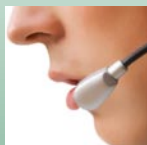


Privacy Commissioner
of Canada



Commissaire à la protection
de la vie privée du Canada

Privacy



Annual Report to Parliament 2006-2007

Report on the *Privacy Act*

Canada 

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

(613) 995-8210, 1-800-282-1376
Fax (613) 947-6850
TDD (613) 992-9190

© Minister of Public Works and Government Services Canada 2007

ISSN 1910-006X

This publication is also available on our Web site at www.privcom.gc.ca.

**Privacy Commissioner
of Canada**

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

**Commissaire à la protection
de la vie privée du Canada**

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél. : (613) 995-8210
Télééc. : (613) 947-6850
1-800-282-1376
www.privcom.gc.ca



October 2007

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

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Privacy Act* for the period from April 1, 2006 to March 31, 2007.

Sincerely,

Original signed by

Jennifer Stoddart
Privacy Commissioner of Canada

**Privacy Commissioner
of Canada**

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

**Commissaire à la protection
de la vie privée du Canada**

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél. : (613) 995-8210
Télec. : (613) 947-6850
1-800-282-1376
www.privcom.gc.ca



October 2007

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

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Privacy Act* for the period from April 1, 2006 to March 31, 2007.

Sincerely,

Original signed by

Jennifer Stoddart
Privacy Commissioner of Canada

Table of Contents

Message from the Commissioner	1
Key Accomplishments in 2006-2007	5
Creating a Modern Law for the 21 st Century	7
<i>Privacy Act</i> – A Chronology.....	13

Key Issues in 2006-2007

IDENTITY THEFT

Avoiding an Identity Crisis	15
How ID Thieves Obtain Information	16
Key Initiatives Needed to Combat Identity Theft	17
How the OPC Helps Fight Identity Theft	19

NATIONAL SECURITY

Is the Post 9-11 Tide Turning?	21
Backgrounder: The <i>Anti-terrorism Act</i>	23

NO-FLY LIST AND OTHER TRAVEL-RELATED SECURITY PROGRAMS

Are Travel-Related Security Programs Respecting Privacy Rights?	27
---	----

TRANSBORDER DATA FLOWS

Protecting Privacy in a World of Transborder Data Flows	33
---	----

PRIVACY IMPACT ASSESSMENT AUDIT

A Critical Privacy Tool Needs to Work Better	39
--	----

Responding to Complaints and Privacy Incidents	43
Complaints	44
Incidents under the <i>Privacy Act</i>	53
Public Interest Disclosures under the <i>Privacy Act</i>	54
What Happens When you File a Complaint with the OPC?	55

Branch Activities	57
Potential Privacy Risks: Monitoring Federal Government Programs	57
In the Courts	60
The Year Ahead	63
Appendix 1	65
Definitions of Complaint Types.....	65
Definitions of Findings and other Dispositions under the <i>Privacy Act</i>	66
Appendix 2	68
Investigation Process under the <i>Privacy Act</i>	68
Appendix 3	70
<i>Privacy Act</i> Complaints Statistics	70
▪ Complaints Received by Complaint Type.....	70
▪ Top 10 Institutions by Complaints Received	71
▪ Complaints Received by Institution.....	72
▪ Complaints Received by Province/Territory	74
▪ Findings by Complaint Type.....	75
o Complaints (All Types) Closed.....	75
o Access and Privacy Complaints Closed	75
o Time Limits Complaints Closed.....	76
▪ Time Limits Closed by Institution and Finding	77
▪ Access and Privacy Complaints Closed by Institution and Finding	79
▪ Complaint Investigations Treatment Times.....	81
o By Finding	81
o By Complaint Type	81
▪ Inquiries Statistics	82

Message from the Commissioner

A key role for Canada's privacy guardian is to push for changes that will help better protect the privacy rights of people in this country. In today's surveillance society, people expect strong privacy laws and want their federal government to take this responsibility extremely seriously. Once again, in 2006-2007, we identified many areas where the government needs to take action to meet those expectations.



At the top of our list of public sector concerns is reform of the *Privacy Act* itself.

The law, which governs how federal government institutions collect and handle personal information, marks its 25th anniversary this year. Unfortunately, this is not a time of celebration – even though the legislation was considered pioneering when it was passed. A law that is crucial to protecting Canadians' privacy rights has been allowed to slip further and further out of sync with the times.

Various privacy commissioners and advocates have been warning for years that **Privacy Act reform** is urgently needed. I will again repeat the message in this annual report: an overhaul of the *Privacy Act* is absolutely critical.

The *Privacy Act* was a socially progressive piece of legislation in its day. However, it has stood still while the world around it has changed profoundly. The law was designed for a time when public servants still had typewriters – not a digital age where reams of personal information can be sent spiralling around the planet at the touch of a button.

▼

In today's surveillance society, people expect strong privacy laws and want their federal government to take this responsibility extremely seriously.

We need an overarching framework on how the government collects, uses, discloses and protects personal information. Accountability and transparency must be its guiding principles and sound management its *modus operandi*.

Many amendments to the Act are necessary and we have outlined these in a detailed report tabled with the Standing Committee on Access to Information, Privacy and Ethics. Of greatest urgency are those legislative changes that are critically needed to respond to Canadians' heightened demands for a more accountable, open and transparent government. We have proposed that the *Privacy Act* be amended to:

- Create a legislative requirement for government departments to clearly define the purpose for collecting personal information and also demonstrate the need to do so by way of a “necessity test”, a step that would help ensure better checks and balances in our security-focused environment.
- Allow Canadians – or the Privacy Commissioner on their behalf – to go to Federal Court to seek a remedy for the government’s inappropriate collection, use or disclosure of their personal information.
- Enshrine the federal Privacy Impact Assessment Policy into law in order to ensure departments fully respect its provisions – something an OPC audit finds is not always happening at the moment.
- Provide the OPC with a clear public education mandate and specify flexible reporting on the personal information management practices of government institutions. We know that Canadians want and expect greater accountability, openness and transparency of their governments all year-round, not just in an annual report.

Much of our attention during the past fiscal year focused on a few key issues: identity theft, national security, travel-related security programs such as the no-fly list, transborder data flows and safeguarding personal information.



The *Privacy Act* was a socially progressive piece of legislation in its day. However, it has stood still while the world around it has changed profoundly.

Identity theft has a clear privacy dimension. A central notion of privacy is that people should be able to control how their personal information is used and disclosed. Identity theft victims have lost control over their personal information – and the impact of this on their lives and livelihood can be devastating. This costly form of fraud is an enormous violation of privacy. We believe the federal government needs to take a leadership role in developing a comprehensive strategy against identity theft.

For the past few years, I have also been very concerned about the incremental erosion of privacy rights in the post 9-11 **national security** environment. There have been signs that some worrying security measures which were adopted very soon after 9-11 are now being reconsidered and we may be turning a corner.

However, we question the extensive use of **travel-related security programs** such as the no-fly list. We remain skeptical about whether security benefits will outweigh privacy risks. We intend to begin an audit of this program within a year of its launch date.

We also remain worried about the increased potential for data breaches stemming from the ever-bigger streams of **personal information crossing borders** without the appropriate and necessary protections in place. It is becoming abundantly clear that international frameworks and global enforcement mechanisms are needed to address transborder data flows.

Our annual report provides us with an opportunity to talk publicly about the **investigations** we conduct into complaints involving federal institutions. Human error was a factor in many of the breaches we investigated over the year, reinforcing the need for training and detailed procedures. As well, the year's investigative findings raised issues about workplace surveillance.

Also highlighted in this report are the findings of our **audit** into how departments are applying the government's policy on Privacy Impact Assessments (PIAs). These assessments are a key tool to identify and then eliminate or reduce the potential privacy risks of new or redesigned federal government programs and services. We were disappointed to find institutions are not fully meeting their commitments under the policy. Clearly, it is time for Treasury Board Secretariat to review this policy. The OPC wants to work with Treasury Board Secretariat and departments and agencies to ensure PIAs are being used to their full potential.

We ended the year preparing for the **29th International Conference of Data Protection and Privacy Commissioners**. We are hosting the world's leading privacy experts at this event in Montreal from September 25 to 28, 2007. The conference is our chance to assess the shifting privacy landscape and to map out ways to address emerging issues such as data mining, authentication and identity management.

The conference also marks a golden opportunity for the federal government to commit to the world that Canada plans to live up to its international reputation as a privacy leader and will move swiftly to overhaul its public sector privacy law. We need to make the *Privacy Act* something that Canada can once again be proud of — a strong legislative tool that Canadians can look up to as a central pillar of our democratic system.

Jennifer Stoddart
Privacy Commissioner of Canada

Key Accomplishments in 2006-2007

Under the *Privacy Act*, the OPC serves three key client groups: Parliament, federal government departments and agencies, and individual Canadians. Some of our key accomplishments in 2006-2007 included:

PROACTIVELY SUPPORTING PARLIAMENT

- Appeared 11 times before parliamentary committees on such issues as the *Federal Accountability Act*, *Elections Act*, *Anti-terrorism Act* and *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*.
- Recommended measures to mitigate privacy risks in travel-related security programs and pilot projects, including the Passenger Protect Program or no-fly list.
- Tabled a reform proposal outlining comprehensive and urgently needed changes to the *Privacy Act*.

