has not accessed the system for 14 months.

The RCMP was, however, unable to demonstrate that it systematically reviews PROS use to ensure it accords with governing policies.

Indeed, we found that there is no active monitoring of PROS user accounts and activity. We noted that there were more than 1,000 accredited users who had not accessed PROS in 14 months or more.

We also found that PROS is technically able to track a user's actions in audit logs. The information records details on which records were viewed and any modifications made.

However, the RCMP informed us that, if misuse by a user is suspected, the level of effort required to consolidate and review the audit logs limits the ability to investigate. While an automated audit log review tool is available within PROS, it has not been implemented to date. As a result, it is highly labour-intensive to extract any details of a user's activity, and thus to investigate potential misuse.

We recommended that the RCMP regularly review the status of PROS user accounts, and disable access when it is no longer required for users to perform their jobs.

In order to aid in the investigation of unauthorized access to personal information stored in PROS, we further recommended that the RCMP enable the audit log review tool.

- **Compliance audits**

We found that the RCMP has Memoranda of Understanding (MOUs) with all partner agencies to ensure that the data in PROS is used only for legitimate law enforcement purposes.

The MOUs, which remain in effect for five years unless terminated for cause, give the RCMP the power to monitor the use of its networks and specific employee use, and periodically to conduct on-site visits to police partner agencies.

The RCMP was unable to demonstrate, however, that it systematically engages this power to ensure that police partner agencies are using the personal information contained in PROS in accordance with the governing terms and conditions of the MOUs.

Indeed, few audits have occurred. While all police partner agencies in Alberta have been audited, for instance, the same was true for only a handful in Nova Scotia and none at all in Prince Edward Island.

We recommended that the RCMP adopt a consistent and regular review process to ensure that all users are complying with the policies and procedures governing the use of the personal information in PROS.

The RCMP committed to addressing all the concerns raised in our audit.

2.3 Privacy Impact Assessments Involving the Collection of Personal Information

2.3.1 OVERVIEW

Privacy Impact Assessments are important tools to help federal institutions examine the privacy effects of new or significantly modified programs or activities.

One reason that Privacy Impact Assessments are so valuable is that they encourage government institutions to consider the privacy impacts of proposed initiatives early in the development process.

Optimally, the Privacy Impact Assessment process should help government institutions justify privacy-invasive programs and activities against a four-part test: Is the project absolutely necessary? Is it likely to be effective in achieving its objectives? Is the project's anticipated infringement on privacy proportionate to any potential benefit to be derived? And are less intrusive alternatives available?

When the four-part test has been met, government institutions must still demonstrate that the information that was collected will be protected. We therefore also encourage proponents to consider the 10 internationally acceptable fair information principles for the stewardship of personal information. Among other things, these principles call for data collection that is minimized and appropriate, and for mechanisms to ensure it is secure, so as to lower the risk of future privacy invasions.

New Directive

On April 1, 2010 the Treasury Board Secretariat (TBS) Directive on Privacy Impact Assessment replaced the Privacy Impact Assessment Policy that had been put in place in 2002. While the Directive differs somewhat from the earlier Policy, federal institutions are still required to conduct Privacy Impact Assessments early in the development of initiatives that pose threats to privacy, and to submit them to our Office.

While we read and assess all files we receive, we conduct more in-depth reviews where, in our view, programs or activities pose significant privacy risks or raise broader human rights or societal privacy issues. For these, we provide departments with detailed recommendations, and follow up to ensure risks have been mitigated.

We do not approve assessments or endorse any projects or proposals during our reviews. Our recommendations and advice on how projects can be improved are intended to better safeguard the privacy of Canadians. While institutions are not obliged to heed our

advice or implement our recommendations, we do find that most are open to our input and work with us to resolve or mitigate privacy concerns.

We received 52 Privacy Impact Assessments during the past fiscal year, down significantly from the 102 submissions we received the year before. The reason for this decrease is not clear; it could be that institutions are taking time to implement new procedures under the new Directive. It is also possible that the spike in submissions in 2009-2010 was due to institutions completing Privacy Impact Assessments under the old Policy.

We applied a triage process in order to focus our resources on files of the highest priority. Thus, we reviewed 19 files that we determined related to projects posing the highest risk to privacy. Another 68 lower-risk files were also examined.

You will find below descriptions of several initiatives for which we reviewed Privacy Impact Assessments over the past fiscal year, along with summaries of our advice and any continuing concerns.

The review process is intended to be iterative and evergreen, so we often review and offer guidance on several versions of Privacy Impact Assessments as initiatives mature from inception to implementation.

2.3.2 CANADIAN AIR TRANSPORT SECURITY AUTHORITY

Passenger Behaviour Observation Program

We received a preliminary Privacy Impact Assessment from the Canadian Air Transport Security Authority (CATSA) for the Passenger Behaviour Observation (PBO) Pilot Project.

PBO is an airport screening measure in which passengers in the pre-boarding security screening lineup are observed for suspicious activity.

PBO-trained CATSA officers may approach passengers and engage them in a brief conversation, and ask to see their identification and travel documents. Depending on the outcome of the conversation, passengers may be directed to secondary screening.

Following each interaction, PBO officers fill out a case card, which describes the incident and the passenger's appearance, but contains no personally identifying information such as names or addresses.

Our concerns

In reviewing CATSA's Privacy Impact Assessment, we were concerned about the effectiveness of this initiative in identifying threats to aviation security. We questioned its necessity, in light of the many other security procedures and programs already in place.

In particular, we noted the potential for inappropriate risk profiling, based on characteristics such as race, ethnicity, age or gender.

We also commented that CATSA appears to be moving towards identity-based screening, representing a significant shift in operations that have previously focused on screening for objects posing a risk to aviation security.

We were further concerned that the details of the PBO pilot were authorized by an Interim Order under the *Aeronautics Act*, rather than prescribed by regulation. Under the Act, the Minister of Transport may issue interim orders if immediate action is required to deal with a serious threat or a significant risk to aviation security. These orders are made without Parliamentary debate or other public input. It does not seem to us that an ongoing program such as PBO falls into this category.

Our recommendation

We recommended that initiatives such as PBO be authorized by regulation rather than through interim orders. Regulations are published in the* Canada Gazette *for public scrutiny and comment. We feel this would promote a more open and transparent process, and lead to better scrutiny of a potentially privacy-intrusive measure.

In the meantime, CATSA has posted signs to notify passengers that they may have to show identification at screening checkpoints, and has assured us that interactions with passengers in the screening line are conducted as discreetly as possible.

CATSA also invited our staff to visit the pilot project at the Vancouver International Airport in June 2011 to more fully assess the program.

2.3.3 CITIZENSHIP AND IMMIGRATION CANADA

Five Country Conference High Value Data Sharing Protocol and Temporary Resident Biometrics Project

The Government of Canada is moving towards the use of biometrics to identify all non-Canadians entering Canada. The initial focus is on people who are required to get visas as visitors, students or temporary workers, as well as on refugee claimants and immigration enforcement cases.

Citizenship and Immigration Canada has asked us for privacy advice on two initiatives involving the collection and use of biometric identifiers, such as fingerprints and digital photographs, for immigration controls. The initiatives involve the Department, the Canada Border Services Agency and the RCMP.

- Under the Five Country Conference High Value Data Sharing Protocol, biometric information required for immigration screening is shared between Canada, Australia, New Zealand, the United Kingdom and the United States.

- Under the Temporary Resident Biometrics Project, scheduled for a phased rollout in 2013, visitors, temporary foreign workers and students applying for visas will be required to enroll abroad with 10 fingerprints and a digital photo. This data will be checked against the enrolled template when the individual arrives at a port of entry to Canada.

Our recommendations

With respect to both initiatives, we called on Citizenship and Immigration Canada to ensure that:

- ***the use of biometrics is both necessary and effective in detecting and preventing fraud;***
- ***sharing of this sensitive information, particularly for vulnerable individuals such as refugee claimants, be undertaken with caution and under strict safeguards and protocols;***
- ***particular attention be paid to safeguarding fingerprints, photos and foundation documents collected by private-sector Visa Enrollment Centres abroad; and***
- ***the criteria for sharing biometric information with other nations be developed carefully and limited to the most serious cases.***

2.3.4 PUBLIC SERVICE COMMISSION

Political Impartiality Monitoring Approach

In last year's annual report, we discussed our concerns about the Public Service Commission's Privacy Impact Assessment for a program that would cross-reference government databases of current and former public servants with candidate lists in federal, provincial and municipal election campaigns.

According to the information we received, the Political Impartiality Monitoring Approach was also intended to monitor the Internet, including media outlets, personal websites, and social networking sites such as Facebook, for signs of potentially inappropriate political activity by public servants.

Since that report, the Commission advised us that the initiative was never fully developed or implemented, and that it has been dropped.

2.4 Complaint Investigations Involving the Collection of Personal Information

2.4.1 CANADA POST DEMANDS TOO MUCH INFORMATION FOR LEAVE REQUESTS

An individual filed a complaint over Canada Post's collection of personal information in connection with two separate applications she made for special paid leave to take care of an ailing relative.

The application form is actually intended only to guide supervisors in weighing whether to grant a request for leave. Supervisors have some discretion in how many of the questions they actually ask. In this instance, however, the complainant's supervisor erroneously gave the complete form to the complainant herself to fill out.

The form required extensive amounts of personal information about the requester, the ill person and even third parties. For example, it asked whether any other Canada Post employee had asked for leave to take care of the same patient.

As we investigated this complaint, Canada Post told us that the Crown corporation receives about 3,000 special leave requests every year, totalling more than 125,000 hours of work.

Over the years, arbitration rulings under the union's collective agreement have helped shape how this category of leave is administered. Those decisions now require Canada Post to collect substantial amounts of information, in order to ensure that leave requests are considered in a fair and reasonable manner.

At the same time, Canada Post is concerned about preventing fraud or misuse of this open-ended leave provision. While acknowledging the organization's duty in that regard, we nevertheless felt that too much personal data is being collected. We were particularly concerned about questions that require a leave applicant to furnish personal information about another person.

We concluded that the complainant had been asked for more personal information than was necessary to establish her entitlement to the leave, and upheld her complaint as ***well founded***.

We also recommended a series of measures that Canada Post could take to address privacy concerns.

The organization accepted some of the recommendations, agreeing to collect only the personal information that is absolutely necessary for the proper administration of the program. Canada Post stated, for instance, that it would no longer require the names of other individuals (third parties) who might have been involved in caring for the sick person.

The organization also agreed to update its written procedural guidelines that supervisors must follow when an employee requests a leave, in order to ensure that only required information is collected.

However, the organization insisted on continuing to collect information on other family members working at Canada Post, in order to ensure that two or more employees were not abusing the benefit by requesting the same leave.

In the absence of proof of extensive abuse, we continue to have reservations about this data collection. We have encouraged the organization to find less privacy intrusive ways to address its concerns about fraud in weighing leave requests.

2.4.2 DRIVER'S LICENCE SUITABLE ID FOR POSTAL BOX RENTAL

An individual complained after Canada Post required him to supply his driver's licence number in order to terminate the rental of his postal box.

Canada Post countered that it requires box renters to furnish personal identification in order to ensure that a box is not being used or closed fraudulently. The postal service also stated that it has used such recorded ID to investigate cases where illegal goods may have been shipped to rented mailboxes.

Our investigation determined that Canada Post has a statutory obligation to provide a secure postal service, and was collecting and using personal information for purposes consistent with that mandate. We found the collection of driver's licence and other identification numbers to be reasonable, and dismissed the complaint as ***not well founded***.

2.5 Follow-up on the RCMP Exempt Databanks Audit

2.5.1 CONTEXT

The *Privacy Act* gives individuals a general right to request access to their personal information held by government institutions. That right, however, has specific limitations.

For example, the Act's section 18 permits certain institutions to set up exempt databanks, which generally contain highly sensitive national security and criminal intelligence information.

Individuals have no access to their personal information stored in those databanks; indeed, they cannot even learn that their information is being held there.

The special and generally secretive nature of security and intelligence work may justify the exemption of certain files from public access. We certainly recognize the importance of assuring law enforcement and security partners, both domestic and foreign, that information shared in confidence will be protected accordingly.

However, in exchange for the privilege of keeping information totally exempt from public access, institutions are expected to ensure that exempt databanks contain only files that legitimately warrant inclusion. As the Privacy Commissioner remarked in

1990: "No exempt bank, once established, can be allowed to become an uncontrolled hiding place for personal information."[2]

This is because people whose names appear in exempt databanks could be at risk of harmful impacts. For example, a person's name could be included in an exempt file simply because the individual was in the wrong place at the wrong time, talking to the wrong person. Some information may also wind up in the databank from an informant who is misinformed, or perhaps motivated by something other than civic responsibility.

If erroneous information is in an exempt bank, even entirely innocent people could have trouble obtaining security clearance for a job, or crossing an international border. Because the files remain secret, individuals may never learn the cause of their problems.

Thus, it is important that exempt files be subjected to ongoing review to ensure they merit continued inclusion in the exempt databank.

We completed an audit of the RCMP's exempt databanks in February 2008. The audit found that the banks were not sufficiently well managed. As a result, they contained tens of thousands of files that should not have been there.

2.5.2 FOLLOW-UP AUDIT

In 2010-2011, we followed up on the 2008 audit to assess whether the RCMP had acted on its commitments with respect to our recommendations.

Officials told us that, in response to our audit, they had re-examined all of the organization's exempt bank holdings — with remarkable results.

In March 2008, there were 5,288 files in the national security exempt bank. By March 2011, all but 190 of the files had been removed.

The review of criminal intelligence files yielded a similar outcome. By the end of the past fiscal year, there were 2,898 files with exempt bank status. That's 58,379 fewer files than were in there three years earlier.

---

[2] Privacy Commissioner's Annual Report 1989-1990, p. 28.

In all, more than 95 percent of the re-examined files had been removed from the National Security Records and Criminal Intelligence Exempt Banks, according to the RCMP.

The RCMP also said they have addressed all our other audit recommendations. In particular:

- ***a new integrated accountability structure is in place to manage exempt banks, with authority delegated to specific individuals for approving the inclusion of files;***
- ***a centralized review mechanism has been established to ensure the status of the files is accurately reflected in both automated and hard-copy format;***
- ***a mandatory two-year internal review cycle has been established for exempt banks.***

The new measures to address the audit findings should provide a framework for ensuring the RCMP's exempt bank holdings comply with the requirements of the *Privacy Act* and associated internal exempt bank policy.

2.6 Integrating Privacy into Public Safety Initiatives

A new generation of mobile devices, remote sensors, high-resolution cameras and analytic software has revolutionized surveillance practices and greatly facilitated the global collection, processing and sharing of data.

Police and government investigators can employ those capabilities for the benefit of a safer society. But, at the same time, the unchecked accumulation of data about the movements, activities and communications of citizens can also carry negative consequences by constraining people's fundamental right to go about their business in anonymity and freedom from state monitoring.