SERVING CANADIANS

- Responded to 3,400 *Privacy Act*-related inquiries and 3,557 general inquiries.
- Investigated hundreds of privacy complaints in the public and private sectors.

SUPPORTING FEDERAL GOVERNMENT INSTITUTIONS

- Reviewed government policies and initiatives as they relate to privacy legislation and provided input to federal institutions as well as Parliamentarians.
- Undertook a government-wide audit of the federal government's Privacy Impact Assessment Policy and worked with Treasury Board Secretariat to improve how these assessments are conducted.
- Completed 22 Privacy Impact Assessments and launched six new audit projects.



OTHER HIGHLIGHTS INCLUDED:

- Prepared for the 29th International Conference of Data Protection and Privacy Commissioners.
- Funded 11 research projects on emerging privacy issues.
- Worked with the Organisation for Economic Co-operation and Development (OECD) and the Asia-Pacific Economic Cooperation (APEC) to enhance the protection of personal information when it is shared across borders.
- Recognizing that the *Federal Accountability Act* brings the OPC under the list of federal organizations covered by the *Access to Information Act* and the *Privacy Act* for the first time, we created an Access to Information and Privacy section within our Office.

Creating a Modern Law for the 21st Century

T*he Privacy Act has remained virtually unchanged since its passage 25 years ago and no longer meets the needs of our dramatically transformed privacy landscape*

Parliament passed Canada's public sector privacy law back in 1982 – the same year the Commodore 64 computer hit the market. At the time, both were considered pioneering.

The Commodore 64, which looked like an over-sized keyboard and had 64 KB of RAM and a 1-Mhz chip, was the first affordable computer designed for home use. This Canadian invention has often been compared to the Ford Model T.

The passage of the *Privacy Act* marked the first time in Canada that privacy was dealt with under separate legislation. Until then, more limited privacy protections were provided as an appendage to the *Canadian Human Rights Act*. Privacy rights had taken an important step forward.

But that was a quarter century ago. Back in 1982, *Time* magazine broke with its tradition of naming a “Man of the Year,” instead naming the computer as its “Machine of the Year.” *Time's* article, which described how the computer had become a tool for the masses, was written on a typewriter.

Times have changed – and so too has the privacy environment. Technology has created new and complex privacy issues.

In 1982, the Internet, global positioning systems, Radio Frequency Identification Devices (RFIDs), cross-border outsourcing and data mining were novel ideas. Today, these technologies are commonplace and are the key issues keeping privacy advocates up at night. Another generation of technologies that carry privacy risks – brain scans and smart dust, for example – is just around the corner.

The privacy challenges for government today are compounded by increased globalization and heightened concerns over national security in the wake of the 9-11 terrorist attacks.

The *Privacy Act* was not designed to address the era we now live in and it is not up to the job of protecting Canadians in this changed world. In fact, it has been desperately out of date for many years.

Proposals for reforming the Act date back to 1987. Unfortunately, successive federal governments have not heeded the numerous – and increasingly urgent – calls for improvements.

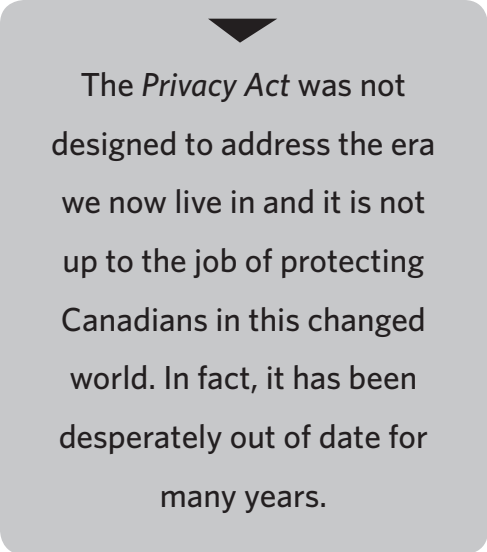
Canada's private-sector privacy law, the *Personal Information Protection and Electronic Documents Act (PIPEDA)*, came into effect in 2001 – making the shortcomings of its public sector sister legislation all the more evident. It is unfortunate that Canadians have stronger privacy safeguards for personal information in the hands of the private sector than they do for that held by government.

Canadians clearly want strong and modern privacy laws. A 2007 Ekos poll commissioned by the OPC found:

- Four in five people place a high level of importance on strong privacy laws.
- Canadians overwhelmingly feel their personal information is less well protected today than it was 10 years ago.
- Three-quarters of Canadians believe there is a strong need to modernize the *Privacy Act* to keep pace with threats posed by new technologies.
- Only 17 per cent of Canadians believe government and businesses take the protection of personal information seriously.

The key message from Canadians is that they expect their government to provide a better level of privacy protection.

In June 2006, the OPC presented to the Standing Committee on Access to Information, Privacy and Ethics a comprehensive plan for reforming the *Privacy Act* so that it will provide the strong safeguards Canadians are seeking. The report, called *Government Accountability for Personal Information; Reforming the Privacy Act*, is posted on the OPC Web site. The committee conducted a comprehensive review of *PIPEDA*, and we hope it will do the same with the *Privacy Act* in the fall of 2007.



The *Privacy Act* was not designed to address the era we now live in and it is not up to the job of protecting Canadians in this changed world. In fact, it has been desperately out of date for many years.

We can, however, report one small bright spot for the long-neglected *Privacy Act*. At the end of 2006, the *Federal Accountability Act*, which expands coverage of the *Privacy Act*, received Royal Assent. While this was a welcome incremental step which expanded the number of government institutions covered by the *Privacy Act*, it did nothing for raising the level of privacy standards to where they ought to be.

Many changes are needed to reform Canada's first generation *Privacy Act*. Some of the key issues to be addressed include: the need for a broader range of fair information practices; greater openness and transparency; an expanded right of access to personal information; limits and conditions for transborder data flows; and greater recourse to the Federal Court.

FAIR INFORMATION PRINCIPLES

A good privacy law needs a robust privacy management regime governing the collection, use and disclosure of personal information. The *Privacy Act's* fair information principles are clearly deficient – with non-existent or overly lenient controls on the federal government's information management practices.


We should take steps to ensure the federal government is collecting as little personal information as possible by introducing a “necessity test” – a legal requirement for departments to demonstrate the necessity of collecting the information. Finding the right balance between security and privacy is particularly important in a post 9-11 world of increased surveillance.

The *Privacy Act* contains no ground rules for data matching, including data mining and data aggregation. We have called for a reformed *Privacy Act* to define the principles governing data matching and the responsibilities of the parties involved. There should be a legislated requirement for federal departments to seek the Privacy Commissioner's review and approval before starting any data matching initiatives – which is not currently the case. The Commissioner should have the power to stop data matching if it raises significant privacy concerns. Other jurisdictions, including Australia, New Zealand and Hong Kong, have addressed concerns about data matching in legislation, whereas our *Privacy Act* remains silent on the issue.

The *Privacy Act* also fails to provide specific legal rules for protecting the personal information of citizens in a government online context. Canada should consider legislating in this area, as the United States did with the *E-Government Act of 2002*.

GREATER OPENNESS AND TRANSPARENCY

Transparency and openness should be at the heart of fair information practices. Section 72 of the *Privacy Act* requires heads of government institutions to table an annual report to Parliament on the administration of the Act within their institution. This was intended to ensure Parliament and the public would have an opportunity to review how government departments are handling privacy issues, and to encourage departments to identify and address systemic or recurring problems. However, since the Act does not specify what information each annual report must contain, these have become a mere accumulation of statistics on how many *Privacy Act* requests have been received and handled, with no details about specific or systemic privacy issues or concerns. This does not illuminate privacy issues or solutions, nor does it do anything to ensure accountability for the actions and decisions of institutions on privacy matters.



We are also concerned the Act does not ensure enough transparency, accountability, and oversight of the personal information management practices of national security agencies. Stricter reporting requirements to Parliament would help make these agencies more accountable to Canadians.

We are also concerned the Act does not ensure enough transparency, accountability and oversight of the personal information management practices of national security agencies. Stricter reporting requirements to Parliament would help make these agencies more accountable to Canadians.

One way to increase transparency across the government is to enshrine the federal Privacy Impact Assessment (PIA) Policy into law – making it far more likely that departments will take PIA requirements seriously.

We would also like to see Canadians better informed about the privacy issues that come to light as a result of the OPC's investigations. Up until now, we have reported on our investigative findings only in annual reports. In the future, we plan to issue special reports when there are exceptional circumstances dictated by urgent issues that have to be addressed by Parliamentarians. We believe Canadians have the right to be informed of privacy issues related to the operations of their federal government in a timely manner.

The *Federal Accountability Act* makes Officers of Parliament, including the Office of the Privacy Commissioner, subject to both the *Privacy Act* and the *Access to Information Act*. We applaud this change, which brings more transparency and accountability to how government operates. We believe our organization should be subject to the *Privacy Act* and the *Access to Information Act* and that we should be held to the same standards expected of the organizations we investigate. We must now set our sights on raising those standards expected of all government institutions.

ACCESS TO PERSONAL INFORMATION

The *Privacy Act* currently provides too many avenues and situations where government institutions can deny people access to their personal information. The Act requires that individuals be present in Canada to have access rights. This means airline passengers, immigration applicants, foreign student applicants and countless others have no legal right to examine or correct erroneous information in Canadian government files, or to know how information about them is used or disclosed. Despite government commitments to interpret the Act more broadly, the *Privacy Act* falls behind current international trends. In the European Union, for example, access rights are granted to every data subject, regardless of citizenship or place of residence.

Fortunately, government institutions such as the Canada Border Services Agency, for example, have concluded an administrative agreement so that people who are residents in the European Union can apply for access to their personal information collected in the course of Advance Passenger Information and Passenger Name Record data compilations of airline travelers.


The right of access to personal information under the *Privacy Act* should also be strengthened by including sanctions – such as those provided in the *Access to Information Act* – for destroying, altering, falsifying or concealing a person's record.

CROSSING BORDERS

The *Privacy Act* is also in critical need of updating to deal with transborder data flows. As it stands now, the Act does not address this issue at all.

The standard for disclosure of personal information set by the *Privacy Act* is extremely low. Many data protection statutes, notably the European Union's legislation, restrict the disclosure of government-held information to only those foreign states which provide adequate levels of privacy protection.

The *Privacy Act* should, at a minimum, make it clear that when government work is outsourced, the government institution remains accountable for personal information which remains under its control. (Further elaboration on the need to reform the *Privacy Act* in relation to transborder data flows can be found on page 36.)



The *Privacy Act* is outdated.
Canadians want - and
deserve - better privacy
protection.

STRONGER ROLE FOR THE FEDERAL COURT

The *Privacy Act* does not give complainants or the Privacy Commissioner the right to pursue in Federal Court any complaints dealing with the inappropriate collection, use or disclosure of personal information by government institutions. At the moment, denial of access to personal information is the only ground to bring a *Privacy Act* breach to Federal Court.

Given the potential that the inappropriate collection, use or disclosure of personal information has to cause humiliation, hurt, embarrassment, economic loss or other harms to people, the legislation should allow for remedies for any damages caused by government actions. Individuals – or the Commissioner acting on their behalf – should be able to ask the Federal Court to review the government’s inappropriate collection, use and disclosure of personal information following the completion of an investigation. The Court should be empowered to assess damages.

These types of powers are provided under *PIPEDA*. The threat that a case will be brought before the Court is a strong incentive for businesses to comply with our recommendations and should serve as an equally effective incentive in the public sector.

CONCLUSION

These are only some of the reforms required to close the many gaps in the *Privacy Act* and transform it into a law that provides effective privacy for Canadians.

The Commodore 64 – as innovative and popular as it was back in the ‘80s – isn’t up to our needs in 2007. The *Privacy Act* is just as outdated. Canadians want – and deserve – better privacy protection.

Privacy Act – A Chronology	
1978 -1983	Canada's privacy legislation included in the <i>Canadian Human Rights Act</i> .
1982	<i>Privacy Act</i> passed by Parliament.
1983	<i>Privacy Act</i> came into force July 1; Office of the Privacy Commissioner of Canada (OPC) opened for business.
1987	Parliamentary committee conducted a mandatory review of the Act and issued a comprehensive report calling for significant change. More than 100 recommendations were unanimously supported. Government committed to amendments; no action follows.
1997	Another parliamentary committee recommended a major overhaul of Canada's privacy regime, including replacing the <i>Privacy Act</i> with data protection legislation.
2000	In his last report, for 1999-2000, then-Privacy Commissioner Bruce Phillips called a major review of the Act "urgent and unavoidable."
2000	OPC submitted detailed review of the Act to the Department of Justice Canada.
2005	OPC told Parliament that "characterizing the current Act as dated in coping with today's realities is an understatement — the Act is tantamount to a cart horse struggling to keep up with technologies approaching warp speed."
2006	Commissioner Jennifer Stoddart called for a new <i>Privacy Act</i> in her annual report, noting: "Canadians deserve real redress when things go wrong."
2006	Commissioner Jennifer Stoddart tabled a proposal on reforming the Act to the Standing Committee on Access to Information, Privacy and Ethics.

Key Issue: Identity Theft

AVOIDING AN IDENTITY CRISIS

Canada urgently needs to develop a comprehensive approach to fighting the proliferation of identity theft

Where do you keep your Social Insurance Number (SIN) card?

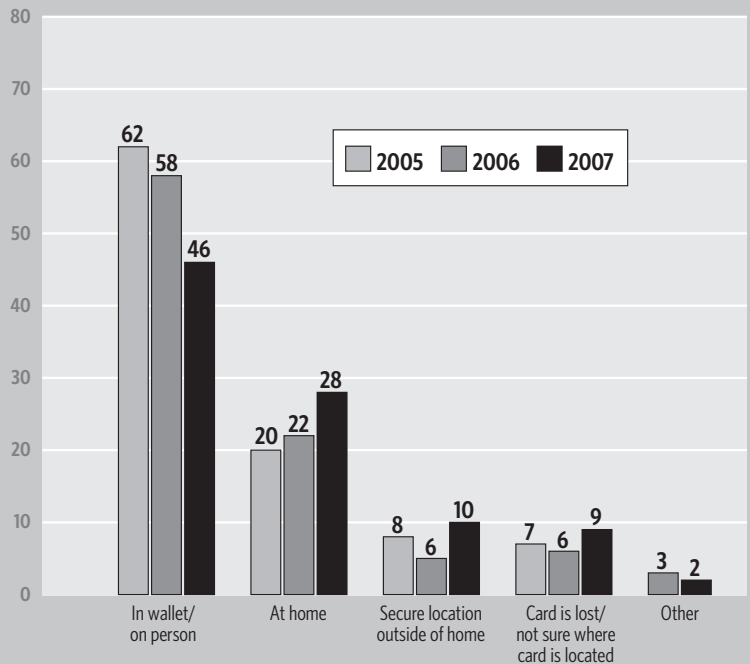
Almost half of Canadians continue to carry a SIN card in their wallet – even though this number is a key piece of personal information used by identity thieves. Many people still aren't doing the basics to protect themselves against identity theft in spite of growing concerns about this type of fraud.

More concerted public education is just one of the many measures needed to tackle identity theft. It is clear that if we want to make real headway, Canada needs a comprehensive identity theft strategy – one that involves a lot of different players.

The OPC has urged the federal government to take the lead role in creating a broad-based plan to combat identity theft – a type of fraud that involves a crook using your personal information to pose as you and

Where Canadians Keep their SIN Card

Canadians don't need to carry their SIN card, but a large number do (albeit on a downward trend).



Source: Ekos poll commissioned by the OPC, March 2007

apply for credit cards and loans, open bank accounts or get new documents such as driver’s licences and SIN cards.

Time to Act

Identity theft means different things to different people. People use the

term identity theft to cover everything from straightforward fraud cases such as a forged cheque or stolen credit cards to very sophisticated cases where an impostor creates a “synthetic” identity using a combination of actual and fabricated personal information. To the majority of Canadians, identity theft means the use or disclosure of another person’s personal identity without their knowledge or consent.

PhoneBusters, an anti-fraud call centre run by the Ontario Provincial Police and the RCMP, provides us with the best numbers available in Canada, but acknowledges it is capturing only a tiny piece of the whole picture. In 2006, PhoneBusters heard from some 7,800 people describing themselves as identity theft victims. These people reported losses to themselves and to businesses totalling more than \$16 million. PhoneBusters estimates these numbers represent a small percentage – perhaps five per cent – of actual figures.

It is clear that identity theft – which some law enforcers have dubbed the “crime of the 21st century” – has grown so rapidly and has such a significant financial and emotional impact, that we must come up with more effective ways to stop it.

Strong Central Focus

We may want to look south for one route towards developing an all-inclusive identity theft plan.

In May 2006, President Bush created an Identity Theft Task Force to marshal the resources of the US government to fight identity theft. The task force is co-chaired by US Attorney General Alberto R. Gonzales and Deborah Platt Majoras, chair of the Federal Trade Commission (FTC) and includes

How ID Thieves Obtain Information

Physical Theft	Technology	Social Engineering
✓ Theft of ID documents	✓ Hacking into databases	✓ Pretexting
✓ Insider theft	✓ Spyware/malware	✓ Bogus contests

▼

Many different government departments and agencies are interested in identity theft, but no one has overall responsibility to do anything about it.

other top-level US officials. It took less than a year for the task force to issue a report containing a comprehensive list of recommendations.

In Canada, many different government departments and agencies are interested in identity theft, but no one has overall responsibility to do anything about it. We urge the federal government to bring together a wide range of players to identify the best range of solutions.

Some of the areas we see as key to fighting identity theft include: effective privacy legislation; stronger sanctions against pretexting and online threats; and public education.

Privacy Laws—Private Sector

Canada's private-sector privacy law, *PIPEDA*, can significantly reduce the risk of identity theft – if the companies covered by the Act respect its provisions. The *Privacy Act*, however, fails Canadians in this regard.

PIPEDA is helpful in that it places limits on the collection of personal information by the private sector. It requires organizations to identify the purpose for which their personal information is being collected and to collect only the minimal amount of personal information necessary to fulfill that purpose. This way, by collecting minimal amounts of personal information, clients are less exposed to risks if a database is compromised.