Undue intrusion into the personal lives of citizens is the antithesis of a secure and confident state. Careful checks and balances were created specifically for the purpose of ensuring a wider social space where citizens could enjoy privacy and freely conduct their personal affairs.

2.6.1 REFERENCE DOCUMENT

Our Office drew on the advice of experts in both privacy and security in academia, the legal community, civil society, politics, intelligence, law enforcement and oversight to develop a reference document that would help policymakers, practitioners and citizens navigate these complex issues.

Entitled *A Matter of Trust: Integrating Privacy and Public Safety in the 21st Century,* the document offers a clear and practical analytical framework for the integration of privacy protections with new public safety and national security objectives, as well as step-by-step guidance on achieving the appropriate balance.

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

2.6.2 LAWFUL ACCESS LEGISLATION

Privacy Commissioners from across Canada also continued to urge federal lawmakers to proceed with caution as they seek to rebalance the legal protections and thresholds around government access to personal information.

In March 2011, Privacy Commissioner Jennifer Stoddart, along with all provincial and territorial privacy guardians, wrote to the Deputy Minister of Public Safety Canada to outline the privacy risks that they see emerging from the government's intention to amend the legal regime governing electronic search, seizure and surveillance.

Our Office continues to argue that there is insufficient justification for the extent of the new lawful access powers, that other less intrusive alternatives can be explored, and that oversight for lawful access ought to be strengthened.

2.7 Biometrics Primer

2.7.1 CONTEXT

In many types of interactions with the state, individuals have no choice but to relinquish personal — often sensitive — information, sometimes in significant amounts. In order to secure a passport, for example, individuals must submit information about their residence and occupation, and consent to the use of a facial image.

Indeed, personal data is generally the currency exchanged for government programs, services or entitlements.

Our Office has noted that government agencies are becoming increasingly interested in biometric systems to manage access to programs and services. The term "biometrics" refers to a range of techniques, devices and systems that enable machines to recognize individuals, or to confirm or authenticate their identities.

Such systems measure and analyze people's physical and behavioural attributes, such as gait, facial features, voice patterns, fingerprints, palm prints, finger and palm vein patterns, or structures of the eye (iris or retina).

Biometric data is collected at a starting point. Identities can subsequently be established or authenticated when new data is collected and compared with the stored records.

The most common example of a biometric is an ID photo used in a passport, driver's licence or health card. A person's facial image is captured and stored, so that it can later be compared against another picture or a live person.

2.7.2 PRIVACY CHALLENGES

Biometric technology can contribute to highly reliable and robust identification systems — more reliable, for instance, than paper-based systems.

On the other hand, they can also raise significant privacy challenges, such as the covert collection of biometric characteristics, cross-matching, and the unwanted disclosure of secondary information embedded in an individual's biometric information.

Many forms of biometric information, such as fingerprints and facial images, can also be collected without a person's knowledge, let alone consent. They can, therefore, be used to surreptitiously monitor and track people's movements and behaviour.

For all these reasons, it is imperative that government institutions and other organizations think carefully before proposing initiatives that call for the collection of biometric information.

To aid in this analysis, our Office prepared a detailed primer that explores the benefits and drawbacks of biometrics. Published in 2010-2011, it is titled *Data at Your Fingertips: Biometrics and the Challenges to Privacy*.

Data at Your Fingertips: Biometrics and the Challenges to Privacy

The primer provides basic information on biometrics and the systems that use them. It also describes some of the privacy implications raised by this emerging field, as well as measures to mitigate the risks.

The publication, which was posted to our website, introduces a method for determining the appropriateness of biometrics for different applications, and makes recommendations for privacy-sensitive designs.

As the primer explains, the challenge for organizations is to design, implement and operate systems that actually improve identification services, without unduly compromising privacy.

CHAPTER 3

To Have and to Hold

Is the Federal Government Making the Right Use of Personal Information?

In the summer of 2010, WikiLeaks stunned the world by publishing classified U.S. military documents about the Afghan War. This was followed a few months later by a similar leak of Iraqi War documents and a massive disclosure of cables between the U.S. State Department and its missions abroad.

The unprecedented release of sensitive government and military information online and through the mainstream media sparked a firestorm of debate on issues ranging from press freedom and open government to data security and U.S. foreign policy.

But one thing became crystal clear: Knowledge is power. The state generally has plenty, the citizen relatively little, and the document dump was one non-governmental organization's attempt to right the balance.

Setting aside the propriety of the WikiLeaks leaks, the fact is that Western societies have always looked for ways to hold their governments accountable to the people they serve. A key measure of accountability can be found in the state's handling of information.

In the ideal, an accountable government would be fully transparent in its own actions, while holding in confidence the personal information of citizens.

Over the past year, our Office spoke to Parliamentarians about the value of open government. We underlined that this is by no means at odds with the government's obligation, under the *Privacy Act*, to protect the privacy of individuals.

As the previous chapter explains, the Act calls for the appropriate collection, retention and disposal of personal information. The next chapter will also describe the importance of safeguards against the inappropriate disclosure of personal information.

APPROPRIATE USES

But there's more. The *Privacy Act* also requires that the government use the personal information of citizens only for defined and appropriate purposes. It is appropriate, for instance, to use income-related information to manage a tax benefit.

It is decidedly not, however, appropriate to use the personal medical information of a man who served in our military in the preparation of a briefing note to the Minister of Veterans Affairs on the man's participation in a Parliament Hill press conference to discuss issues related to veterans.

Use of Personal Information

Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be used by the institution except. . .for the purpose for which the information was obtained or compiled by the institution, or for a use consistent with that purpose. . . .

— *Privacy Act*, section 7

With the exception of certain types of data that are specifically exempted, the Act also gives people a right to request access to their personal information held by government. Without that opportunity, people have no idea whether the information the government holds on them is accurate or complete.

This chapter examines the uses and misuses of personal information by the Government of Canada in 2010-2011. It explores issues of access to personal information, and concludes with a discussion of privacy in the context of more open and transparent government.

3.1 Veterans Affairs Canada Breach

VETERAN'S PERSONAL INFORMATION SERIOUSLY MISHANDLED, INVESTIGATION FINDS

3.1.1 OVERVIEW

An investigation into a high-profile complaint by a former soldier raised significant concerns about the stewardship of sensitive medical and other personal information by Veterans Affairs Canada. We were particularly concerned about the apparent lack of controls to protect sensitive personal information from being widely accessed and disseminated within the Department.

That investigation brought to light serious systemic issues, prompting us to announce plans to conduct an audit of the Department's compliance with the privacy law. Since then, we have continued to receive further complaints.

In this original complaint, the veteran alleged that the Department had violated the *Privacy Act* by using his personal information inappropriately when it included excessively detailed and sensitive medical, financial and other personal information in briefing notes to the Minister of Veterans Affairs. The complainant also alleged that the Department had transferred his medical file to a hospital administered by Veterans Affairs, without his consent.

The incidents referred to in the complaint occurred in 2005 and 2006. We published a summary of our investigative findings and recommendations to the Department in October 2010. Our audit of the Department is ongoing and we expect to conclude it in the winter of 2012.

3.1.2 MINISTERIAL BRIEFING NOTES

Our investigation confirmed that several briefing notes prepared for the then-Minister of Veterans Affairs contained personal information about the complainant. The volume and sensitivity of personal information, including medical and financial information, contained within two briefing notes to the minister was excessive and went far beyond what was necessary for the stated purpose of the briefings.

In particular, the notes included significant detail about how the complainant interacted with the Department, as a client and an advocate for veterans. Of particular concern was a note prepared in March 2006 to brief the Minister on the complainant's participation in a Parliament Hill press conference to discuss issues related to veterans.

In addition to briefing the Minister on the complainant's advocacy activities, the note contained sensitive information about his medical diagnosis, symptoms, prognosis, frequency of appointments, recommended treatment plans, chronology of client interactions with the Department, and amount of financial benefits received. The complainant had given the Department this information when he applied for veterans benefits.

Of further concern was the way the complainant's personal information was widely circulated within Veterans Affairs, including Program Policy, Communications and Media Relations branches, as the briefing notes were prepared. Sensitive personal information was shared among officials who would normally require little or no access to it to fulfill their duties.

3.1.3 TRANSFER OF PERSONAL DATA TO HOSPITAL

On the second issue raised in the complaint, the investigation found that the Department had sent several large volumes of the complainant's personal and medical information to a hospital that it administers. Included were medical reports, letters between the complainant and the Department, and a briefing note prepared for the Minister.

Veterans Affairs stated that it transferred the information to the hospital in order to establish his suitability for referral to a treatment program offered there.

Departmental guidelines require clients to authorize such data transfers in writing. This was, however, not done.

3.1.4 FINDINGS

In both matters raised in the complaint, the investigation found that Veterans Affairs' use of the complainant's personal and medical information contravened section 7 of the Act. This section states that personal information under the control of a government department shall not, without an individual's consent, be used by the department, except for the purpose for which the information was obtained or compiled, or for a use consistent with that purpose.

Accordingly, we upheld the complaint as ***well founded***.

3.1.5 RECOMMENDATIONS

The Assistant Commissioner recommended that Veterans Affairs Canada:

- ***take immediate steps to develop an enhanced privacy policy framework with adequate protections and controls to regulate access to personal information within the Department;***
- ***revise existing information-management practices and policies to ensure that personal information is shared within the Department only on a need-to-know basis;***
- ***provide training for employees about appropriate personal information-handling practices;***
- ***review procedures to ensure that consent is obtained before personal information is transferred to other institutions.***

3.1.6 DEPARTMENTAL RESPONSE

Following the publication of our investigative findings, the Department began rolling out a 10-point action plan to address our concerns. The Department reported that, by the end of the fiscal year, it had appointed external experts in privacy and electronic information systems, and was proactively monitoring and investigating employee access to client information.

Veterans Affairs Canada also said it was providing its staff with mandatory training on privacy and introducing new procedures for the appropriate use of client information in briefing notes and other departmental documents. Staff were also informed of a strengthened disciplinary policy, with clear sanctions for violations.

For the longer term, the Department pledged to undertake independent annual assessments to ensure compliance with the *Privacy Act*.

3.1.7 PRIVACY COMPLIANCE AUDIT

At the time of our investigation, we found that Veterans Affairs Canada officials could not clearly identify or explain policies, procedures or typical information-sharing practices. We were therefore not persuaded that the Department had adequate policies and procedures in place to ensure the appropriate handling of veterans' personal information.

Accordingly, we announced an audit to assess whether the Department had followed up on our recommendations to address weaknesses identified in our investigation. We also wanted to know whether its 10-point action plan was leading to the policies, procedures and processes necessary to manage personal information in a manner that complies with the *Privacy Act*.

We expect to report on the results of our audit during the winter of 2012.

3.2 Other Complaint Investigations Involving the Use of Personal Information

3.2.1 LETTER CARRIER ACCUSES BOSS OF INTERCEPTING AND READING A DOCUMENT

A Canada Post letter carrier complained that his supervisor had gained unauthorized access to a medical form related to a disability insurance claim.

The complainant claimed he had given the form in a sealed envelope to his supervisor, with the understanding that the supervisor would forward it, unopened, to the medical insurance company. The letter carrier asserted that the supervisor had opened the envelope, read the form, and used the information to challenge the validity of other medical documentation he had supplied to Canada Post.

In our investigation, the supervisor acknowledged she may have read the form, although she said she could not remember having done so. She insisted, however, that she would never have opened a sealed envelope.

Our investigation could not determine whether the form had, in fact, been sealed in an envelope. We did, however, confirm that the supervisor had used the health information on the form to contradict other health-related documentation supplied by the employee.

We concluded that the employee's personal information had, indeed, been used for a purpose inconsistent with the purpose for which the data was collected, and was used in this way without the complainant's permission. We therefore upheld his complaint as ***well founded***.

We did, however, find that the breach was isolated, and that Canada Post has clear practices for managing disability claims.

We recommended that Canada Post remind all staff to submit their insurance claim forms directly to the insurer. We also recommended that the organization remind managers to refuse to accept such forms on behalf of their staff.

3.2.2 HIRING PROGRAM FOR EX-MILITARY STAFF MAKES PROPER USE OF INFORMATION

An individual complained to us that the Public Service Commission of Canada had improperly collected and disclosed personal information about his release from the Canadian Forces for medical reasons.

The information was collected for use in a program that gives former military personnel priority consideration for vacant positions in the federal public service.

Our investigation determined that all aspects of the process had conformed fully with the *Privacy Act*. Indeed, we found that the complainant had consented in writing to the collection and disclosure of his medical release record from the military for the priority hiring program.

Accordingly, we dismissed the complaint as ***not well founded.***

3.3 Complaint Investigations Involving Access to Personal Information

3.3.1 HEALTH CANADA ERRED IN WITHHOLDING PERSONAL INFORMATION

An individual complained to us after Health Canada refused to give him access to personal information that had been collected about him before, during and after an evaluation of his fitness for work. The evaluation was carried out by a Health Canada program that deals with occupational health and safety.

The Department declined to turn over the information, citing section 28 of the *Privacy Act*. That section states that the head of a department may choose to withhold personal information related to the physical or mental health of an individual if examining the information would be contrary to the best interests of the individual.

The regulations further stipulate that the head of the organization may show the personal information to a medical practitioner or psychologist who is qualified to determine whether disclosure of the information would be against the individual's

best interests. Involving a medical professional, however, requires the consent of the individual concerned.

Upon investigation, we concluded that the personal information that the complainant was seeking was not confined to sensitive records related to his mental or physical health. We therefore concluded that section 28 of the Act did not give Health Canada an appropriate reason to withhold access to his personal information.

Consequently, we upheld the complaint as ***well founded***. However, after the Department undertook to release the requested information, we also deemed the file to be ***resolved***.

3.4 Legal Work in Support of Access to Personal Information

Under section 41 of the *Privacy Act,* individuals who have been refused access to their personal information in the hands of a federal institution may apply for a hearing before the Federal Court for a review of the refusal.

Under section 42 of the Act, the Commissioner may also apply for a hearing before the Court for a review of a refusal to grant an individual access to requested personal information.

The Act does not currently permit an individual or the Commissioner to apply for a hearing regarding other violations of the Act, such as the wrongful collection, use or disclosure of personal information by a federal institution. Over the years, our Office has often recommended that the federal government broaden the grounds for which an application under the Act may be made to the Federal Court.

One court application with which we were involved in 2010-2011 is described here. In keeping with the spirit of our mandate, we do not publish the names of plaintiffs. We do, however, provide court docket numbers and names of respondent institutions as applicable.

3.4.1 *X. v. PRIVACY COMMISSIONER OF CANADA* FEDERAL COURT FILE NO. T-555-10

This is an application for judicial review against the Privacy Commissioner, in which the applicant seeks an order compelling the Office to reinvestigate a complaint the applicant filed against the Social Sciences and Humanities Research Council (SSHRC) regarding a denial of access to his personal information under the *Privacy Act*. The applicant alleges

that the Office of the Privacy Commissioner failed to conduct a proper investigation of his complaint and that the Office was biased.

Our Office is fully defending this application. After a number of interlocutory matters, the case was set down for a hearing on Sept. 6 and 7, 2011.