Under *PIPEDA*, organizations engaged in commercial activities are required to take appropriate steps to protect their customers' personal information. The more sensitive the information is, the stronger the security safeguards should be. This is another way to stymie would-be identity thieves.

Privacy Act and Identity Theft

At the moment, *PIPEDA* provides for a far stronger level of protection of personal information held by the private sector than the *Privacy Act* does for data held by government institutions.

Key Initiatives Needed to Combat Identity Theft

- A comprehensive federal identity theft strategy.
- *Privacy Act* reforms requiring stronger protection of personal information held by government institutions.
- New civil sanctions and *Criminal Code* amendments to more effectively punish those who engage in identity theft.
- Legislative reforms to address "pretexting."
- Federal government action to stop spam.
- More concerted public education.

This gap must be closed. Government institutions store a lot of personal information and, thus, the potential for identity theft is great. In a March 2007 report, Symantec, a US-based company, found that the government sector in 180 countries was responsible for 25 per cent of the data breaches that could lead to identity theft.

We have recommended the *Privacy Act* be amended to require government institutions to collect only the minimal amount of personal information which is needed. Institutions should also be required to appropriately safeguard the personal information they collect, use or disclose.

On the government side, Treasury Board's Guidelines on Privacy Breaches are a good step, but we need more emphasis on protection of information within government.

Privacy legislation is important, but it is only one part of the solution because it applies to government bodies and commercial organizations. Stronger legal sanctions may be a more appropriate way to deal with those individuals who engage in identity theft.

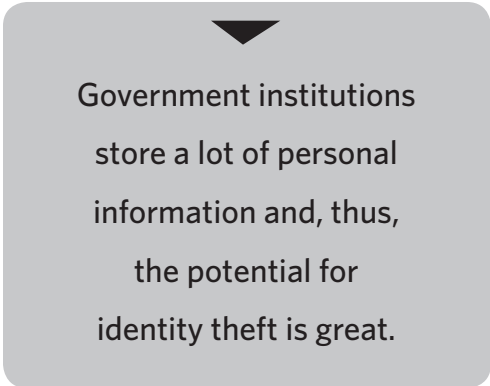
Stronger Sanctions

Identity theft is clearly an important law and order issue. Criminals are increasingly relying on technology and the weaknesses of existing personal information management systems to extract huge sums of money.

Justice Canada launched consultations on identity theft in 2004. We have strongly urged the Minister of Justice to move forward with *Criminal Code* amendments that would more effectively punish those who engage in identity theft. We also believe it is important to look at new civil sanctions.

Pretexting

Legislative reforms are also needed to address “pretexting” — a form of social engineering in which an individual, armed with some information about a person, is able to obtain additional information about that person by tricking an organization. For example, a fraudster calls an organization pretending to be the person whose information is being



Government institutions
store a lot of personal
information and, thus,
the potential for
identity theft is great.

sought, a relative of that person or someone authorized to obtain the information.

In cases we investigated under *PIPEDA*, we found that a US-based information broker had used pretexting to gain unauthorized access to personal phone records from Canadian telecommunications companies. See the OPC's Web site at http://www.privcom.gc.ca/cf-dc/2007/372_20070709_e.asp.

In the much-publicized ChoicePoint case, criminals posing as legitimate businesses were able to trick the US consumer data broker into providing personal information on more than 160,000 consumers. It is alleged that hundreds of people became victims of identity theft due to security lapses.

Pretexting as such is not an offence in Canada – it only becomes an offence if it can be established that the person did so intentionally for fraudulent purposes. We believe the Minister of Justice and his cabinet colleagues must explore means to address the wrongful possession and collection of personal information.

One way in which organizations can protect themselves from pretexting is by using appropriate authentication procedures to ensure people requesting information are who they claim to be. In October 2006, we published a how-to guide for organizations on identification and authentication. The document is on the OPC's Web site at http://www.privcom.gc.ca/information/guide/auth_061013_e.asp.



How the OPC Helps Fight Identity Theft

- *Privacy Act* investigations and Privacy Impact Assessments help federal government departments better protect personal information.
- Investigations and audits under *PIPEDA* help private sector organizations better protect personal information.
- Informing Parliamentarians about identity theft issues and offering recommendations to fight this type of fraud.
- Publishing information such as our *Guidelines for Identification and Authentication* to help organizations safeguard personal information.
- Issuing public education documents aimed at helping individuals protect themselves from identity thieves.
- Speaking regularly to the media about identity theft in an effort to raise public awareness.
- Funding research into identity theft issues.

Online Threats

Another way to stop identity thieves from collecting personal information is to take measures to stop spam from popping up in people's computer mailboxes. Spam is often used by ID thieves to launch "phishing" attacks, where e-mails that look like they come from legitimate organizations are used to trick people into revealing personal information.

The international non-profit group Spamhaus lists Canada as No. 6 in the top ten worst countries for originating spam. Much more than a mere nuisance, spam has financial consequences for our economy, affects productivity and undermines confidence in electronic commerce.

To date, the federal government has not implemented any of the recommendations of its Task Force on Spam. To our dismay, Canada is now the only G-8 country without anti-spam legislation. The Commissioner has written the Minister of Industry urging action in this regard. The letter can be viewed on the OPC's Web site at http://www.privcom.gc.ca/parl/2007/sub_070222_07_e.asp.

Public Education

More concerted public education campaigns should remind people about the importance of protecting wallets and credit card numbers, taking online security seriously and shredding documents that contain personal information.

We have undertaken a number of public education initiatives in this area – producing documents on preventing identity theft; funding research on identity theft and raising identity theft issues in presentations across the country.

Conclusion

Identity theft is a complex problem. Organizations and individuals can only do so much. The federal government has an important leadership role to play in developing a much-needed strategy; co-coordinating the efforts of different stakeholders; and creating a legal framework offering police the tools they need to fight identity theft.

Key Issue: National Security

IS THE POST 9-11 TIDE TURNING?

After several years of putting privacy and other rights on the back burner in favour of national security initiatives, there are signs some are rethinking this trade-off

Canada's national security landscape has changed dramatically since the September 11 terrorist attacks. Stronger state surveillance powers with little or no oversight, the expansion of integrated data banks, and information sharing across agencies and jurisdictions have all taken their toll on privacy rights.

Privacy and civil rights advocates have long warned that privacy and other individual rights were being given short shrift in governments' haste to improve national security.


Now – some five years after the 9-11 attacks – we are beginning to see new voices raising questions about the balance between rights and security. We are also seeing some promising signs that some of these security measures are being curtailed.

A Changed World

The passage of the *Anti-terrorism Act* in November 2001 marked the beginning of a new Canadian national security environment characterized by enhanced surveillance powers for law enforcement and national security agencies, and fundamental changes to the machinery of government. This legislation also led to the increased flow of personal information across borders without adequate privacy provisions.

All of these changes were put into place with too little scrutiny or debate.

The OPC has raised many red flags over the last few years.



▼
Privacy and other individual rights were being given short shrift in governments' haste to improve national security.

On several occasions, we pointed to how broader state surveillance powers were harmful to privacy rights. We questioned the blurring of the distinction between national security and law enforcement intelligence-gathering activities in many post-September 11 initiatives. We also argued that standards governing the collection of information should be more stringent for anti-terrorism activities than for general law enforcement.

It was troubling to see that, as the role and powers of law enforcement and national security agencies were being broadened, constraints on these surveillance powers were weakened. Along the way, government accountability and transparency were significantly eroded.

We have repeatedly questioned the need for strong surveillance powers, their effectiveness and their proportionality. We have also called for greater oversight over the day-to-day activities of law enforcement and national security agencies.

Promising Signs

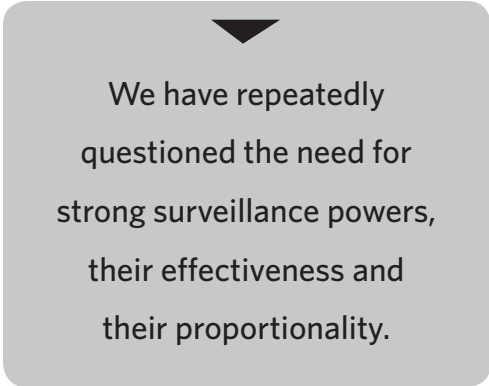
It was encouraging to see in 2006-2007 that calls for a balanced approach were beginning to be heard. In some cases, we have seen the proportionality and the fairness of some anti-terrorism measures finally being re-examined.

This sober reconsideration has taken many forms. Parliamentary reviews, court challenges and a high-profile inquiry have shed new light on the scope of the *Anti-terrorism Act*.

The Arar Inquiry

For example, the enhanced powers of law enforcement and national security agencies in the post 9-11 era were put under the microscope by the federal inquiry into the tragic case of Mr. Maher Arar, a Syrian-born Canadian deported to Syria by US officials who suspected he was a terrorist. Calls for greater oversight were forcefully presented by the head of that Commission of Inquiry, Mr. Justice Dennis O'Connor.

Mr. Justice O'Connor documented in detail the RCMP's disclosure of misleading and inaccurate information about Mr. Arar to US authorities. He found it was very likely that on that basis, Mr. Arar was sent to Syria where he was jailed and



We have repeatedly questioned the need for strong surveillance powers, their effectiveness and their proportionality.

tortured. Inquiry investigators thoroughly searched for evidence connecting Mr. Arar to terrorist activities and found none.