3.5 Open Government

The principle of open government holds that the business of government should be transparent at all levels to allow for full citizen engagement and effective public scrutiny and oversight.

Our Office endorses government transparency as a key principle of democracy. Indeed, open government is about building trust between government and the citizens it serves.

However, we also take the view that transparency should not come at the cost of individuals' statutory rights to privacy. The trust of citizens hinges equally on assurance that the government will treat their personal information with respect, safeguard it, and ensure it is not inappropriately disclosed.

During 2010-2011, we advocated for this balance through several forums, including a July 2010 letter to the House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI).

Two months later, Canada's federal, provincial and territorial access-to-information and privacy commissioners signed a resolution to endorse and promote open government as a means to enhance transparency and accountability. The resolution specifically stated that open government must afford due consideration to privacy, confidentiality and security.

Then, in mid-February 2011, Assistant Commissioner Chantal Bernier appeared before the ETHI Committee to further elaborate on the issues.

She pointed out that the line between identifiable and non-identifiable information is becoming increasingly blurred with the emergence of new information technologies. What initially appears to be anonymous or de-identified information can, in some cases, be combined with information from other sources and linked back to specific individuals.

If data is found to contain personal information about an identifiable individual, then all the requirements and protections of the *Privacy Act* must be observed.

Data protection authorities here and around the world are increasingly convinced that governments need to build privacy considerations directly into the design of any program or service if personal data is to be gathered. Privacy must be the default position, rather than something added on as an afterthought.

At an operational level, it is vital that consideration be paid to ongoing employee privacy training, proper rules and processes for disclosing information, and the mechanics and resourcing of the access-to-information and privacy systems.

3.6 Requests to the OPC under the *Access to Information Act* and the *Privacy Act*

The Office of the Privacy Commissioner of Canada is subject to both the *Access to Information Act* and the *Privacy Act*. Here is a summary of our activities under both Acts over the past fiscal year.

3.6.1 *ACCESS TO INFORMATION ACT*

In 2010-2011, our Office received 63 new requests under the *Access to Information Act* for government records under our control, 11 more than the year before. One request in 2010-2011 was carried forward from the previous year. A total of 31 access requests that we received during the past fiscal year were seeking records under the control of other federal institutions, and were therefore redirected.

In all, we responded to 64 access-to-information requests by the end of the fiscal year, and none was carried forward.

We received notice of one complaint submitted to the Information Commissioner under the *Access to Information Act* in 2010-2011, compared to two the year before. This new complaint alleged denial of access to government records. The Information Commissioner determined that it was not well founded.

3.6.2 *PRIVACY ACT*

We received 105 requests under the *Privacy Act* for personal information contained in documents under our control in 2010-2011, and closed 106. This compares to 61 requests received and 60 closed in the 2009-2010 fiscal year.

A total of 91 privacy requests that we received in 2010-2011 were seeking records under the control of other federal institutions, and were therefore redirected.

We received five complaints under the *Privacy Act* during the fiscal year, four of them from the same individual. One complaint related to delays in obtaining access to personal information, one related to exemptions invoked for the withholding of documents, and three were about missing documents.

These complaints were referred to the Privacy Commissioner *Ad Hoc*, whose mandate is to independently investigate any complaints that may be lodged against the Office of the Privacy Commissioner of Canada under the *Privacy Act*.

CHAPTER 4

Generous to a Fault?

How Personal Information Gets Disclosed by Government

Call it frugal, tightfisted, thrifty or parsimonious, it's what Canadians expect their government to be when it comes to parcelling out their personal information.

The *Privacy Act* requires federal departments and agencies to hold safe the personal information of Canadians. Without the consent of the individual concerned, the government may not disclose personal information under its control, except under a strict set of rules.

By modernizing its information-management infrastructure, the government has moved to further strengthen its prudent stewardship of personal information. Unfortunately, as this chapter describes, that initiative hit a snag with a data breach in late-September, 2010.

Breaches aside, when it comes to deliberately sharing data — whether among departments or with other domestic or foreign authorities — the government must err on the side of stinginess. Data must be shared only when necessary and appropriate, and only to the extent required to achieve the stated purpose.

Section 8(2) of the Act sets out the circumstances under which personal information may be disclosed. One example is to help an investigative body enforce a federal or provincial law, but only if the request specifies the purpose and describes the information to be disclosed. The Act also allows personal information to be disclosed without consent if the head of an institution believes that the public interest in the information outweighs the invasion of privacy.

Over the years, the limitations set out in the Act have been further defined and strengthened through directives from Treasury Board. If personal information is to be

disclosed to other authorities, for example, formal information-sharing agreements must set out exactly who gets to see the information, and under what terms.

The idea is to protect sensitive personal information from being disclosed to the wrong people. After all, any breach of personal data can have consequences for the individuals concerned. They may be exposed to embarrassment, inconvenience or even identity theft and the economic hardship that often accompanies it.

GRAVE CONSEQUENCES

The need to protect personal information is especially important when individuals have no right under the *Privacy Act* to see or correct it — typically because the information is held in databanks exempted from the Act's access provisions.

For instance, individuals are not permitted to know about, view or amend information held by security agencies.

Therefore, if inaccurate or incomplete information is shared with other authorities, people may find their liberties curtailed. They may be wrongfully placed on watch lists and banned from international travel. In extreme cases, they may even be jailed or deported.

Aside from information that is improperly shared, some is simply spilled. Data breaches can be deliberate acts of malfeasance, or simple accidents and oversights.

Some breaches come to our attention because the affected individual files a complaint with our Office. In other instances, the department or agency reports the breach to us, along with steps it is taking to mitigate the damage.

The *Privacy Act* contains no reporting requirement and no sanction for breaches, but Treasury Board policy strongly encourages institutions to notify us if personal information under their control is improperly exposed.

We're pleased to report that, unlike in other years, there were no egregious data breaches in 2010-2011, involving the personal information of tens of thousands of people.

We did, however, notice the tenacity of human error as a cause for data breaches. Files and binders were forgotten on buses and airplanes, CVs were inadvertently posted online, and a list of Social Insurance Numbers was left lying about in plain sight.

This chapter reports on our investigations of complaints about the inappropriate disclosure of personal information, as well as reports of breaches submitted to our Office.

It also describes a Privacy Impact Assessment we received from the RCMP about new data-sharing technologies, and summarizes the actions that various institutions have taken to address concerns about data security that we expressed in past privacy audits.

The chapter wraps up with an update on instances in which institutions have notified us that they have disclosed personal information without consent, but in the public interest.

4.1 Complaint Investigations Involving the Disclosure of Personal Information

4.1.1 PSYCHIATRIC NURSE FORGETS EX-INMATE'S TREATMENT FILE ON BUS

A former inmate residing at Toronto's Keele Community Correctional Centre complained after a psychiatric nurse employed by the facility left an envelope containing his treatment notes on public transit.

The director of the centre, a halfway house for 40 men freed from federal institutions under statutory release provisions, wrote to the complainant to advise him of the loss of the documents.

The director conceded that the complainant's privacy had been breached and apologized for the incident. He also stated that the matter had been investigated internally, and that actions were taken to prevent a recurrence.

In particular, the nurse was reminded of his duty to safeguard the personal information of patients. He was also reminded not to transport patient files from the office, unless they are encrypted.

Our investigation confirmed that the complainant's privacy had been breached and upheld his complaint as ***well founded***.

We also concluded that the facility, which falls under the jurisdiction of the Correctional Service of Canada, had taken appropriate corrective measures in the wake of this incident.

4.1.2 CUSTODIAN OF SOCIAL INSURANCE NUMBERS LOSES LIST OF THEM

A woman complained to us about the mishandling of her personal information at an information session for employment insurance (EI) claimants. Human Resources and Skills Development Canada (HRSDC) holds these mandatory information sessions primarily to validate the identity of EI claimants, who generally apply for the benefit online, without face-to-face contact.

At the end of the session, the complainant learned that the attendance sheet had gone missing. She was told it contained the names, telephone numbers and Social Insurance Numbers (SINs) of the session's 32 participants.

Departmental officials prepared a report and advised their access-to-information and privacy office, as well as our Office, about the incident. They also notified all affected individuals, apologized, and directed them to information on protecting themselves from identity theft.

Upon investigation, we agreed that the Department had not properly safeguarded the personal information printed on the sheet. We upheld the complaint as ***well founded***.

We were especially disturbed that the breach involved the SIN, which is a critically important piece of personal information for people dealing with federal and other institutions. Because of its value, the number is highly vulnerable to misuse if it falls into the hands of identity thieves.

Worse, the breach was the fault of HRSDC, the very Department that issues and manages the use of the SIN.

Still, we noted that officials in the region where the incident occurred had taken all reasonable steps to mitigate any consequences from the data breach and to prevent a recurrence.

Among other things, they directed officials to fully black out the SINs on attendance sheets before the documents are used at EI claimant information sessions, a practice that is expected to be adopted across the country.

4.1.3 MINISTER'S SUSPICIONS ABOUT WHEAT BOARD LEAKS UNFOUNDED

In November 2009, the then-Minister of Agriculture and Agri-Food Canada, who was also responsible for the Canadian Wheat Board, filed a privacy complaint against the wheat marketing agency.

The complaint was sparked by media reports about an internal wheat board audit on the Permit Book process, which tracks grain sales made by Western Canadian producers through the wheat board.

One of the questions raised by the audit was whether the Canadian Wheat Board had improperly disclosed to third parties such personal information as the farmers' Social Insurance Numbers (SINs). Third parties included grain handlers who facilitate sales transactions, and the Canada Revenue Agency.

The audit, conducted in 2008 and made public under an access-to-information request in the fall of 2009, highlighted potential privacy weaknesses. The resulting media coverage left the impression of impropriety, after which the minister filed a privacy complaint to our Office.

Our investigation found that the wheat board has in place the appropriate protocols, procedures and agreements necessary to ensure that the personal information of grain producers is collected, used, safeguarded and shared with care. In particular, we found that the wheat board does not disclose SINs to third parties, and only shares personal data with the tax agency when required to by law.

Accordingly, the complaint was dismissed as ***not well founded***. We also commended the Canadian Wheat Board for its good information-management practices.

4.1.4 PRISON TO PUT SENSITIVE MAIL IN ENVELOPES AFTER DOCUMENT INTERCEPTED

An inmate at a maximum-security prison near Agassiz, B.C., complained to us after a 10-page National Parole Board decision about him was circulated among his fellow inmates.

The decision, which included a graphic description of the prisoner's offence, was to have been delivered to the inmate through the Kent Institution's internal mail. However, the document was not placed in an envelope. Instead, it was simply folded and stapled, and his name was written on the outside.

The parole board decision never reached the inmate. Instead, it appears to have been intercepted, photocopied and circulated among the prison population.

Prison officials wrote to the inmate to acknowledge the privacy breach and to advise him of his right to complain to our Office.

The warden of Kent Institution, which falls under the jurisdiction of the Correctional Service of Canada, also launched an investigation of the incident. The investigation confirmed that the document had been viewed by various inmates without the complainant's permission, but could find no evidence that a staff member had intentionally delivered the papers to the wrong inmate.

Our investigation determined that the disclosure violated the *Privacy Act* and upheld the complaint as ***well founded***.

Following the incident, the warden implemented some changes to the penitentiary's mail delivery process. Confidential documents are now placed in sealed envelopes.

4.1.5 ERRANT REPORT SPARKS PROCEDURAL CHANGES AT PRISON

Two prisoners at the Correctional Service of Canada's Grande Cache Institution, west of Edmonton, filed complaints after a prison report containing their personal information turned up among the personal effects of a fellow inmate.

An investigation by the minimum-security facility determined that, in early-April 2009, a contract worker had printed off a single copy of the report, which listed the names, dates of birth and other personal information of all serving inmates. The report was given to a welding instructor, who took the report to his office in the welding shop and referred to it frequently when interacting with inmates.

In late-May 2010, as an offender's effects were being packed in the prison's discharge area, an officer discovered the report. The investigation could not determine how the document wound up among the prisoner's belongings. The inmate claimed he did not know he had the report, and the welding instructor denied having given it to him.

The investigation further revealed that both the contractor and the welding instructor had been trained on the importance of safeguarding personal information.

Correctional service officials formally acknowledged the privacy breach. They also took a number of steps to minimize the risk of inappropriate disclosures.

For example, the kind of report that went missing is no longer to be printed out; it can only be viewed on a computer screen. Procedures were also put in place to ensure that staff and external contractors fully understand the need to safeguard personal information, and how to protect it from unauthorized disclosure.

Our own investigation confirmed that the privacy rights of the complainants had been breached and upheld their complaints as ***well founded***. Because of the corrective measures already underway, we did not call for further action.

4.2 Data Breach Reports

4.2.1 OVERVIEW

A data breach is an unauthorized loss or disclosure of personal information. Some breaches occur without the affected individuals knowing about them. In other cases, people are notified of the breach or learn about it in some other way. Some of them file complaints with our Office.

Federal public-sector data breaches reported to OPC 2004-2005 to 2010-2011	
2004-2005	27
2005-2006	55
2006-2007	54
2007-2008	44
2008-2009	26
2009-2010	38
2010-2011	64

Regardless of the real or potential reaction of affected individuals, the Government of Canada has guidelines encouraging its departments and agencies to report all significant data breaches to our Office, and to do so in a timely manner.

In the past fiscal year, 64 data breaches were reported to us by federal institutions, two-thirds more than the 38 reported to us the year before. This is the highest number we have seen in recent years.

The rising number of reports is not necessarily cause for alarm, however. It could simply mean that organizations are becoming more diligent in reporting incidents to us.

Indeed, we know that a single department — Human Resources and Skills Development Canada — filed 21 reports last year, one-third of all the reports we received, and three times as many as it filed the year before.

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 the 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.

Benefits of reporting

While some departments may still feel uneasy about confessing to errors, we encourage all of them to notify us of breaches. When they contact us for advice on an incident, we always suggest they fill out the *Privacy Breach Incident Report* on our website and forward it to our Office.

We find, in fact, that most institutions are now familiar with their obligations under the reporting guidelines, and are prepared to step up. Aside from their notification duties, it's up to the organizations themselves to do whatever is necessary to fix or mitigate the damage and to ensure it doesn't happen again.

There are also benefits to reporting.

For example, if we know that remedial efforts are already underway, individuals who call to complain about the incident can be told that the matter is in hand. In such circumstances, they are more likely to be satisfied, and less likely to file a formal complaint.

Of the 64 data breach notifications we received, five related to lost or stolen information. In two instances, employees misused personal information they obtained through their work by posting it to their personal websites. Four breaches were traced back to technical troubles — typically a web application that was inadequately tested.

On eight occasions, a third party's personal information was not properly severed before documents were released in response to access-to-information requests. There were a further three cases in which documents containing personal information were left in an open recycling bin or other open area at work.

The remaining cases were blamed on ordinary employee error where, for instance, a document containing personal information was sent to the wrong recipient. Indeed, year after year, human error in the stewardship of personal data tends to be the most common reason for data spills.

RISK: HUMAN ERROR

Impossible though it is to outlaw forgetfulness, this report nevertheless serves as a yearly reminder of the need to take the utmost care in handling the personal information of Canadians. Even in this Age of Distraction, data breaches caused by inattention, negligence or other human errors should be preventable.

4.2.2 TRANSPORT CANADA EMPLOYEE LEAVES BINDER ON BUS

Transport Canada advised us that one of its employees had left a binder with sensitive personal information on a city bus. The binder contained contact lists to be used in the event of an emergency affecting the transportation system during the Vancouver Olympic Games.

The lists contained the BlackBerry personal identification numbers, as well as the home and cellular phone numbers, of approximately 65 federal employees, up to the level of deputy minister.

The binder was never recovered.

Transport Canada reminded all employees about the proper handling of protected and classified information, including procedures that must be followed when sensitive documents have to be removed from the Department's premises.

4.2.3 EXPERT MEDICAL ADVISER FORGETS FUNDING REVIEW DOCUMENTS ON AIRPLANE

A senior medical investigator heading a peer review committee for funding applications submitted to the Canadian Institutes of Health Research (CIHR) forgot a sheaf of documents on a flight to Ottawa. The documents reviewed proposals for university-based medical research projects, to assess their suitability for federal grants.

It is not known exactly how many of the reviews were left on the aircraft seat, but it is believed there were between 60 and 70. They were never recovered.

An investigation by the medical research granting council concluded that the documents contained some personal information of funding applicants, but that the information was not so sensitive as to raise the risk of identity theft or other fraud.

In a subsequent letter to all grant applicants, the organization stated that the documents, for the most part, would have included professional biographical details that most researchers already post online.

The institution also noted that, while grant application reviews generally include the opinions of outside experts on the qualifications of individual funding applicants, these review documents tended to focus more generally on the composition and expertise of proposed research teams.

The professor who lost the documents served as an outside expert in the application review process on a volunteer basis.

In the wake of the incident, the CIHR undertook to strengthen its security guidance information for its peer reviewers, including best practices for the secure handling of protected documents. The organization also promised to design a security briefing specifically for volunteer members of its peer review and advisory committees.

4.2.4 STUDENT LOAN DOCUMENTS DESTINED FOR BANK FAXED TO LAWYER INSTEAD

Human Resources and Skills Development Canada intended to send a Canada Student Loan agreement to a student's educational institution, but the document was accidentally faxed to a third party.

The agreement and related paperwork contained the student's name, address, telephone number, a portion of her Social Insurance Number, e-mail address, program of study, loan certificate number, loan amount and student identification number.

In this instance, the documents were faxed to a law office, which agreed to destroy them. The student was informed about the incident in a letter.

The breach was traced back to an incorrect fax number. The private company handling transactions between the Canada Student Loans Program and financial institutions undertook to verify the fax numbers of financial institutions at least once per semester. It would also maintain a registry to record each time fax numbers are confirmed.

4.2.5 MAILING MIX-UP TRACED TO TYPO

A mistyped postal address is thought to explain why Public Works and Government Services Canada sent two boxes of sensitive documents to an incorrect address in Ottawa.

The boxes wound up at the office of a government relations specialist. Because he was accustomed to receiving printed materials from federal departments, his staff inadvertently opened the boxes.

Realizing that the documents contained personal and protected information and had been misdirected, he contacted our Office. We, in turn, notified the Department.

An investigation by the institution found that a series of human errors, compounded by the confusion of an office move, had led to the mix-up.

The investigator recommended a number of procedural changes, including ensuring that all envelopes and parcels contain the sender's full return address. A security transmittal form should also accompany all protected or classified information.

RISK: TECHNOLOGY

In other years, we have encountered instances in which a breach in computer security exposed the personal information of anywhere between a handful and tens of thousands of people. Sometimes hackers are to blame; other times the foul-ups can be traced back to programming or user errors.

This year, technological gremlins continued to wreak havoc, although the number of people affected was mercifully small.

4.2.6 SERVICE CANADA ONLINE ACCOUNT REVEALS PERSONAL DATA OF PREVIOUS USER

At 11:25 a.m. on Sept. 28, 2010, Human Resources and Skills Development Canada (HRSDC) noted that its brand new online Service Canada portal had a technical glitch under which a user could see financial and other personal information of previous visitors to the site.

By noon, the My Service Canada Account site, launched the day before, was shut down and an internal investigation was ordered.

The probe traced the problem to a feature of the underlying architecture, called Access Key, which allowed people who had previously used an older technology, called epass, to transfer over their old user IDs and passwords with relative ease.

This so-called auto login function was disabled and, by 9 p.m., the site was reactivated without further incident.

The investigation determined that, while 85,000 people had used the site on its first day of operation, only 75 of them may have been affected by the technical problem. All were contacted and advised that their personal information may have been viewed by others.

HRSDC continued to work with Bell Canada, which provides the Access Key service on behalf of Public Works and Government Services Canada, to find a permanent and reliable technical solution. The organizations also undertook to review their test procedures to reduce the chances that a similar glitch will occur in future.

Privacy Impact Assessment review

In September 2010, we received a Privacy Impact Assessment from Public Works and Government Services Canada on its Access Key Authentication System.

Access Key authenticates individuals and businesses in their online dealings with the Government of Canada. Users previously signed on using epass, a component of the government's Secure Channel infrastructure, but this was changed in the government's Cyber Authentication Renewal project.

The Access Key Authentication System is administered for the government by a private company, so the assessment we received used a cross-jurisdictional approach.

Our recommendations

On the basis of our review of the Privacy Impact Assessment, we made a series of recommendations related to:

- ***issuing guidelines on the collection, use and disclosure of IP address data***
- ***developing retention and disposal schedules for log information***
- ***telling users more clearly how the personal information they supply when registering for a Key may be used, and***
- ***creating secure user IDs and verifying password strength.***

4.2.7 FILM AGENCY POSTS INFORMATION ABOUT CONSULTANTS ONLINE

In July 2010, Telefilm Canada, the federal cultural agency that develops and promotes Canada's audiovisual industry, posted to its website a directory of mentors and scriptwriting consultants. The idea was to support the professional development of the cinematographic industry by facilitating access to such established experts.

A few weeks later, a member of Telefilm's legal services unit happened to notice that the directory listed more than the names and contact information for the 92 mentors and consultants; many also included links to the individuals' resumés. Those links were immediately deleted.

Telefilm launched an internal investigation, which discovered that two of the resumés had included a Social Insurance Number and three included complete dates of birth. Telefilm advised all five affected individuals about the breach, so that they could take steps to minimize the risk of identity theft or other misuse of their personal information.

The CVs and the directory also included street addresses and other personal information, much of it already in the public domain. Telefilm concluded that the risks posed by the temporary disclosure of this data were minimal.

Consequently, the organization opted not to inform the remaining 87 mentors and consultants, so as not to unduly alarm them.

The internal review made several recommendations. One was that any document containing personal information be subject to review by Telefilm lawyers before being posted on the Internet. The review also raised the possibility of re-examining the decision not to inform all mentors and consultants of the incident.

4.2.8 SOCIAL INSURANCE NUMBERS SLIP ONTO BANK STATEMENTS

Two people who received direct deposit payments of an Ontario sales tax benefit administered by the Canada Revenue Agency noted that their Social Insurance Numbers were visible on their bank account statements.

They contacted their financial institutions, which notified Public Works and Government Services Canada. PWGSC, which processed the deposits through its Standard Payment System, launched an investigation.

The investigation determined that, in setting up the program for this tax benefit payment, the programmer neglected to require the encryption of Social Insurance Numbers, which the Canada Revenue Agency uses as a client reference number.

In all, the system made 1.8 million direct deposit payments to various financial institutions. All contained the unencrypted Social Insurance Numbers.

However, in a quirk unique to one bank's computer system, the Social Insurance Numbers were uploaded and posted to the bank statements of tax beneficiaries who happened to be that bank's customers. The numbers were also visible on their online banking pages.

While the glitch prompted no further calls to the government or the bank, PWGSC fixed the technical problem and took steps to ensure that all future direct deposit payments include only encrypted Social Insurance Numbers.

The Department also undertook to review its programming procedures for new products, as well as its quality assurance processes, and to conduct training to prevent recurrences.

RISK: ACCESS TO INFORMATION REQUESTS

Year after year, we encounter incidents in which the processing of requests under the *Access to Information Act* and the *Privacy Act* leads to the inadvertent release of personal information that should have been protected. This year was no different.

4.2.9 HUMAN RIGHTS COMMISSION RELEASES NAME OF INFORMATION REQUESTER

The Canadian Human Rights Commission experienced one such slip-up when it accidentally released the name of the individual who was requesting access to information under the Act.

The individual's name, which should have been kept confidential, was included in a letter to a third party, who was being consulted on whether all or part of the requested information ought to be released.

The Commission notified the third party that he had received the requester's name in error, and directed him to protect it and not disseminate it further. The individual was also notified of the breach.

4.3 National Integrated Interagency Information System and Integrated Query Tool — Privacy Impact Assessments from the RCMP

We continued in 2010-2011 to review Privacy Impact Assessments related to a large-scale and evolving project that enables the sharing of investigative information collected by the Royal Canadian Mounted Police (RCMP) and provincial, territorial, aboriginal and municipal police forces — amongst themselves and with federal government departments.

The National Integrated Interagency Information System (N-III) data-sharing structure consists of two systems.

- One is the Police Information Portal (PIP), which allows police agencies to share detailed occurrence-level information from their respective records-management systems. There are numerous such records-management systems in police forces across Canada. One example is the RCMP's PROS, the Police Reporting and Occurrence System, which is described in section 2.2 of this report.

- The second element of the N-III data-sharing structure is the Integrated Query Tool (IQT), which is used by federal departments and agencies involved in public safety and security in order to access law-enforcement information contained in the PIP. In all, 34 federal institutions have access to the PIP. Some,

such as the Canada Border Services Agency, Passport Canada and the Financial Transactions and Reports Analysis Centre of Canada, have used the IQT.

We received and reviewed an overarching Privacy Impact Assessment on this program from Public Safety Canada, as well as several related assessments from participating federal agencies.

Our concerns

Based on our reviews, we continue to be concerned by the extent to which occurrence and case file information is being shared.

Unlike the Canadian Police Information Centre (CPIC) database, which contains factual information about criminal charges and their disposition through the court system (see section 2.2 of this report for more information), the PIP allows access to police records systems containing detailed information about, or provided by, witnesses, victims, family members and others associated, however tangentially, with an investigation.

Such information may be highly subjective and may, in fact, indicate no wrongdoing at all. Used without the appropriate context and safeguards, it could lead to detrimental outcomes for innocent individuals.

Our recommendations

We continue to advocate for publicly transparent controls over the sharing of this information, with accountability for stewardship of the information resting with Public Safety Canada.

Among other recommendations, we called on Public Safety Canada to appoint a Chief Privacy Officer to oversee the use of the personal information in the PIP.

4.4 Follow-ups on Previous Audits

Under section 37 of the *Privacy Act*, the Privacy Commissioner has the discretion to carry out audits to ensure that federal departments and agencies are complying with sections 4 to 8 of the Act. Those sections relate to the appropriate collection, use, retention, disclosure and disposal of personal information under the organizations' control.

If an audit finds any shortcomings with respect to compliance, the Commissioner can recommend remedial actions. These recommendations are made to the institution, and may also be published in annual or special reports to Parliament.

Because the Act provides no further enforcement powers, our Office sometimes conducts follow-up audits to determine whether a previously audited organization is acting on our recommendations, or following through on past commitments.

This year we followed up on three previous audits. One, focusing on the RCMP's handling of its exempt databanks, is described in section 2.5 of this report. Two other audits, where a key element was the protection of personal information from inappropriate disclosure, are described here. They are:

- Canadian Passport Operations (2008)

- Privacy Management Frameworks within Selected Federal Institutions (2009)

Overall, we concluded that the audited entities have responded positively: 32 of the 34 recommendations we made in the three follow-up audits — 94 percent — had been fully or substantially implemented, and work has begun on one more.

4.4.1 CANADIAN PASSPORT OPERATIONS

We checked up on the progress that Passport Canada, a special operating agency of the Department of Foreign Affairs and International Trade (DFAIT), has made since we completed our audit of its activities in December 2008. That audit highlighted some deficiencies that posed an appreciable risk to the protection of personal information of passport applicants.

In particular, we found weaknesses in the application process; the way personal information was collected and stored; how it could be accessed; and how it was destroyed.

We made 15 recommendations for improving the agency's privacy protections.

Passport Canada and DFAIT response

So far, Passport Canada and its parent department have indicated to us that they have fully or substantially implemented 14 of those recommendations and that the remaining one has been partially addressed.

Among other things, the institutions told us they have undertaken the following activities in response to our audit:

- ***implementing measures and technical safeguards to minimize the risk of inappropriate access to passport information;***
- ***modifying the layout of Passport Canada public service partitions to enhance privacy for clients;***
- ***reducing the retention period for passport applications and related documentation;***
- ***encrypting the network links between Passport Canada and the Department of Foreign Affairs, as well as data residing on Passport Canada's Case Management System; and***
- ***establishing a privacy breach directive.***

While some work remains necessary to fully address all of our recommendations, our follow-up inquiries suggest that significant progress has been made in strengthening controls to protect the privacy of passport applicants.

4.4.2 PRIVACY MANAGEMENT FRAMEWORKS WITHIN SELECTED FEDERAL INSTITUTIONS

In February 2009, the Commissioner submitted a special report to Parliament that described our examination of the privacy management frameworks of four federal institutions — Elections Canada, Passport Canada, the Canada Revenue Agency and the Service Canada portion of the department then referred to as Human Resources and Social Development Canada.

Each institution's privacy management framework was at a different stage of maturity at the time. While we noted good privacy practices, we also identified opportunities for improvement.

In all we made 15 recommendations, many of them directed at strengthening governance and accountability for privacy, expanding privacy awareness training, and addressing shortcomings in the management of information-sharing agreements.

Entities' responses

The audited entities indicated to us that they have fully or substantially implemented 14 of our 15 recommendations. For example:

- **Elections Canada has purged from its database all information on individuals under 18 years of age, and has implemented measures to ensure privacy risks are considered for new initiatives.**
- **The department now renamed Human Resources and Skills Development Canada has strengthened and consolidated its privacy governance and oversight processes, and has created a departmental inventory of personal information-sharing agreements.**
- **The Canada Revenue Agency has developed a privacy policy suite that formalizes and defines roles, responsibilities and accountabilities throughout the institution. In addition, the Security and Internal Affairs Directorate and the Access to Information and Privacy Directorate have established an information-sharing agreement with respect to privacy breach reporting.**

We will continue to follow the institutions' progress in fully implementing the Commissioner's recommendations.

4.5 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 if, in the opinion of the head of the institution,

> a) the public interest in disclosure clearly outweighs any resulting invasion of privacy, or
>
> b) the disclosure would clearly benefit the individual to whom the information relates.