The O'Connor report called for:

- The creation of an Independent Complaints and National Security Review Agency to review the activities of the RCMP; and
- The expansion of the Security Intelligence Review Committee's mandate to review the national security activities of not only the Canadian Security Intelligence Service (CSIS), but also the activities of Citizenship and Immigration Canada, Transport Canada, FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) and Foreign Affairs and International Trade Canada.

We expect the government to carefully consider implementing these recommendations.

The Anti-terrorism Act

The Anti-terrorism Act came under intense scrutiny in 2006, five years after it was rushed through Parliament in the wake of 9-11. Two parliamentary committees conducted mandated reviews of the legislation.

The OPC made representations to both committees, arguing the Act went too far, that it largely ignored privacy rights, and that it should be repealed “in the absence of serious evidence in support of its continued existence.”

Backgrounder - The Anti-terrorism Act

The *Anti-terrorism Act* brought sweeping changes to Canada's national security environment. It:

- Amended the *Criminal Code* making it easier for law enforcement and national security agencies to obtain electronic surveillance warrants;
- Expanded the scope of the *Proceeds of Crime Act and Terrorist Financing Act (Money Laundering)* to deal with terrorist financing;
- Amended the *National Defence Act* to provide the Communications Security Establishment with the power to intercept Canadian communications rather than only foreign communications;
- Amended the *Canada Evidence Act* to allow the Attorney General to prohibit the release of information in legal proceedings on the grounds it might harm national security or international relations; and
- Amended the *Privacy Act* and *PIPEDA*, allowing the Attorney General to issue certificates prohibiting the disclosure of information to protect national security and international relations.

The OPC welcomed a special Senate committee's 40 recommendations, which would go a long way towards fixing what we consider a fundamental imbalance in the *Anti-terrorism Act*. In its February 2007 report, *Fundamental Justice in Extraordinary Times*, the committee recommended:

- The appointment of special advocates to represent the interests of individuals who have been denied full access to the evidence against them in terrorism-related charges; and
- Amendments to the *Canada Evidence Act* to build in additional privacy safeguards when certificates are issued prohibiting the disclosure of information to protect national defence, national security, or Canada's relations with foreign entities.

The second review by a subcommittee of the House of Commons Standing Committee on Public Safety and National Security resulted in a March 2007 report entitled *Rights, Limits, Security: a Comprehensive Review of the Anti-terrorism Act and Related Issues*. This report was much more supportive of the Act. However, it recommended the Commissioner of the Communications Security Establishment (CSE) be required to review CSE's interception activities to ensure they comply with the *Privacy Act* and the *Canadian Charter of Rights and Freedoms*.

Curtailing Police Powers

Another encouraging sign was the curtailment of police powers related to anti-terrorism activities. Preventive arrests and investigative hearing provisions contained in the *Anti-terrorism Act* were repealed. Those powers had allowed police officers to arrest and detain a suspected terrorist without charge for up to 72 hours. They also compelled a person believed to have information about terrorist activities to testify before a judge, thereby removing an individual's right to remain silent.

The Act provided that these two provisions would expire after five years unless they were renewed. On February 27, 2007, the House of Commons voted against extending the provisions. Those two provisions ceased to exist on March 1, 2007.

Proceeds of Crime and Terrorist Financing Act (Money Laundering)

The *Proceeds of Crime and Terrorist Financing Act* was also subject to a mandated parliamentary review. In this case, amendments significantly expanded the scope of the Act. More organizations will now be collecting more information about more individuals with respect to a broader range of transactions.

On a more positive note, a new amendment requires the OPC to review the measures FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) takes to protect personal information every two years. We will report our findings to Parliament. Although we already had the authority to review FINTRAC's operations under the *Privacy Act*, we welcome the express recognition that Canada's anti-money laundering and anti-terrorist financing regime requires special attention.

Court Challenges

Another welcome development was a Supreme Court of Canada ruling that the security certificate process under the *Immigration and Refugee Protection Act* was unconstitutional. In the groundbreaking *Charakaoui v. Canada* case, the Supreme Court ruled that the process, which predates the 2001 terrorist attacks, was inconsistent with the *Canadian Charter of Rights and Freedoms*.

The case involved Moroccan-born Mr. Adil Charakaoui, who was living in Canada when he was detained under a security certificate on allegations he constituted a threat to Canada's national security. He has since been freed under strict conditions.

The security certificate process allows the Ministers of Citizenship and Immigration and Public Safety and Emergency Preparedness to sign a certificate stating that, in the interest of national security, a permanent resident or a foreign national is inadmissible to Canada. This process leads to detention and removal from Canada. The Court's decision is important in terms of fair information practices because it sets limits on the ability of the State to deny individuals access to information that is being used against them.

The Court found this process violates an individual's right to a fair hearing because the named person and his counsel are excluded from the proceedings and thus, cannot challenge the evidence introduced.

Concerns Remain

While many voices are calling for change, we were disappointed to see the introduction of new federal measures – in particular the expansion of anti-terrorist financing regimes and the no-fly list – that threaten the privacy rights of Canadians.

Is the tide beginning to turn towards a better balance between privacy rights and national security concerns? Only time will tell.

The OPC will continue to challenge the expanded use of state surveillance powers at the expense of privacy rights. The post 9-11 legacy – a culture of secrecy and focus on security at all costs – will be difficult to undo.



The post 9-11 legacy
– a culture of secrecy and
focus on security at all
costs – will be difficult
to undo.

Key Issue: No-Fly List and other Travel-Related Security Programs

ARE TRAVEL-RELATED SECURITY PROGRAMS RESPECTING PRIVACY RIGHTS?


The OPC is concerned about the privacy risks of such programs and believes they warrant close parliamentary scrutiny

The proliferation of travel-related security programs has raised concerns about the delicate balance between privacy rights and national security. Are there adequate privacy protections for the traveling public? How will these programs be implemented? As part of our audit planning, the OPC surveyed the federal government's extensive collection of travel-related security programs and pilot projects.

Privacy Risks

We researched a host of these programs – the best-known of which is probably the new no-fly list – in order to better understand their purpose and scope. As we pulled together information for audit planning purposes, we found there are many intertwined travel-related security programs and systems. These are inherently privacy intrusive in that they all collect, store, sort, and use personal information.

The OPC is concerned about the privacy risks of such programs and believes they warrant close parliamentary scrutiny. In particular, one of the programs that warrants a closer look is Transport Canada's Passenger Protect Program or no-fly list. In this program, airline passengers may be forbidden to travel if their name appears on a government no-fly list. Given the importance and sensitivity of the no-fly list, we plan to begin an audit of this program within a year of its launch date.



There are many intertwined travel-related security programs and systems. These are inherently privacy intrusive.

A Sample of Key Travel-Related Security Programs

Canada Border Services Agency (CBSA)	Primary Automated Lookout System	Custom inspectors and intelligence officers create, access, maintain and disseminate lookouts – flagging travelers or vehicles based on risk indicators or intelligence.
	Advance Passenger Information/Passenger Name Record	Identifies people who may pose a security risk before they travel by air. Airlines provide passenger information which is analyzed to identify people potentially linked to terrorism or serious crimes.
	High-Risk Traveler Identification Initiative	Facilitates sharing of Advance Passenger Information data from CBSA's Passenger Information System and the US Automated Targeting System-Passenger system. Traveler information is used for risk scoring.
	CANPASS - Air	Facilitates entry into Canada for low-risk air travelers. Pre-approved travelers clear customs by looking into a camera that recognizes the iris as proof of identity.
	NEXUS	A partnership program between the CBSA and US Customs and Border Protection. Members can clear the border faster when traveling to the US and Canada.
Canadian Air Transport Security Authority	Pre-Board Screening	Screening passengers and carry-on baggage for prohibited items and dangerous goods. Can involve search and seizure of possessions and a body pat-down.
	Boarding Pass Security Scan	Pilot project aimed at enhancing security breach response past airport security checkpoints by scanning a boarding pass.

Passport Canada	E- Passport	Under development; aimed at reducing passport tampering and identity theft. Involves contactless chip technology and possibly a biometric identifier.
	Facial Recognition Pilot Project	Investigates the potential of facial recognition software to prevent passport fraud.
RCMP	Integrated Border Enforcement Teams	Aims to enhance national security by identifying and investigating people and organizations who pose a threat. Individuals can be arrested and goods seized. This is a Canada-US law enforcement initiative.
Transport Canada	Passenger Protect Program (no-fly list)	Designed to prevent individuals who pose an immediate threat to aviation security from boarding an aircraft in Canada or destined for Canada.
Canadian Security Intelligence Service (CSIS)	Front-End Screening and Port of Entry Interdiction Program	Intended to identify security risks stemming from the refugee claimant stream. CSIS advises the Minister of Citizenship and Immigration on security inadmissibility criteria and provides security assessments. CSIS also screens refugee claimant information.
Citizenship and Immigration Canada	Biometrics Field Trial	Visa offices abroad and in Canada use fingerprint and facial recognition technologies to process temporary resident visa applications and refugee claimants. Scanned information is transmitted to a database.