Institutions planning to make a public interest disclosure are required to notify our Office in writing — prior to the disclosure where reasonably practicable or, in the alternative, immediately afterwards.

Our Office reviews the disclosure and, if the individual whose personal information is being disclosed has not been notified, and if we feel it is reasonable to do so, we encourage the department to issue the notification. The department usually agrees to our suggestion but, if it refuses, the Privacy Commissioner has the power to notify the individual herself.

During the 2010-2011 fiscal year, we handled 80 disclosures under section 8(2)(m), down by nearly one-quarter from the 104 we dealt with the year before.

Most common disclosures

- *Department of Foreign Affairs and International Trade*

The Department of Foreign Affairs and International Trade made 34 disclosures in 2010-2011, the most of any institution. Most commonly, the Department released to provincial or territorial public health authorities the contact information of people who may have been exposed to tuberculosis infection from another passenger on a flight.

In another case, the Department disclosed a deceased woman's passport application to her two sons, enabling them to confirm her Canadian birth and apply for Canadian citizenship.

- *Correctional Service of Canada*

The Correctional Service of Canada made 16 disclosures under section 8(2)(m), typically for two types of reasons: To inform the media or victim services groups about an escaped inmate or violent incidents unfolding within an institution, or to inform family members about the circumstances surrounding the death of an inmate.

In June and September 2010, the Service also released the personal information of a deceased inmate to the Canadian Association of Elizabeth Fry Societies following a Federal Court ruling.

- *Royal Canadian Mounted Police*

The Royal Canadian Mounted Police (RCMP) made 10 public interest disclosures in the past fiscal year. Some related to individuals being released into the community after serving time for sexual assault or possession of child pornography. There were also instances in which information involving sexual offences was disclosed to local police detachments for further investigation.

Other examples

Some other disclosures made under section 8(2)(m) last year involved these situations:

- The Immigration and Refugee Board disclosed on its website that an individual was prohibited from appearing as counsel before the board until he satisfied the board that he was not charging fees for his services. The information was also shared with the Canadian Society of Immigration Consultants and all provincial and territorial law societies.

- In December 2010, the Office of the Auditor General tabled an audit report containing personal information about the former Public Sector Integrity Commissioner of Canada.

CHAPTER 5

The OPC in Action

Strengthening the Privacy Rights of Canadians

Upon her reappointment to a second term in December 2010, Privacy Commissioner Jennifer Stoddart highlighted three priorities for the next three years:

- Leadership on priority privacy issues,
- Supporting Canadians, organizations and institutions to make informed privacy decisions, and
- Service delivery to Parliament and all Canadians.

Of course, we have been moving in this direction for many years and, as the previous chapters of this annual report describe, we made significant further strides in 2010-2011.

This chapter outlines additional work we have done to advance our mission to protect and promote the privacy rights of individuals.

The chapter describes how we respond to the inquiries and complaints of citizens who feel their rights have been violated by departments and agencies. It also discusses our work in support of Parliament and federal institutions, as well as our efforts to further the state of knowledge about privacy issues.

You will find the following sections in this chapter:

5.1 Our "Front Office" Work

5.1.1 INQUIRIES

***Received*:** In 2010-2011 we received 1,944 inquiries from Canadians about privacy-related matters arising from their dealings with the Government of Canada. We received a further 2,188 inquiries about issues that related to privacy, but where it was unclear whether the public- or the private-sector privacy law applied.

The total of these inquiries was down 24 percent from last year. Since the number of visits to our Office website continues to rise — up by 31 percent since 2007-2008 to 2.2 million visitors in 2010-2011 — we surmise that more people are going online to find answers to their privacy-related questions. There were another 1.01 million visits to our blogs and other websites during the past fiscal year, a number that has held steady from the year before.

Closed: Our inquiries unit responded to 1,859 inquiries related directly to the *Privacy Act* in 2010-2011, a number that was likewise down by 30 percent from the year before. Most of those contacts (56 percent) were by phone, although people also mailed, faxed and e-mailed their inquiries, or walked into our Office with their questions.

We fielded another 2,183 inquiries where the applicable law could not be determined, or that pertained to neither of the two privacy laws — a 24-percent decline from 2009-2010. (See Appendix 3 for full statistics.)

5.1.2 EARLY RESOLUTION OF COMPLAINTS

In pursuing our goal of enhanced service to Canadians, we understand that their issues and concerns must be addressed in a manner that is at once effective and efficient. A big part of that is the rapid resolution of complaints. The best way to speed up the process is to divert a complaint toward a satisfactory conclusion without triggering a formal investigation.

For that reason, we intensified our efforts to resolve complaints without investigations, and have assigned one officer specifically to this task.

Early resolution is often a matter of sharing information with the complainant or the department and clearing up misunderstandings.

For example, complainants are sometimes satisfied once they are told how similar complaints were resolved in the past. If departments in similar circumstances were found to have complied with the *Privacy Act*, complainants tend to accept that there is no point in proceeding with another investigation.

Similarly, complainants who unsuccessfully sought access to their personal information may be unaware of statutory exemptions that the withholding department is permitted to apply. Once they understand the law, some complainants are satisfied and the matter is considered resolved.

Early Resolution

When a complaint is filed under the *Privacy Act*, our complaints registrar determines whether it could be a candidate for early resolution. This determination is based on factors such as the apparent complexity of the case, and whether it appears to involve issues that have been addressed in the past.

In about one-quarter of the cases, the issue proves to be unsuitable for early resolution, or the parties are unwilling to come to terms in their dispute. In those situations, the case is reassigned for a formal investigation.

On average, our early-resolution files were closed in 3.6 months in 2010-2011, compared to eight months for the files that required formal investigations.

Many factors contribute to the relatively rapid resolution of files that do not require a formal investigation. Sometimes, for instance, the issues can be cleared up with little more than a phone call.

Moreover, while investigations are sealed off with a formal letter of finding, which can take some time to draft, early resolution cases are quickly summarized in an internal report that serves as a reference for similar circumstances in future.

In 2010-2011, we received 98 complaints that we identified as candidates for early resolution. Of those, 15 files were received later in the fiscal year and remained unresolved by March 31, 2011.

Of the remaining 83 files received and closed during the fiscal year, 61 were closed through the early-resolution process, while the remaining 22 ended up, for various reasons, being assigned to investigators.

In addition, our early-resolution efforts successfully handled another 17 of the 22 early-resolution case files that had been opened in 2009-2010 and were being treated in 2010-2011. The remaining five held-over cases were referred to investigators.

In total, then, 78 complaints that in the past would likely have been handled through more resource-intensive investigations were resolved rapidly and satisfactorily under the early-resolution process in 2010-2011. As a proportion of all the 105 files we had identified as candidates for early resolution, this represents a success rate of 74 percent.

Signed, sealed and delivered

A man complained about what he perceived to be a *Privacy Act* violation by Canada Post after being asked to provide an electronically scanned signature in order to pick up a parcel.

Our early resolution officer contacted Canada Post, which advised that individuals are not obliged to sign for a package. They can print their names, provide initials, or simply decline to sign. If an electronic signature is provided, the sender of the parcel can use a specially assigned personal information number to view it on the agency's website during a 60-day period.

We passed this information along to the complainant, who said he was pleased to hear that he did not have to furnish his signature. The matter was deemed resolved.

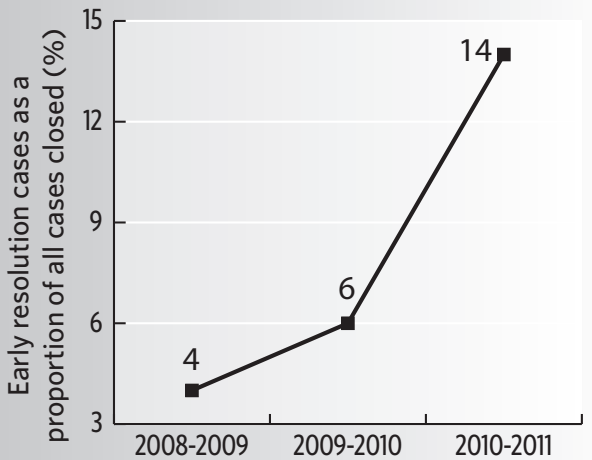
GRADUAL PROGRESS

These 78 cases also represent 14 percent of all the cases we closed during the fiscal year.

By comparison, 68 files were successfully closed using early-resolution strategies in 2009-2010, comprising just six percent of that year's caseload. The year before we closed 42 of 990 cases (four percent) in this manner.

As gratifying as it is to note this trend, the truth is that progress is slow. As an option for treating complaints, early resolution is not always appropriate.

PROPORTION OF FILES CLOSED THROUGH EARLY RESOLUTION STRATEGIES



Some issues, for instance, are just too complex. Others point to systemic problems. Still others appear on their face to involve a privacy violation so egregious that an investigation is called for. Such cases are referred directly to an investigator.

Although we have not had an opportunity to study the matter formally, we have observed several other factors that stand in the way of a more enthusiastic embrace of the early-resolution approach.

For example, some complainants generate files that contain dozens, even hundreds, of requests for access to personal information, held in the databanks of numerous federal institutions. Under such circumstances, early resolution is a vanishingly faint hope.

There are also fewer options to achieve "customer satisfaction" in the public sector than in the private sector. While a bank might waive some fees to make a client happy, or a store might throw in a free product as a peace offering, government has fewer options for settling disputes in a quick and relatively informal way.

Even so, we are cautiously optimistic about the outcome of our early-resolution efforts to date. The success rate has grown, even if only modestly, and we will continue to learn from and build on our experiences. We have every intention of persisting in this process in the years ahead.

5.1.3 COMPLAINTS

In all we received 708 complaints last year, up six percent from the 665 we received in 2009-2010. Even though we were successful in diverting 76 of them with early-resolution strategies, 632 files were sent on to investigators in 2010-2011.

In the past, the most common reason people filed complaints with our Office was if they felt a federal institution had taken too long to respond to their requests for personal information.

In 2010-2011, however, time-limit complaints* fell to second spot, accounting for 251 of the 708 complaints (36 percent) we received. The most common complaints related to problems people encountered in gaining access to their personal information. Such access complaints comprised 328 of our complaints, or 46 percent.

* Complaint types are defined in Appendix 1.

The remaining 129 complaints (18 percent) related to the collection, use, disclosure or retention of personal information by government departments or agencies.*

MOST COMMON COMPLAINT TYPES RECEIVED

	Number	Percentage
Access: Difficulties gaining access to personal information	328	46
Time Limits: Concerns that an institution took too long to respond to a request for access to personal information	251	36
Privacy: Concerns about an institution's collection, use, disclosure, retention or disposal of personal information	129	18
Total	**708**	**100**

In 2010-2011, the largest share of complaints originated in Ontario (30 percent), Quebec (27 percent), and British Columbia (23 percent). A similar pattern, reflecting Canada's population distribution, is seen in most years.

Canadians living abroad have the same rights of access to their personal information as those living in Canada, and two people exercised those rights in 2010-2011.

As in every other year, the lion's share of complaints we received (276, or 39 percent of the total) were laid against the Correctional Service of Canada. All but 23 of those complaints came from people having trouble accessing their personal information, or because they felt the institution had taken too long to respond to their requests for information.

The number of complaints against that Department in 2010-2011 was down by five percent from the 290 complaints laid the year before. However, the overall trend is upward: Indeed, there has been a 42-percent increase in complaints against the Correctional Service of Canada since 2006-2007.

In a pattern similar to other years, the Royal Canadian Mounted Police (RCMP), the Department of National Defence and the Canada Revenue Agency were next in terms of complaints received — 75, 65 and 53 respectively.

* Detailed data tables are in Appendix 3.

Departments that received a lot of complaints this year have generally also been in our top-10 list in other years. Because of their mandates, some institutions are required to hold a substantial amount of personal information. Therefore, they are more likely to receive numerous requests for access to that information, which may, in turn, lead to complaints about the way the data is handled.

The number of complaints filed against an institution does not necessarily mean the organization is not compliant with the *Privacy Act*; this can only be established through investigation.

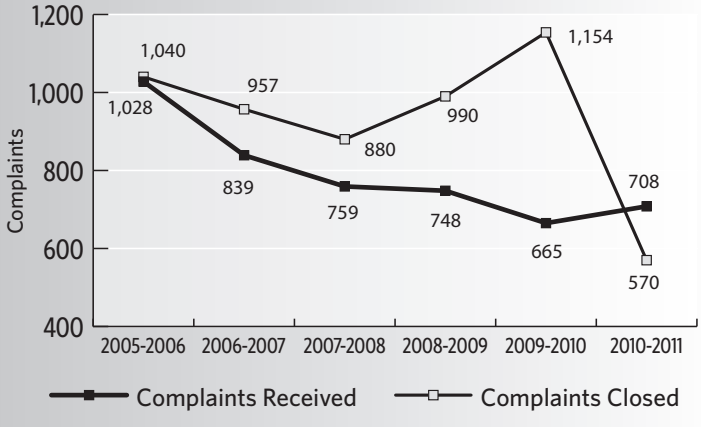
A newcomer to the top-10 chart this year was Veterans Affairs Canada. It received 15 complaints, compared with just two the year before. One of those complaints became the subject of an extensive investigation, which led us to follow up with a privacy-compliance audit. See section 3.1 of this report for more details.

5.1.4 INVESTIGATIONS AND OTHER DISPOSITIONS

We were able to close a total of 570 complaint files in 2010-2011, almost exactly half of the 1,154 we closed the year before. The principal reason for this decline is that two years of additional resources had come to an end at the conclusion of 2009-2010. These funds were specifically earmarked for clearing up an investigative backlog. At the start of 2008-2009, that backlog stood at 575 cases older than one year from the date of receipt.

The dedicated funds enabled us to hire investigators and engage in a blitz of strategies that ultimately wrestled our backlog of older files down to just 10 at the end of 2009-2010.

SIX-YEAR OVERVIEW OF COMPLAINTS RECEIVED AND CLOSED

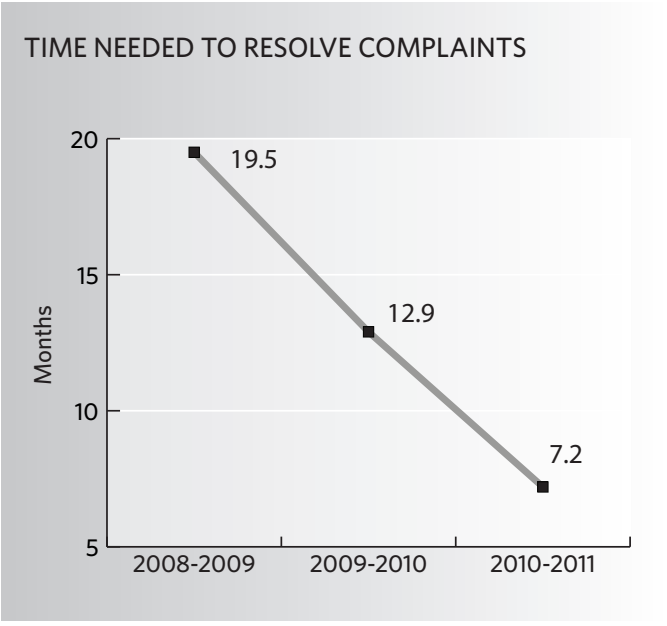


In the absence of those extra human and financial resources, however, we were unable to keep up with the complaints load last year. By the end of 2010-2011, our backlog had grown to 35 files.

On the plus side, however, our emphasis on early complaint resolution means we are continuing to shrink the time it takes to resolve each file, from a weighted average of 19.5 months in 2008-2009 to 12.9 months in 2009-2010 and just 7.2 months in 2010-2011. This represents a 63-percent decline in treatment times in just two years.

Indeed, the average treatment time for the 78 early-resolution cases we closed in 2010-2011 was just 3.6 months — less than half of the eight months it took to close the average case that went on to investigation.

This suggests that, if we can continue to increase the proportion of complaints that can be resolved without formal investigations, we can further trim the overall average time it takes to deal with our entire complaint load.



DISPOSITIONS

Complaint type		Investigative Findings			Other Dispositions			Total
		Well founded *	Not well founded	Resolved	Discontinued	Early resolution	Settled during investigation	
Access	Access	32	108	13	20	26	6	**205**
	Correction – Notation	1	0	0	0	3	0	**4**
	Fees	0	0	0	0	1	0	**1**
	Language	2	0	0	0	0	0	**2**
Time Limits	Extension Notice	12	10	0	2	0	0	**24**
	Time Limits	208	13	0	6	6	0	**233**
Privacy	Collection	1	4	0	0	9	0	**14**
	Retention and Disposal	4	1	0	3	0	0	**8**
	Use and Disclosure	21	13	0	10	33	2	**79**
Total		**281**	**149**	**13**	**41**	**78**	**8**	**570**

Aside from the 78 cases handled through the early-resolution process, 492 of the 570 files we closed in 2010-2011 were assigned to investigators. Of those, 41 were discontinued by the complainant. Another eight were settled during the investigation. That left 443 cases in which the investigation came to a conclusion and we issued formal findings.

Well founded: In 281 (63 percent) of those cases, we sided with the complainant. By far the most common reason for substantiating a complaint was because the respondent organization had not given the complainant timely access to his or her personal information. Complaints related to time limits resulted in 220 (79 percent) of our findings of "well founded."

* This includes 31 access cases previously categorized as "well founded and resolved".

This is not surprising and is, in fact, consistent with our observations in other years. Complainants do not typically file a complaint with us until after the end of the 30-day period during which organizations are generally obliged to produce requested personal information. If the statutory deadline has passed and the institution can make no compelling argument for an extension, the complaint is well founded, practically by definition.

Not well founded: In 149 cases, representing just over one-third of our 443 investigations, we concluded that the complaint was not well founded.

In 108 (72 percent) of these unsubstantiated cases, the complaint related to a frustrated attempt to gain access to personal information. The *Privacy Act* contains several exemptions, or reasons why departments or agencies may refuse to release personal information in their possession. If our investigation of an access complaint determines that an exemption had been properly invoked or applied, we would ordinarily issue a finding of "not well founded."

Resolved: Thirteen further cases, all of them involving complaints about access to personal information, were classed as "resolved" after a thorough investigation traced the problem back to a misunderstanding. In these instances, we found that the allegation was justified but a negotiated settlement was possible.

Privacy complaints: Privacy complaints, as a category, involve the collection, use, disclosure, retention or disposal of personal information. In all, we dealt with 101 of this type of investigation in 2010-2011, about 18 percent of the 570 cases we closed.

Well over half of these cases were discontinued (13), resolved early (42), or settled during the investigation (2).

Of the remaining 44 privacy cases that were investigated through to completion, 26 were upheld as well founded, and 18 were dismissed as not well founded. Irrespective of the finding, the majority of our completed privacy investigations focused on the improper use or disclosure of personal information.

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

5.2 Supporting Parliament

5.2.1 PARLIAMENTARY APPEARANCES

During 2010-2011, our Commissioner, Assistant Commissioner and other officials of the Office made 15 formal appearances before Members of Parliament and Senators, of which 14 related to matters wholly or in large part within the public sector. Among issues discussed were:

- the privacy implications of aviation safety measures;
- the extension of the Commissioner's seven-year term for another three years;
- new legislative initiatives such as the *Canada Consumer Product Safety Act* and the *Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service*;
- amendments to the *Criminal Code* to protect victims from sex offenders;
- the decision to make the long-form portion of the 2011 census voluntary rather than mandatory.

5.2.2 AVIATION SECURITY

We continued in 2010-2011 to express concerns about the privacy impacts of certain legislative measures related to aviation security, including the Advance Passenger Information/Passenger Name Record program, the Passenger Protect Program, and the Secure Flight Program under what was then called Bill C-42.

These measures have resulted in the creation of massive government databases, the use of secretive no-fly lists, the increased scrutiny of travellers and airport workers, and greater information sharing with foreign governments.

The Secure Flight initiative under Bill C-42, for instance, allows American or other authorities to collect personal information about travellers on flights to and from Canada that fly through American airspace. This, in turn, allows American authorities to prevent individuals from flying to or from Canada.

During our Parliamentary committee appearance on this initiative, we underscored that the Canadian government has a duty to protect the privacy and civil rights of its citizens.

We acknowledge that aviation security has always been important and, for reasons that we all understand, it has become a priority in Canada and around the world. Even so, we are of the view that privacy and security can be integrated; they do not need to be at odds.

From a practical perspective, the protection of privacy dictates that the collection of personal information be minimal; that retention periods be limited; that Canadians be informed of the scope of the collection of personal information; and that robust and accessible redress mechanisms be put in place. The effectiveness of security rests on the collection of information restricted to that which is relevant.

5.3 Reaching out to Federal Institutions

During the past fiscal year, our Office has continued to engage in constructive dialogue with as many as possible of the 250 federal institutions that fall under the authority of the *Privacy Act*.

Our objectives are to help organizations resolve outstanding privacy issues, to better understand our expectations for the completion of Privacy Impact Assessments, and to promote the importance of notifying our Office of privacy breaches.

Departments, for their part, have generally demonstrated a willingness to work with us to better safeguard the personal information of Canadians.

5.3.1 HELP WITH PRIVACY IMPACT ASSESSMENTS

The review of Privacy Impact Assessments is a vital role played by our Office. Through our review of these assessments of government programs or initiatives that involve the personal information of Canadians, we are able to evaluate institutional compliance with the *Privacy Act* (amongst other legal and policy requirements). We can also offer pertinent guidance on how programs can be tailored to operate in a more privacy-protective manner.

The details of many of the initiatives we review are not publicly available due to their sensitive nature. Through the assessment process, however, we serve as the public's eyes and ears to ensure the government is functioning in a manner respectful of the privacy rights of Canadians.

NEW DIRECTIVE

In line with this important role, we are continuing our efforts to reach out to federal institutions in order to help them adapt to the Treasury Board Secretariat's new Directive on Privacy Impact Assessments.

We also want to explain what our Office is looking for when we analyze assessments to make certain that important content is not overlooked and thorough assessments continue to be conducted.

Over the past fiscal year, we held consultations with the RCMP on its draft victims assistance policy; Citizenship and Immigration Canada in connection with its increasing collection of biometrics from certain immigrants, refugees and visa applicants; and the Canada Border Services Agency in conjunction with its renegotiation of Canada's Advance Passenger Information/ Passenger Name Record agreement with Europe.

Treasury Board Secretariat Directive on Privacy Impact Assessments

A new Treasury Board Secretariat Directive, in force since April 1, 2010, introduced the concept of a "core" Privacy Impact Assessment, which represents the minimum level of analysis required for certain low-risk files. In our view, however, such an analysis could be inadequate. Indeed, we have received files that could not be reviewed without additional information.

More than a year after the implementation of the Directive, public servants charged with preparing Privacy Impact Assessments were still awaiting the Treasury Board Secretariat's publication of formal supplementary guidance. In the absence of such key documentation, the quality of reviews has been inconsistent.

Our consultations often precede our receipt of a Privacy Impact Assessment, which helps ensure that privacy risks are recognized, assessed and mitigated before a program gets underway.

WORKSHOP AND *EXPECTATIONS* DOCUMENT

In March 2011 we hosted our second annual Privacy Impact Assessment workshop, which was attended by more than 100 officials from 40 federal institutions. The event allowed us to guide a diverse audience on how best to complete Privacy Impact Assessments.

We used the occasion of the workshop to launch a new guidance document, entitled *Expectations: A Guide for Submitting Privacy Impact Assessments to the Office of the Privacy Commissioner of Canada*.

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

The document, which has been posted to our website as a complement to the Treasury Board Secretariat's new Directive, outlines the type and depth of information and analysis that we would like to see included in Privacy Impact Assessments.

For more privacy-invasive initiatives, for instance, we ask institutions to demonstrate the necessity, proportionality and effectiveness of the proposed measure, and to explain whether less privacy-intrusive alternatives would be available.

Once this four-part test has been addressed and the proposed collection and use of personal information have been justified, we ask institutions to demonstrate the security of the information they aim to collect.

In particular, we encourage institutions to analyze the risks of their proposals against the 10 universal privacy and fair information practice principles of the Canadian Standards Association *Model Code for the Protection of Personal Information*. Those principles deal with matters such as accountability, the minimization of information collection, consent, safeguards, individual access and more.

In the meantime, we continue to explore other ways to expand our outreach efforts within the public service, and have surveyed workshop participants with an eye to fine-tuning our offerings on Privacy Impact Assessments for next time.

STREAMLINING THE PROCESS

At the same time, we continued this year to streamline our assessment review process and to focus our resources on initiatives posing the greatest risks to the privacy rights of Canadians. This year, for instance, we further refined and formalized our triage process.

Every Privacy Impact Assessment file we receive is examined by a review officer to assess the sensitivity of the information collected, the nature of the risks posed by the initiative, the numbers of Canadians affected by the program or activity, and whether the initiative falls into one of the four areas that we feel will have the greatest impact on privacy — public safety; information technology; genetic technologies; and the protection of identity integrity.

While we read and assess all files we receive, we conduct more in-depth reviews where, in our view, initiatives pose significant privacy risks or raise broader human rights or societal privacy issues. For these, we provide departments with detailed recommendations, and follow up to ensure risks have been mitigated.

5.3.2 PRIVACY PRACTICES FORUM

On March 15, our Office hosted its inaugural Privacy Practices Forum, an opportunity for federal public servants to share their experience and knowledge about ways to advance privacy in their respective departments.

In all, 64 employees from 15 departments and agencies registered to attend.

Representatives from four federal institutions described tools and processes that they have implemented in their respective workplaces. This was followed by small-group discussions among forum participants interested in further exploring specific topics or approaches.

The forum covered important matters such as privacy governance structures, breach-management protocols, web-based tools for preparing better Privacy Impact Assessments, and developing an internal policy for the use of social media.

The presentations were filmed so that they could be posted for later viewing on GCPEDIA, the online collaborative work tool for federal public servants.

5.3.3 CANADA SCHOOL OF PUBLIC SERVICE

A public service that understands its obligations to protect the personal information of Canadians in its care is critical to the functioning of our democratic system of government. That is why our Office continues to work with the Canada School of Public Service on ways to promote personal information protection among federal employees.

In October 2010, the Commissioner held a well-attended armchair discussion at the Gatineau, Que.-based common learning provider for the federal public service. She described how to integrate privacy considerations into broader government priorities and outlined the Office's priorities, activities and approaches aimed at strengthening privacy protections in the government.

The School has also agreed to host Management Excellence Series workshops on privacy. The workshops are designed to go beyond the day-to-day administration of databanks and personal information, to focus on the key considerations that senior policymakers should bear in mind when developing new programs and services that could affect the privacy rights of Canadians.

We are also working with the learning centre to develop privacy workshops for its new Deputy Ministers Series, which will offer another opportunity for top bureaucrats in federal institutions to meet and discuss emerging issues.

We continue to be interested in reviewing the organization's course offerings, to ensure that key privacy principles are imparted to all civil servants who require them in their daily activities.

5.4 Judicial Proceedings

Under the *Privacy Act*, the Privacy Commissioner may apply to or appear before the Federal Court in cases where a federal institution has denied an individual access to his or her personal information. Our involvement in such cases is described in section 3.4.

From time to time, however, our Office may seek to become involved as interveners in other matters before the courts or other tribunals, in order to clarify issues around the interpretation of certain provisions of the *Privacy Act*, or other issues involving privacy or personal information. As well, our Office may sometimes face applications for judicial review.

Here are summaries of cases in which we were involved during 2010-2011. 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.

5.4.1 *PROFESSIONAL INSTITUTE OF THE PUBLIC SERVICE OF CANADA v. CANADA REVENUE AGENCY* 2011 PSLRB 34

In this case, an employee of the Canada Revenue Agency, whose unionized workplace was represented by the Professional Institute of the Public Service of Canada, objected to her employer disclosing her home contact information to the union, pursuant to a July 2008 Order by the Public Service Labour Relations Board (PSLRB). The employee was a "Rand Deductee", an employee who chooses not to become a member of the union, but must nevertheless pay union dues.

The union and the employer came to an agreement under which the personal information of employees within the bargaining unit may be shared with the employer. This agreement was, in turn, sanctioned by the PSLRB in its July 2008 Order.

Unhappy with the agreement, however, the employee in 2009 applied to the Federal Court of Appeal for a judicial review of the Order, on grounds of privacy and procedural fairness.

In February 2010, the Federal Court of Appeal granted the employee's application and sent the case back to the PSLRB for redetermination. In its decision, the Federal Court specified that our Office should be notified of the rehearing and granted full intervener status. Accordingly, our Office participated as an intervener at the redetermination hearings before the PSLRB in November 2010.

We took the view that the union did not need an employee's home contact information in order to fulfill its obligations under statute to inform all members in the bargaining unit of a strike vote.

The Board issued its decision on March 23, 2011, finding that the employer could, under the *Public Service Labour Relations Act* and the *Privacy Act*, provide the union with employee home contact information without the employee's consent.

However, the adjudicator made a number of privacy-enhancing amendments to the impugned information-sharing agreement between the employer and the union.

The PSLRB also acknowledged that, in the context of this case, there was a gap in statutory privacy protection for unionized employees. Given the activity in which the union was engaged, neither the *Privacy Act* nor the *Personal Information Protection and Electronic Documents Act* applied to it.

In April 2011, the employee once again applied for a judicial review before the Federal Court of the PSLRB's Order following the re-determination hearing. The matter was transferred to the Federal Court of Appeal on May 5, 2011, further to an order of the Federal Court.

5.4.2 *X. v. PUBLIC SERVICE COMMISSION* FEDERAL COURT FILE NO. T-1659-08

In a long-running case whose progress has been tracked in previous annual reports, an individual was investigated by the Public Service Commission for allegedly engaging in improper political activities while working for the federal public service.