Canada's No-Fly List

The Passenger Protect Program involves the secretive use of personal information in a way that will profoundly impact privacy and other related human rights such as freedom of expression and the right to mobility.

Under the program, Transport Canada, working with information provided by the RCMP and the Canadian Security Intelligence Service, has developed a list of people considered to be an immediate threat to aviation security. Air carriers check traveler's names against the list and report any matches to Transport Canada, which may instruct the airline to bar passengers from boarding flights.

The OPC has worked with Transport Canada to review its Privacy Impact Assessment of the program. We made many proposals to help mitigate privacy risks. Certain recommendations were followed. However, we remain very concerned about the program as a whole and are skeptical about whether security benefits will outweigh privacy risks.

Some of our key concerns include:

- The process for putting an individual's name on the list is not transparent and individuals won't have the right to know they are on the list until they try to board an airplane.
- There is a risk people will be stopped from flying because they have been incorrectly listed or share the name of someone on the list. (There have been many cases with the US no-fly list where false positives have meant children and well-known public figures such as Senator Edward Kennedy have been questioned or denied boarding.)
- There are serious risks arising from the possible sharing of the list with other governments by Transport Canada. There is also a risk air carriers would share the list with other countries.
- The process for people to have their names removed from the list is set out only in administrative procedures rather than in legislation, which must be passed by Parliament.

We are troubled that Canadians will not have legally enforceable rights of appeal or compensation for out-of-pocket expenses or other damages. We do not want to see the rights of Canadians unduly affected or compromised when traveling.

Conclusion

Parliament may not be sufficiently informed about how these various travel programs work and how they impact privacy both individually and collectively. Unfortunately, the current means of parliamentary reporting are not designed to provide detailed information about how such programs work or the privacy risks they entail.

Key Issue: Transborder Data Flows

PROTECTING PRIVACY IN A WORLD OF TRANSBORDER DATA FLOWS

We live in an era where the personal information of hundreds of thousands of people can be sent to the other side of the planet at the touch of a button

One of the most problematic privacy areas for Canadians is how to protect the ever-growing stream of personal information swirling around the globe.

Technology has made it easier for government departments to send Canadians' personal information beyond our borders – either as part of information-sharing arrangements with other countries or outsourcing contracts with information-processing companies.

These kinds of transborder flows are of increasing concern to the OPC – particularly given that shortcomings in the *Privacy Act* leave personal information without adequate legal protection.

Once information leaves Canada, it may become subject to the laws of a foreign country, including search and seizure laws. It may no longer be under the control of Canadian organizations or government institutions, except where there are contractual provisions.

How Information is Shared

In today's climate of concern about national security and criminal justice matters, governments are increasingly sharing sensitive personal information with foreign governments, police and security agencies. There is a risk that foreign governments and agencies may use such information in ways that may have a harmful effect on law-abiding Canadians.

The Government of Canada has many agreements with other countries and international agencies to share personal information. Federal departments share information directly with government institutions in other countries, generally under agreements which determine what the foreign institution can do with that information. In other cases, federal departments may, for administrative efficiency, “outsource” the processing of Canadians' personal information to companies abroad.

Transferring Information: a Risky Business

As we have already seen in the case of Mr. Maher Arar, the transfer of individuals' personal information outside Canada can have disastrous consequences.

In our 2005-2006 Annual Report on the *Privacy Act*, we reported on significant risks to privacy stemming from the information-sharing practices of the Canada Border

Services Agency (CBSA). The OPC's audit found the CBSA was verbally sharing a large amount of personal information with American officials rather than providing it on the basis of written requests – in contravention of both CBSA policy and a Canada-US agreement. As a result, the CBSA could not say how much information was being shared. The OPC made numerous recommendations which the CBSA agreed to implement. The OPC is following up to see whether these deficiencies have been addressed.

The CBSA audit raised important questions about the information-sharing practices of many federal government departments and whether more can be done to protect the privacy of Canadians when personal information is shared outside Canada's borders.

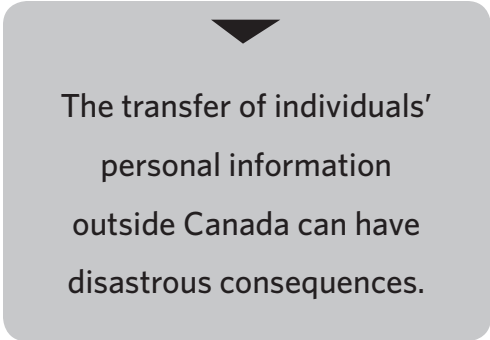
US Law Impacts Privacy in Canada

The fallout from 9-11 also prompted the development of another key piece of American legislation which has raised significant concerns on this side of the border – the *USA PATRIOT Act*. This legislation allows the US Federal Bureau of Investigation to obtain the personal information of people from around the world, including Canada, held by US companies.

In 2006, we looked at another significant issue involving US authorities secretly accessing Canadians' personal information.

In this case, American officials used subpoenas rather than the *USA PATRIOT Act* to gain access to massive amounts of international financial data, and Canadians' personal information was caught in this large net.

The information disclosures came to light in a *New York Times* article describing how, since 2001, the US Department of the Treasury has been regularly accessing tens of thousands of records from the Society for Worldwide Interbank Financial Telecommunication (SWIFT).



The transfer of individuals' personal information outside Canada can have disastrous consequences.


We investigated how personal information collected by Canadian financial institutions was subsequently disclosed to US authorities by SWIFT, a European-based financial cooperative that supplies messaging services and interface software to financial institutions in more than 200 countries, including Canada. We dealt with the case under *PIPEDA* and concluded that SWIFT did not contravene the Act when it complied with lawful subpoenas served outside the country. *PIPEDA* allows for an organization such as SWIFT to be able to abide by the legitimate laws of the other countries in which it operates.

However, in making her findings public, the Privacy Commissioner asked Canadian officials to urge their US counterparts to use Canada's anti-money laundering and anti-terrorism financing mechanisms to seek access to personal information rather than the subpoena route used to obtain such information from SWIFT. If American authorities feel they need to obtain information about financial transactions involving Canadians, they should be encouraged to use existing information-sharing mechanisms that have some degree of transparency and built-in privacy protections.

Part of our continuing concerns about personal information that flows to US government agencies is that the privacy safeguards afforded under the *US Privacy Act* are not extended to foreign nationals. Canadians are therefore deprived of privacy protections – including access and redress rights – under that law. On the other hand, anyone whose personal information is held in Canada can claim the protection of Canadian privacy law. It is worth noting that, during the reporting period covered in this annual report, the US and European Union were negotiating an agreement on air passenger data which we hope will extend *US Privacy Act* protections to all travelers, including Canadians, when their personal information is collected by the US government.

The Federal Government Response

The Treasury Board Secretariat has tried to address the fallout from the *USA PATRIOT Act* – releasing in 2006 a federal strategy in response to privacy concerns stemming from the law. Its review of outsourcing contracts among 160 federal institutions revealed that more than 80 per cent rated their contracts as having “no” or “low” risk. The review also helped departments and agencies identify measures to further mitigate privacy risks. Treasury Board Secretariat also developed guidelines setting out rules for outsourcing activities in which Canadians' personal information is handled or accessed by private sector agencies under contract with government institutions.



**Legal reforms are
urgently required.**

Having a federal strategy and policies to deal with transborder flows of personal information in the private sector are both welcome and useful, but legal reforms are also urgently required. As indicated earlier in this report, the *Privacy Act* lags woefully behind when it comes to dealing with globalization and the extensive outsourcing of personal information processing and storage.

Reforming the *Privacy Act*

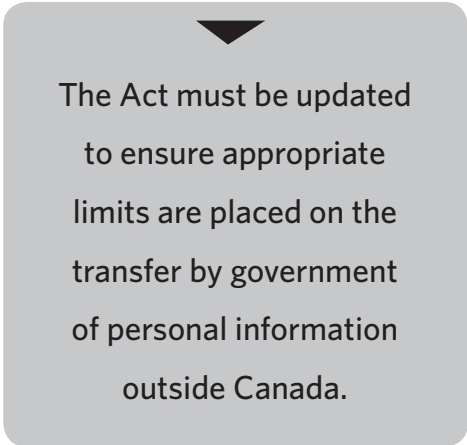
As mentioned, the *Privacy Act* is ill-suited for dealing with many of the pressures on privacy that flow from governments tempted to dismiss privacy concerns in their rush to “do something” about increasing security. The Act must be updated to ensure appropriate limits are placed on the transfer by government of personal information outside Canada.

The current law imposes very few controls on the transfer of personal information by government institutions to foreign government agencies and international agencies. For example, it allows a government institution to transfer personal information outside Canada without an individual’s consent if (a) there is an agreement or arrangement between Canada and the government of a foreign state, and (b) the disclosure is for the purpose of enforcing any law or carrying out a lawful investigation.

The *Privacy Act* also provides government institutions with general powers of disclosure. Heads of government departments may disclose personal information for any purpose – which could include providing the information to an organization outside Canada – when they believe the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure.

None of the *Privacy Act* provisions permitting the transfer of personal information outside Canada includes a requirement that the organization receiving information must treat it in accordance with the privacy standards Canadians expect.

An information-transfer agreement between a government department and a foreign agency may contain specific privacy safeguards, but that is a matter of happenstance, not a consistent obligation imposed by the *Privacy Act*. We need something more than happenstance to protect the privacy of Canadians when departments transfer personal information beyond our borders.



The Act must be updated to ensure appropriate limits are placed on the transfer by government of personal information outside Canada.

International Developments

As we push for changes to strengthen the *Privacy Act* in Canada, the OPC is also working on the international scene to deal with transborder issues. The Privacy Commissioner chairs an Organisation for Economic Co-operation and Development (OECD) volunteer group that has been examining ways to encourage cooperation between data protection authorities and other enforcement bodies with respect to cross-border complaints and cases arising from transborder data flows.

A report has been produced that summarizes the powers of enforcement authorities in OECD member countries and their ability to share information to facilitate cross-border cooperation. The report notes that despite differences in national laws, there is considerable scope for a more global and systematic approach to cross-border privacy law enforcement cooperation.

The volunteer group has also started working on a policy framework setting out a number of policy objectives and a description of the steps member countries can take to promote and support enforcement cooperation.

The OPC has also contributed to the work of the Asia-Pacific Economic Cooperation (APEC) on privacy issues. In light of our increasing data flows with a number of APEC member countries, Canada has been active in ensuring that core privacy values and principles are reflected in APEC data protection rules. Current work involves exploring ways to implement the APEC Privacy Framework that was adopted at the end of 2005.

Conclusion

Canadians want a better understanding of when and how their personal information is shared across international boundaries, whether as part of arrangements to outsource processing or under information-sharing agreements between governments in criminal, taxation or national security matters.

We need to constantly ask ourselves how information sharing is consistent with the privacy interests of Canadians. This does not mean that we ignore international cooperation in important matters such as national security, but it does mean we carefully consider the privacy impact of such cooperation and find ways to promote internationally the enforcement of privacy laws.

Key Issue: Privacy Impact Assessment Audit

A CRITICAL PRIVACY TOOL NEEDS TO WORK BETTER

An audit into the implementation of the federal Privacy Impact Assessment Policy concludes progress has been made, but there is still a significant way to go

One of the best tools federal government departments have to identify – and then reduce – the potential privacy risks of new or redesigned programs and services is a Privacy Impact Assessment (PIA).

An audit the OPC conducted this year into how departments and agencies are implementing the federal government’s Privacy Impact Assessment Policy identified serious flaws. The result is that Canadians’ privacy is not always as well protected as it could be.

Privacy Impact Assessments take a close look at how government departments protect personal information as it is collected, stored, used, disclosed and ultimately destroyed.

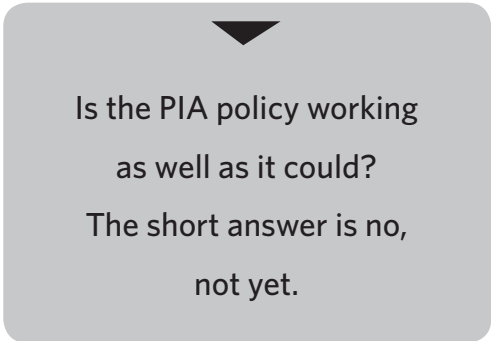
These assessments, which the 2002 federal PIA policy requires to be conducted in the planning phase of all new government initiatives raising privacy risks, are meant to help create a privacy-sensitive culture in departments by ensuring privacy protection is a core value.

Privacy Implications Overlooked

Given the importance of PIAs, the OPC undertook a government-wide audit into their use. We wanted to know: Is the PIA policy working as well as it could?

The short answer is no, not yet.

Some government institutions have made serious efforts to apply the PIA directive and have made progress. More work, however, is needed to ensure the policy is having the desired effect of promoting awareness and



Is the PIA policy working
as well as it could?
The short answer is no,
not yet.

understanding of the privacy implications associated with program and service delivery across government.

Audit Findings

While we did not identify cases of pervasive non-compliance, many institutions are not fully meeting their commitments under the policy – and, by extension – the intent or spirit of the *Privacy Act*.

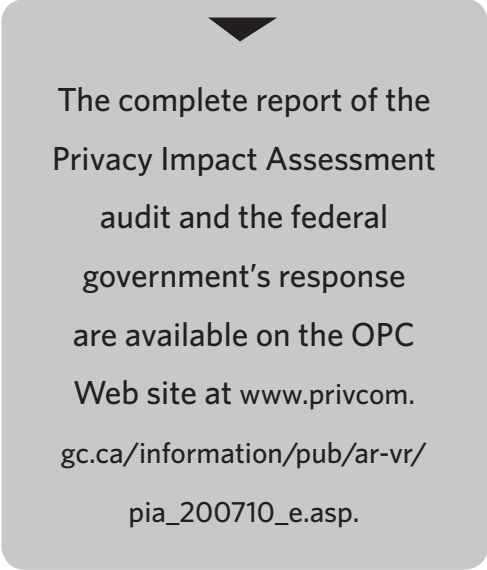
Some of the problems we identified are:

- PIAs are frequently completed well after program implementation – despite the policy’s primary aim of ensuring privacy protection is a key consideration in the initial framing of a project, program or service.
- In some cases, PIAs were not completed at all, even in cases where there was evidence of potential privacy issues stemming from a program or service.
- Not enough privacy consideration is provided for projects involving the sharing of personal information between institutions and with provincial and foreign governments, departments or agencies.
- Despite a requirement to make a public summary of each PIA, a minority of government departments regularly post and update their PIA reports to their external Web sites. Summaries that are posted often fail to disclose the privacy impact of the service or program or how any issues are being resolved.

There are many privacy risks associated with government programs and services, including identity theft, unintended disclosures and inappropriate data matching or data mining. Increasingly, we are seeing the government send Canadians’ personal information beyond our borders – raising the level of risk even higher.

The potential threats to privacy in all programs and services involving the handling of personal information need to be identified, evaluated and mitigated.

The extent to which privacy issues are appropriately managed depends on the maturity of a department’s PIA management framework.



The complete report of the
Privacy Impact Assessment
audit and the federal
government’s response
are available on the OPC
Web site at [www.privcom.
gc.ca/information/pub/ar-vr/
pia_200710_e.asp](http://www.privcom.gc.ca/information/pub/ar-vr/pia_200710_e.asp).

Our audit findings make clear that the privacy risks of many new programs and services are not being adequately considered or addressed. As well, the current PIA reporting provides little assurance or information to Canadians who want to understand the privacy implications of using a government service or program.

Public opinion polls consistently show Canadians are concerned about privacy and how the federal government is handling their personal information.

Treasury Board Secretariat has said that the government is “committed to protecting Canadians’ personal information in the delivery of services across all channels.”

In keeping with this declaration, the federal government introduced its Privacy Impact Assessment Policy (http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/siglist_e.asp) as a key privacy policy instrument and major feature of the federal privacy management framework.

The policy, which took effect May 2, 2002, requires assessments be conducted during the planning phase of all new initiatives which raise privacy risks. Some key steps include:

- Identifying all the personal information related to a program or service and looking at how it will be used;
- Mapping where personal data is sent after it is collected;
- Identifying privacy risks and the level of those risks; and
- Finding ways to eliminate or reduce privacy risks.

Departments are required to share the results of their assessments with the OPC and make a summary of the PIA available to the public. (A more detailed description of PIAs is included in a fact sheet on the OPC Web site at http://www.privcom.gc.ca/fs-fi/02_05_d_33_e.asp)

Strategic PIAs

We would like to see the privacy impacts of federal programs and systems assessed not only on a program-by-program basis, but also on a cross-cutting, strategic, government-wide basis.

For example, this year we reviewed a PIA of Transport Canada’s Passenger Protect Program (no-fly list) and concluded an opportunity may have been missed for a more strategic PIA into a broad range of national security measures.

PIAs should consider the cumulative privacy effects which are likely to result from a program in combination with other projects or activities. This would help ensure that the incremental effects of various programs are properly assessed.

The results of more strategic PIAs would offer Parliamentarians an early opportunity to modify programs in order to protect Canadians' personal information and to reduce future costs associated with program changes.

We believe Treasury Board Secretariat should consider the importance of strategic and larger-scope PIAs. Reviewing the whole PIA policy would ensure that its original goals are being achieved and that it helps build trust with Canadians. This policy renewal should include a review of the roles of the Treasury Board Secretariat and the OPC.

Conclusion

We have presented these PIA audit findings to the federal government and were pleased that the Treasury Board Secretariat of Canada and Privy Council Office agreed with our recommendations. Furthermore, departments and agencies subject to an audit have also generally agreed with our findings.

The responses appear to signal a re-commitment to assessing the privacy impacts of federal programs and systems, not just on an individual departmental or program basis, but also on a strategic government-wide basis. We hope this will mean the PIA process is set to mature and provide better privacy for Canadians. (See PIA Audit Report at www.privcom.gc.ca/information/pub/ar-vr/pia_200710_e.asp)

Responding to Complaints and Privacy Incidents

A look at how the OPC dealt with complaints and incidents under the Privacy Act in 2006-2007

Twenty-five years after the passage of the *Privacy Act*, the potential for privacy breaches has grown. Technology has made it easier for organized criminals and other fraudsters to obtain personal information illegally through the Internet; vast data banks store your personal information; and thieves can walk out the door with a computer hard drive containing your name and Social Insurance Number.