Following an internal investigation into the matter, the Public Service Commission determined that it would post a summary of its findings on the Internet, in keeping with the Commission's practices at the time. The individual felt that posting the findings

would be an unjustified invasion of his privacy rights, and filed an application for judicial review before the Federal Court.

The matter raised issues about the disclosure of personal information on the Internet and the extent to which the open courts principle applies to administrative tribunals such as the Public Service Commission.

The Privacy Commissioner sought and was granted intervener status to assist the Court with some of the legal issues raised in the application.

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

The applicant ultimately discontinued the application.

5.4.3 *X. v. PRIVACY COMMISSIONER OF CANADA AND INFORMATION COMMISSIONER OF CANADA*
COURT FILE NO. DC-09-88-JR

As reported in last year's annual report, this was a judicial review application, filed in the Ontario Superior Court of Justice, Divisional Court, in which the applicant sought an order of mandamus requiring the Office of the Privacy Commissioner of Canada and the Office of the Information Commissioner of Canada to complete investigations regarding complaints filed by the applicant with both offices. The application was ultimately dismissed on Jan. 22, 2010.

The matter, however, resumed during the past fiscal year, when the applicant sought to have the order dismissing the application set aside by the Ontario Court of Appeal.

The Court of Appeal instructed the applicant to follow proper procedure by going to the Ontario Divisional Court to seek to have the Order set aside, but ultimately adjourned the applicant's appeal to no fixed date.

The applicant sought to appeal the Court of Appeal's ruling, but was unsuccessful. To date, the applicant has not pursued the matter in Ontario Divisional Court.

5.5 Advancing Knowledge

5.5.1 COMMISSIONED RESEARCH

We commissioned several research papers over the past year. Most examined the factors that could challenge the integrity and protection of personal identity, which is one of our strategic priorities. Research reports that were directly relevant to the public sector include the following:

- *Qualitative Research with ATIP Officers*

We commissioned Phoenix Strategic Perspectives Inc. to interview a selection of access-to-information and privacy officers to learn more about their top concerns. These turned out to include the proper preparation of Privacy Impact Assessments, and the challenge of safeguarding personal information at a time when the government is collecting ever more data.

The government's increasing ability to monitor citizen activity through technologies such as GPS systems, traffic surveillance, web crawlers and monitoring of social media sites was identified as a key emerging issue.

Other issues cited by the respondents were the difficulty of balancing the right to privacy with the need for security and public safety, and ensuring privacy while embracing social media.

Our Office will use this study to better understand the context in which these officers work, and how we can continue to support them.

- *Research on Privacy and Developing Countries*

Dr. Gus Hosein, a visiting senior fellow at the London School of Economics and Political Science with research interests in technology policy, regulation and civil liberties, notes that nearly all international declarations of rights include explicit protections for privacy.

It is often argued that, for developing countries, economic development is more important than human rights such as privacy. The reverse, however, is arguably true, given that respect for human rights is essential to good governance.

The paper explains that developing countries are at the forefront of the development and adoption of new surveillance practices. National identification systems, surveillance of

movement and communications, DNA databases, and electronic health systems have all found traction in the developing world.

However, the paper notes that the laws to protect data in these countries are lagging behind.

The author suggests that Canada's International Development Research Centre has led the world with unprecedented levels of support for capacity building on privacy in developing countries.

As well, our Office was recognized for being actively involved internationally in privacy promotion and protection, primarily through groups such as APEC, the Ibero-American Forum of Data Protection Authorities, and the Association of Francophone Data Protection Authorities.

- *Guided Literature Review on Identity Management Systems*

In June 2010, the federal government announced the appointment of a Task Force for the Payments System Review to examine the existing system by which Canadians pay for products and services online. The task force is to report to the Department of Finance by the end of 2011.

In anticipation of the task force's consultation report, we commissioned a literature review of Federated Identity Management systems.

The review, prepared by Jennifer Barrigar, a specialist in privacy and technology issues and a former counsel with our Office's legal services branch, concluded that third-party authentication and reliable online identity markers have the potential to reduce the risk of identity theft and fraud, and in so doing enhance people's comfort with e-commerce.

Implemented poorly, however, those same features could facilitate — rather than prevent — criminal access to personal information.

Similarly, having a single information repository and a single password or access token has the power to increase security, but the flawed implementation of such security measures could grant unauthorized access to an unprecedented collection of information.

The review suggested that such identity-management systems, which will also become more prevalent in government, should be subject to flexible regulation that focuses on the information rather than the specific technology. Meaningful knowledge and consent on the part of users is also imperative.

5.5.2 INSTITUTE OF PUBLIC ADMINISTRATION ROUNDTABLES

Our Office funded the Institute of Public Administration of Canada to hold roundtables on the use of social media in government, including a consideration of the related privacy issues. Five roundtables were held over the year in Edmonton, Victoria, Toronto, Kingston, Ont., and Ottawa, attracting public servants from the federal, provincial, and municipal levels of government, as well as representatives from academia.

The roundtables established that social media tools can at once help institutions better achieve their missions, while also facilitating a more effective management style. They can measurably reduce costs, increase productivity, and contribute to staff and citizen satisfaction. They can, moreover, be effectively used without violating privacy regulations.

The roundtables noted that most governments now have internal social media processes, such as the GCPEDIA in the Government of Canada, but there is no overall integration across jurisdictions. Among other things, the roundtables recommended:

- a central cross-government source of information and networking. Public servants could visit such a site to see guidelines and business cases developed in other jurisdictions. They could also use it to connect with others working on similar issues, post problems and share solutions.

- further work to clarify how governments can use social media to make public-sector organizations more productive and better able to meet today's complex challenges, while also improving policy development and implementation.

The institute's research aimed to bolster our Office's understanding of the implications of social media use in government, including measures of success, use of reporting tools, and cost/benefit analyses.

The work was also meant to inform social media implementation and use in other government departments, thus satisfying our mandate for public education and outreach.

The institute is inviting stakeholder feedback on the report, which is to be made public.

5.5.3 LA FRANCOPHONIE

Our Office continues to be an active member of the *Association francophone des autorités de protection des données personnelles* (AFAPDP), an association of data-protection authorities in French-speaking countries. Founded in Montreal in 2007, the association's mandate is to promote the protection of personal data by strengthening capacity among the membership and by exploring new challenges to privacy rights.

As several of the association's 24 members are developing states, the participation of the Office of the Privacy Commissioner of Canada constitutes a significant contribution to the furtherance of good governance practices in those countries.

At the association's annual general meeting in Paris in November 2010, Assistant Commissioner Chantal Bernier described the evolution of personal data protection in Canada, as well as the governance principles essential to independent privacy oversight.

The Year Ahead

This report details how our audits, investigations, Privacy Impact Assessment reviews, and interactions with Parliament, the public service and citizens served in 2010-2011 to strengthen the protection of personal information in the public sector.

But, as we peer ahead into the next year and beyond, it is evident that the challenges will only continue to mount.

Consider, for example, the issue of cybersecurity, a looming preoccupation for the Government of Canada and, indeed, governments around the world.

Certain aspects of enhanced cybersecurity, such as measures to better protect personal information in cyberspace, are crucial to the protection of privacy and are therefore welcome initiatives on the part of the government.

By contrast, however, certain other aspects — most notably the expansion of police powers in the Internet environment — continue to raise concerns. We will continue to express our view that such so-called lawful access measures must respect fundamental rights to privacy.

Canadians today are accustomed to secure communications that enable them to express themselves, create, share and innovate. They expect their government to deliver services in a confidential and trustworthy manner, and to be an irreproachable steward of their personal information.

At the same time, however, they also expect their government to be open and responsive, not paralyzed by an obsession with security.

In the year ahead, our Office will work to ensure that the security vulnerabilities of computer networks and government systems are confronted, but in ways that respect the law — be it the privacy rights arising from the *Canadian Charter of Rights and Freedoms*, the provisions of the *Privacy Act,* or the protection of privacy provisions in the *Criminal Code*.

As for the broader issues, one of the primary risks to privacy in the 21st century remains information sharing between government departments, levels of jurisdiction, and with other states. Ensuring oversight and review mechanisms are well thought out, properly resourced and carry meaningful consequences remains another major challenge for governance and control over personal information-handling practices.

And so, in all new programs and legal initiatives involving surveillance, monitoring or screening, our Office will continue to argue for open discussion, high standards of privacy protection, robust review mechanisms, strong judicial oversight and clear redress procedures, as well as a firm commitment to due process and the rule of law.

WORKING FOR CANADIANS

More specifically, we will produce in 2011-2012 a report on the overarching privacy concerns associated with a suite of nine Privacy Impact Assessments that we have received since 2007 in relation to Canada's anti-money laundering and anti-terrorist-financing regime.

Any common or systemic privacy risks and issues that we turn up will help inform our next mandated review of FINTRAC, the Financial Transactions Reports Analysis Centre of Canada. We are obliged to conduct such a review every other year, pursuant to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. The upcoming review will also examine measures that FINTRAC has implemented to address the findings contained in a full audit that we conducted in 2009.

We will also complete our audit of Veterans Affairs Canada, launched over the past fiscal year after a complaint investigation uncovered some serious and systemic problems in the Department. Our audit, which we expect to complete over the winter of 2011-2012, will determine whether the Department is acting on the recommendations we made in our report of findings in that investigation, and is implementing the 10-point action plan it developed in order to strengthen its own privacy policies and practices.

In the year ahead, we will continue to strengthen our internal processes and our capacity to deliver on our mandate on the basis of the best available evidence.

Thus, for instance, we plan to analyze all 500-plus Privacy Impact Assessments that have been submitted to our Office since 2002, in order to produce statistics on the nature of the files we receive, the types of issues we encounter, and which departments and agencies submit the majority of our files.

We are confident that this data will support the work of the entire Office, while also informing the public service, Parliament and Canadians about the value of the Privacy Impact Assessment review process.

Recognizing how challenging the evolving privacy landscape can be for public servants entrusted with the personal information of Canadians, we also intend to carry on with our outreach activities. Toward that end, we plan to build a collaborative workspace on GCconnex, the social networking site for federal public servants.

We also intend to host more of our practical hands-on sessions to help institutions prepare Privacy Impact Assessments. We have canvassed participants from our last Privacy Impact Assessment workshop for ideas, and will use the results of our recent survey of federal access-to-information and privacy co-ordinators to try to better address their needs.

With a renewed commitment to better serving Canadians, we will also continue to engage and educate citizens across Canada on privacy issues, protection of personal information, and their right of access to their own personal information.

We will do this by further strengthening our capacity to respond in a rapid and effective manner to their inquiries and complaints. We will also do it through public events, timely research, open discussions and seminars, and our burgeoning online presence.

As the issues of government information collection and protection grow more complex, the public trust of Canadians demands that the discussion remain accessible to citizens and focused on their lives.

Privacy is far too critical to our society and democratic values for it to become an issue of government alone.

APPENDIX 1
DEFINITIONS

COMPLAINT TYPES

1. Access

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

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

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

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

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

2. Privacy

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

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

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

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

3. Time Limits

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

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

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

FINDINGS AND OTHER DISPOSITIONS UNDER THE *PRIVACY ACT*

1. Investigative Findings

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

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

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

2. Other Dispositions

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

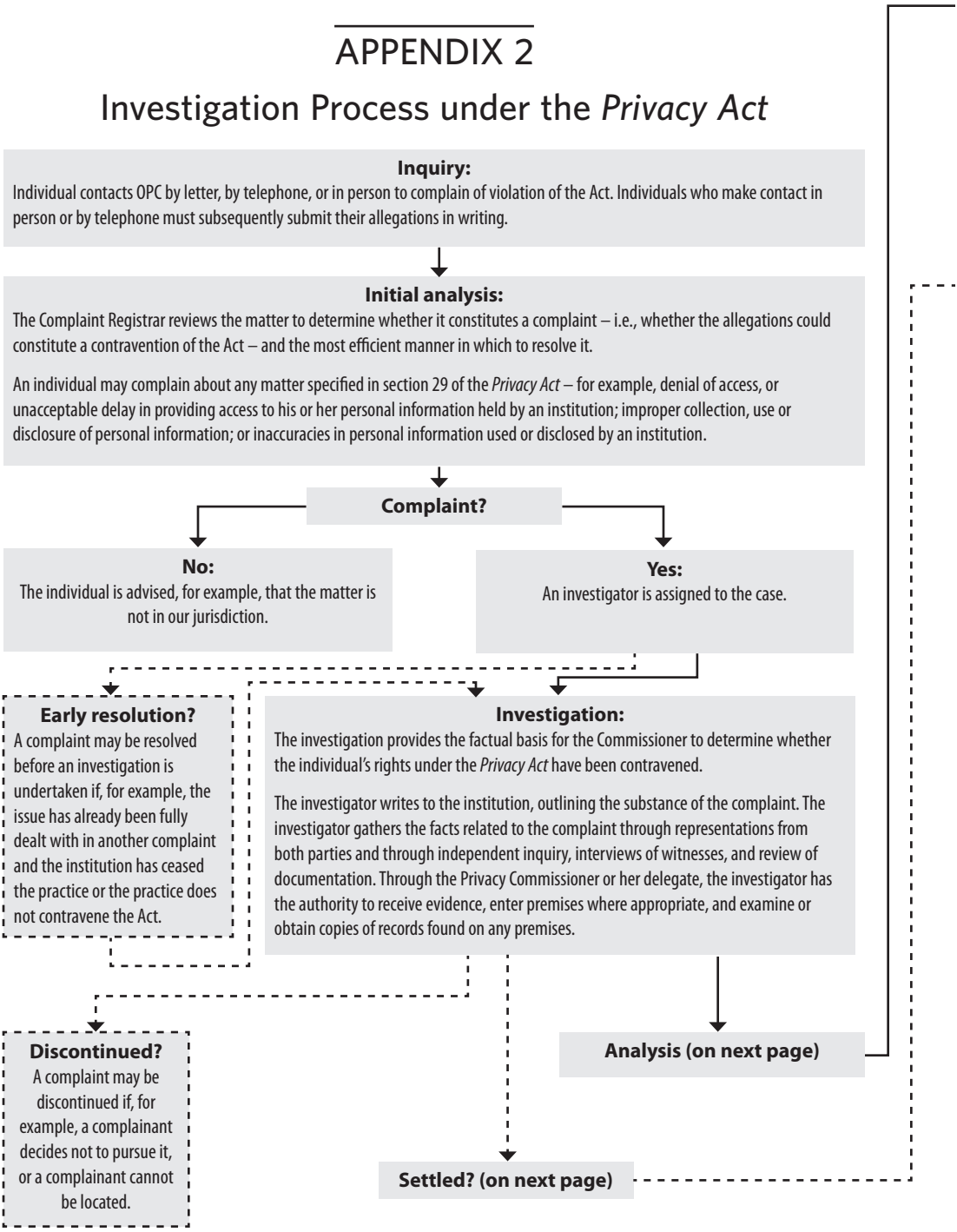
length with the individual and should he or she choose not to proceed further, the file is closed as "early resolution".

Settled during the course of investigation: The OPC helped negotiate a solution that satisfied all parties during the investigation, but did not issue a finding.

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

APPENDIX 2

Investigation Process under the *Privacy Act*



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

Analysis:

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

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

Settled?

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

Findings:

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

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

The possible findings are:

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

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

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

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

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

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

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

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

APPENDIX 3
Inquiries, Complaints and Investigations under the *Privacy Act*, April 1, 2010 to March 31, 2011

INQUIRIES STATISTICS

Inquiries Received under the *Privacy Act*

By telephone:	1,046
Other*:	898
Total:	1,944

General† Inquiries Received

By telephone:	1,974
Other:	214
Total:	2,188

Responses to Inquiries under the *Privacy Act*

By telephone:	1,034
Written:	825
Total:	1,859

Responses to General† Inquiries

By telephone:	1,972
Written:	211
Total:	2,183

* May include e-mail, postal mail, fax or walk-in inquiries.

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

COMPLAINTS RECEIVED BY COMPLAINT TYPE

Complaint Type	Number		Total	Percentage	Total by Complaint Type
	Early resolution	Formal Complaints			
Access	28	293	321	45	**Access 328**
Correction – Notation	2	4	6	1	
Fees	0	1	1	0.1	
Correction – Time Limits	0	1	1	0.1	**Time Limits 251**
Time Limits	3	231	234	33	
Extension Notice	0	16	16	2	
Collection	7	5	12	2	**Privacy 129**
Language	0	3	3	1	
Retention and Disposal	0	9	9	1	
Use and Disclosure	36	69	105	15	
Total	**76**	**632**	**708**	**100**	**708**

The most common category of complaints to our Office in 2010-2011 related to difficulties people were encountering in gaining access to their personal information in the hands of government departments or agencies. These complaints accounted for a combined total of 328, or 46 percent of all the complaints we received. The number of access complaints we received is up by 31 percent from 2009-2010.

The second-most common reason for people to file complaints with our Office related to the length of time that institutions were taking to respond to access requests. We received 251 time-limits complaints, just over one-third (35 percent) of our incoming caseload. This represented a 14-percent decline from the previous year.

Privacy complaints, which include problems related to the collection, use, disclosure, retention or disposal of personal information, comprised a total of 129 complaints, representing 18 percent of the total. This represented only a small (seven percent) increase from 2009-2010, when we had 122 of this category of complaints.

See Appendix 1 for definitions of complaint types.

TOP-10 INSTITUTIONS BY COMPLAINTS RECEIVED

Organization	Access			Time Limits			Privacy			Total
	Early resolution	Formal Complaints	Access Total	Early resolution	Formal Complaints	Time limits Total	Early resolution	Formal Complaints	Privacy Total	
Correctional Service of Canada	7	87	**94**	1	158	**159**	11	12	**23**	**276**
Royal Canadian Mounted Police	11	46	**57**	0	8	**8**	1	9	**10**	**75**
National Defence	0	42	**42**	0	19	**19**	1	3	**4**	**65**
Canada Revenue Agency	0	29	**29**	0	16	**16**	1	7	**8**	**53**
Canada Border Services Agency	0	15	**15**	0	9	**9**	1	4	**5**	**29**
Canada Post Corporation	2	5	**7**	0	3	**3**	7	10	**17**	**27**
Human Resources and Skills Development Canada	3	9	**12**	0	4	**4**	2	7	**9**	**25**
Citizenship and Immigration Canada	0	12	**12**	0	2	**2**	0	2	**2**	**16**
Canadian Security Intelligence Service	1	13	**14**	0	2	**2**	0	0	**0**	**16**
Veterans Affairs Canada	3	2	**5**	0	0	**0**	0	10	**10**	**15**
Other	3	38	**41**	2	27	**29**	19	22	**41**	**111**
Total	**30**	**298**	**328**	**3**	**248**	**251**	**43**	**86**	**129**	**708**

These 10 institutions account for 84 percent of all complaints received during 2010-2011. This proportion is virtually unchanged from the 85 percent of complaints represented by the top-10 departments and agencies in 2009-2010.

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.

COMPLAINTS RECEIVED BY INSTITUTION

Institution	Early resolution cases	Formal complaints	Total
Business Development Bank of Canada	0	1	**1**
Canada Border Services Agency	1	28	**29**
Canada Post Corporation	9	18	**27**
Canada Revenue Agency	1	52	**53**
Canadian Broadcasting Corporation	1	1	**2**
Canadian Food Inspection Agency	1	7	**8**
Canadian Human Rights Commission	1	3	**4**
Canadian Human Rights Tribunal	0	4	**4**
Canadian International Development Agency	0	1	**1**
Canadian Radio-television and Telecommunications Commission	1	0	**1**
Canadian Security Intelligence Service	1	15	**16**
Citizenship and Immigration Canada	0	16	**16**
Correctional Service of Canada	19	257	**276**
Environment Canada	0	1	**1**
Finance Canada	0	1	**1**
Financial Transactions and Reports Analysis Centre of Canada	1	2	**3**
Fisheries and Oceans Canada	0	4	**4**
Foreign Affairs and International Trade	1	7	**8**
Health Canada	0	8	**8**
Human Resources and Skills Development Canada	5	20	**25**
Immigration and Refugee Board	0	3	**3**
Indian and Northern Affairs Canada	1	0	**1**
Industry Canada	0	1	**1**
Justice Canada	0	9	**9**
Library and Archives Canada	0	2	**2**

COMPLAINTS RECEIVED BY INSTITUTION (cont.)

Institution	Early resolution cases	Formal complaints	Total
National Defence	1	64	**65**
National Parole Board	0	1	**1**
National Research Council of Canada	0	1	**1**
Office of the Commissioner of Official Languages	0	1	**1**
Office of the Information Commissioner of Canada	0	4	**4**
Parks Canada	0	2	**2**
Passport Canada	2	0	**2**
Public Prosecution Service of Canada	0	1	**1**
Public Safety Canada	0	1	**1**
Public Service Commission of Canada	0	1	**1**
Public Service Labour Relations Board	1	1	**2**
Public Works and Government Services Canada	7	1	**8**
Royal Canadian Mounted Police	12	63	**75**
Statistics Canada	2	2	**4**
Transport Canada	1	13	**14**
Treasury Board of Canada Secretariat	4	1	**5**
Veterans Affairs Canada	3	12	**15**
VIA Rail Canada	0	1	**1**
Western Economic Diversification Canada	0	1	**1**
Total	**76**	**632**	**708**

COMPLAINTS RECEIVED BY PROVINCE/TERRITORY

Province/Territory	Complaints	Early resolution cases	Total	Percentage
Ontario	192	21	**213**	30
Quebec	173	19	**192**	27
British Columbia	142	20	**162**	23
Alberta	43	7	**50**	7
Newfoundland and Labrador	24	0	**24**	3
Manitoba	20	2	**22**	3
Saskatchewan	18	0	**18**	3
Nova Scotia	8	2	**10**	1
New Brunswick	7	2	**9**	1
Prince Edward Island	4	1	**5**	0.7
Nunavut	0	1	**1**	0.1
International*	1	1	**2**	0.2
Total	**632**	**76**	**708**	**100**

The number of complaints originating in Quebec more than doubled between 2009-2010 and 2010-2011, rising from 87 (13 percent of all complaints) to 192, or 27 percent of all complaints during the past fiscal year. This increase, most of it related to multiple complaints from a small group of complainants, moved the province from third place to second, ahead of British Columbia.

* 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 two people chose to exercise those rights in 2010-2011. 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.

DISPOSITION BY COMPLAINT TYPE

Complaint type		Investigative Findings			Other Dispositions			Total
		Well founded *	Not well founded	Resolved	Discontinued	Early resolution	Settled during investigation	
Access	Access	32	108	13	20	26	6	**205**
	Correction – Notation	1	0	0	0	3	0	**4**
	Fees	0	0	0	0	1	0	**1**
	Language	2	0	0	0	0	0	**2**
Time Limits	Extension Notice	12	10	0	2	0	0	**24**
	Time Limits	208	13	0	6	6	0	**233**
Privacy	Collection	1	4	0	0	9	0	**14**
	Retention and Disposal	4	1	0	3	0	0	**8**
	Use and Disclosure	21	13	0	10	33	2	**79**
Total		**281**	**149**	**13**	**41**	**78**	**8**	**570**

Time Limits: Complaints about the time it takes for institutions to respond to requests for access to personal information were the most common category of files we closed last year – a total of 257, or 45 percent of our caseload. Because most complainants only come to us after the statutory deadline for their complaint has passed, 220 (or 86 percent) of those complaints were well founded.

Access: We closed a total of 212 complaints about access to personal information, comprising 37 percent of all the complaints we closed last year. More than one-quarter of those cases were discontinued, resolved early or settled during investigation. Of the remaining 156 cases that were investigated, 108 (69 percent) were not substantiated upon investigation, while 35 (22 percent) were upheld as well founded. Another 13

* This includes 31 access cases previously categorized as "well founded and resolved".

access cases were investigated and found to have merit, but were resolved through negotiation rather than a formal finding.

Privacy: Cases involving the collection, use, disclosure, retention or disposal of personal information combined to account for 101, or 18 percent, of all complaints we closed in 2010-2011. Our investigations found that 26 of the complaints were well founded, and 18 were not well founded. The vast majority of all privacy complaints related to the improper use or disclosure of personal information.

DISPOSITION OF TIME LIMITS COMPLAINTS BY INSTITUTION

	Well founded	Not well founded	Early resolution	Settled during investigation	Discontinued	Total
Canada Border Services Agency	5	2	1	0	0	**8**
Canada Post Corporation	0	0	0	0	3	**3**
Canada Revenue Agency	20	4	1	0	0	**25**
Canadian Food Inspection Agency	4	2	1	0	0	**7**
Canadian Human Rights Commission	0	0	1	0	0	**1**
Canadian Security Intelligence Service	1	0	0	0	0	**1**
Citizenship and Immigration Canada	3	0	0	0	0	**3**
Correctional Service of Canada	141	5	2	0	4	**152**
Fisheries and Oceans Canada	0	1	0	0	0	**2**
Foreign Affairs and International Trade	0	1	0	0	0	**1**
Health Canada	3	1	0	0	0	**4**
Human Resources and Skills Development Canada	4	2	0	0	0	**6**
Justice Canada	2	2	0	0	0	**4**
National Defence	23	0	0	0	0	**23**
Public Health Agency of Canada	1	0	0	0	0	**1**
Public Prosecution Service of Canada	1	0	0	0	0	**1**
Public Works and Government Services Canada	0	0	0	0	1	**1**
Royal Canadian Mounted Police	4	3	0	0	0	**7**
Transport Canada	8	0	0	0	0	**8**
Total	**220**	**23**	**6**	**0**	**8**	**257**

DISPOSITION OF ACCESS AND PRIVACY COMPLAINTS BY INSTITUTION

	Well founded*	Not well founded	Resolved	Early resolution	Settled during investigation	Discontinued	Total
Agriculture and Agri-Food Canada	1	0	0	0	0	0	**1**
Canada Border Services Agency	2	4	0	3	2	1	**12**
Canada Post Corporation	10	5	2	9	0	1	**27**
Canada Revenue Agency	2	8	0	1	1	2	**14**
Canadian Broadcasting Corporation	2	0	0	1	0	0	**3**
Canadian Human Rights Commission	1	0	0	1	0	0	**2**
Canadian Security Intelligence Service	0	7	0	1	0	0	**8**
Canadian Wheat Board	0	1	0	0	0	0	**1**
Citizenship and Immigration Canada	2	0	1	1	1	1	**6**
Correctional Service of Canada	14	47	4	15	1	10	**91**
Environment Canada	0	0	1	0	0	0	**1**
Finance Canada	0	1	0	0	0	0	**1**
Financial Transactions and Reports Analysis Centre of Canada	0	0	0	1	0	0	**1**
Foreign Affairs and International Trade	1	1	1	1	0	0	**4**
Health Canada	2	0	0	0	0	2	**4**
Human Resources and Skills Development Canada	4	3	1	3	1	0	**12**
Immigration and Refugee Board	0	1	0	0	0	0	**1**
Indian and Northern Affairs Canada	1	0	0	1	1	1	**4**
Industry Canada	1	0	0	0	0	0	**1**
Justice Canada	1	2	0	0	0	0	**3**
Library and Archives Canada	0	0	0	0	0	1	**1**
National Defence	8	22	0	2	1	4	**37**
National Parole Board	1	0	1	0	0	0	**2**
National Research Council of Canada	0	0	0	1	0	0	**1**

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

	Well founded*	Not well founded	Resolved	Early Resolution	Settled during investigation	Discontinued	Total
Office of the Commissioner of Official Languages	0	0	0	0	0	1	**1**
Office of the Information Commissioner of Canada	0	1	0	0	0	0	**1**
Parks Canada	0	1	0	0	0	0	**1**
Passport Canada	0	0	0	2	0	0	**2**
Public Health Agency of Canada	0	0	0	1	0	1	**2**
Public Prosecution Service of Canada	0	0	0	7	0	0	**7**
Public Safety Canada	0	0	1	0	0	0	**1**
Public Service Commission	0	3	0	0	0	0	**3**
Public Works and Government Services Canada	1	1	0	0	0	0	**2**
Royal Canadian Mounted Police	3	14	0	11	0	2	**30**
Social Science and Humanities Research Council of Canada	1	0	0	0	0	0	**1**
Statistics Canada	1	2	0	3	0	3	**9**
Transport Canada	1	2	1	1	0	1	**6**
Treasury Board of Canada Secretariat	0	0	0	4	0	0	**4**
Veterans Affairs Canada	1	0	0	2	0	2	**5**
Total	**61**	**126**	**13**	**72**	**8**	**33**	**313**

* This includes 31 access cases previously categorized as "well founded and resolved".

TREATMENT TIMES UNDER THE *PRIVACY ACT*

Early-resolution cases by complaint type

Complaint Type	Cases	Average Treatment Time (Months)
Use and Disclosure	33	3.1
Access	26	3.4
Collection	9	5.0
Time Limits	6	3.8
Correction – Notation	3	4.1
Fees	1	10.4
Total	**78**	**3.6**

Formal investigations by complaint type

Complaint Type	Cases	Average Treatment Time (Months)
Time Limits	227	5.9
Access	179	10.1
Use and Disclosure	46	9.9
Extension Notice	24	6.0
Retention and Disposal	8	12.6
Collection	5	12.4
Language	2	3.0
Correction – Notation	1	14.0
Total	**492**	**8.0**

All closed files by disposition

Complaint Type	Cases	Average Treatment Time (Months)
Well founded	250	6.8
Not well founded	149	8.6
Early Resolution	78	3.6
Discontinued	41	7.6
Well founded/resolved	31	13.4
Resolved	13	9.2
Settled	8	11.0
Total	**570**	**7.2**

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

Our emphasis on early-resolution strategies enabled us to reduce the average treatment times from 19.5 months in 2008-2009 to 12.9 months in 2009-2010 and 7.2 months in 2010-2011.