The OPC conducted close to a thousand investigations over the course of the fiscal year. While there were no discernable trends, human error and workplace surveillance surfaced as broad themes in the complaints and incidents we looked at. We also dealt with a clear case of identity theft concerning the Bank of Canada where fraudsters gained access to Canada Savings Bonds accounts and stole \$100,000. This incident was brought to our attention by the central bank. A police investigation was launched and charges were laid.

The OPC received 839 *Privacy Act* complaints in 2006-2007. That number is down from 1,028 complaints a year earlier. We have not tracked any significant trends that explain this slippage. Two institutions, Correctional Service Canada (194) and the RCMP (141) received the greatest number of complaints, accounting together for 40 per cent of total complaints received.

The OPC finalized 957 investigations in 2006-2007. The most common types of complaint files closed were Time Limits (441) and denials of access to personal information requests (240). (See Findings by Complaint Type p. 75). Time Limits complaints are lodged when requests for personal information are not met in the 30-day statutory timeframe (can be extended to 60 days in some circumstances). This type of complaint represented almost half of the total number of complaints (46 per cent). Delays in receiving personal information can greatly impact, for instance, on the outcome of work-related grievances or court and administrative tribunal hearings. It can also affect access to social services.

Over the year, the RCMP (115), Correctional Service Canada (43) and the Immigration and Refugee Board (40) topped the list of well-founded Time Limits complaints (includes well-founded and well-founded resolved. See page 77). It is to be noted, however, that, because of their mandate, some institutions deal with a high volume of personal information, and, therefore, are more likely to receive requests for personal information. This situation increases the likelihood of Time Limits complaints when statutory deadlines for access to personal information are not met. Complaints under the *Privacy Act* are lodged by government employees and in the large part, by the public.

Detailed statistical charts, definitions of types of complaints and findings under the *Privacy Act*, as well as a chart describing the OPC's investigation process, are included in the Appendices of this report.

COMPLAINTS – EXAMPLES OF CASES THE OPC INVESTIGATED

CASES INVOLVING HUMAN ERROR

Human error is the most predominant factor in privacy violations. As some of our cases have shown, carelessness in handling personal information can lead to privacy breaches. Government departments should urge employees to double-check procedures and remain vigilant when handling personal information. As part of its investigations, the OPC works with departments to prevent further breaches.

Offenders' personal information discovered in recycling area

Documents containing the personal information of approximately 100 offenders at the Correctional Service Canada (CSC) Regional Psychiatric Centre in Saskatoon were left in the facility's recycling area. A correctional officer found three offenders reading documents they had found in a garbage container.

CSC was not able to determine with any certainty how the documents, which contained medical information, became part of the regular garbage. It is likely that papers had overflowed from the shredding boxes and were mistaken for regular garbage. CSC notified those people whose information had been compromised. Eight people complained to the OPC.

The complaints were well-founded. The case was a combination of human error and ill-advised procedures. There was a similar case at the centre less than a year earlier. In both cases, the centre's handling of personal information left much to be desired and increased the potential for human error. The OPC made a number of recommendations on information-handling procedures which the CSC agreed to implement.

Correctional officer breaches privacy to prove a point

An offender complained that a Correctional Service Canada officer used his canteen purchase records to prove a point about an unrelated matter.

An offender had asked CSC for information relating to the possible health risks associated with inhaling smoke from sweet grass. In a written response, CSC informed him there did not appear to be any health studies about exposure to sweet grass. One officer added a note at the bottom of the document: “If you are worked up about the effects of smoke, I would suggest you stop using tobacco products as these contain numerous carcinogens, cause emphysema and heart problems.” He also attached a two-page printout of the offender’s canteen purchases, highlighting all tobacco products.

The complaint was well-founded. The OPC determined that canteen purchase records were personal information collected for security and management purposes. It concluded that those records could only be used for those purposes – not to prove a point about an offender’s health query.

Judicial review documents tucked into wrong envelope

A legal assistant with the Canadian Human Rights Commission accidentally included two packages of documents intended for separate individuals in the same envelope. As a result, the complainant’s personal information was disclosed to another person.

The Canadian Human Rights Commission had been served with applications for judicial review by two people. In accordance with Federal Court rules, the Commission must disclose relevant documents to the individuals who filed the applications. While preparing the two packages, a legal assistant accidentally inserted both sets of documents in the same envelope for mailing.

The person who received both sets of documents alerted the Commission, which then advised the complainant’s lawyer. The Commission receives approximately 100 applications for judicial review every year and stated this was the first time such an incident had occurred.

The complaint was well-founded. The incident occurred as a result of human error. To ensure the mistake does not happen again and to reinforce to staff the importance of protecting personal information, the Commission implemented a number of changes to its procedures. For example, legal assistants will write their initials on address labels. The lawyer responsible for the judicial review will be accountable for the disclosure of documents and review packages for accuracy.

The Commission also prepared a detailed list of steps to take whenever there is an information breach, including the retrieval of documents and immediate notification of the director and senior counsel.

CASES INVOLVING WORKPLACE SURVEILLANCE

Privacy in the workplace is a balancing act. People spend a lot of time at work but they do not lose their privacy rights when they enter the office. Continual surveillance affects employees' sense of dignity and freedom. However, some surveillance in the workplace is required – and clearly acceptable. Employers have the right to know whether workers are doing the job they are paid to do. In the following two investigations, we found that an appropriate balance had been struck.

Manager is justified in tapping into employee's e-mail account

An employee at Natural Resources Canada (NRCan) complained that his manager improperly accessed both his government e-mail and his personal Yahoo account in a bid to find cause to fire him.

Department officials stated they had not searched the employee's personal e-mail account but confirmed they had searched his government e-mail account. This was done, they said, after they came across a copy of an e-mail – addressed to one of the department's international clients – in which the employee made malicious references to the manager.

Concerned the employee may have sent other similar e-mail messages to clients, Natural Resources Canada officials searched the employee's government e-mail account. Several e-mails containing derogatory comments about supervisors were discovered.

NRCan concluded these e-mail messages were defamatory and spread false allegations and rumours that could harm the professional reputation of branch directors. It also found they undermined the manager's authority and constituted an inappropriate use of the government's electronic networks.

The federal government's policy on the use of electronic networks states e-mail is primarily a communication tool provided to employees for conducting official government business. The policy also prohibits unlawful activities, including defamation. The NRCan e-mail policy is available to all employees on the department's intranet site. Employees are given an electronic reminder when they log on to the network that they can be monitored for work-related purposes.

The complainant's e-mails were thought to be defamatory and therefore, in breach of government policy. The policy states that if an institution reasonably suspects an authorized individual is misusing the network, it must refer the matter for further investigation.

The complaint was not well-founded. The OPC concluded the employee had enough information to help him make an informed decision about the proper use of the department's e-mail system. It was the supervisor's duty to conduct an investigation and gather supporting documentation into what was considered workplace misconduct.

Harassment and vandalism complaints justify surveillance

The OPC received complaints from 37 CSC employees who argued their employer was using hidden surveillance cameras to collect their personal information without consent.

Managers at the Leclerc Institution, in Laval, Quebec, notified Correctional Service Canada that they were being threatened and harassed by staff.

In response to these threats, security measures were intensified. Two surveillance cameras were installed. The first, installed in July 2004, monitored movements in the corridor, while the second, installed in September, monitored movements in the administrative locker room and mailroom belonging to correctional officers. The first camera recorded continuous footage of the comings and goings in the corridor. The system looped recordings on the same tape every eight hours. Since no incidents occurred in this area, this tape was not viewed. The other camera was on for only one day because it was discovered by an employee while doing his rounds.

The complainants argued CSC had collected their personal information without their knowledge or consent by secretly videotaping them.

The complaint was unfounded. The OPC determined that under the *Financial Administration Act*, CSC was responsible for providing a safe work environment for its managers. Under the Treasury Board's anti-harassment policy, the institution's senior management should have launched an investigation to identify the individuals responsible for the harassment. Under the circumstances, the gradual measures used by CSC to try to put an end to the abuse against the supervisors were reasonable. The employer first sent a notice to employees and union representatives and added patrols in sectors where these incidents had occurred. The use of surveillance cameras was a logical next step in the investigation.

CASES OF INTEREST

Employee complains DND disclosed personal information

A full-time, non-union employee of the Canadian Forces Personnel Support Agency complained that a Department of National Defence (DND) labour relations officer disclosed a list containing the name, status, position title, pay-band and actual salary for all union and non-union members to the union.

The Canadian Forces Personnel Support Agency and the United Food and Commercial Workers Union were in contract negotiations. DND had prepared a detailed wage proposal containing the salaries of employees for discussion at the negotiation table. Union representatives were told the information was strictly confidential. The union negotiator did, however, share copies of the pay rates with members.

The case was settled in the course of investigation. The investigation established that, while the union requires information for negotiation purposes, it does not need the name and actual salary of union and non-union employees. DND decided it will no longer provide the names and actual wages of the employees in contract negotiations. It will only provide general information about pay rates.

Voter alarmed by political party canvasser's comments

A woman complained Elections Canada disclosed her personal information to a political party after a canvasser asked if the party could count on her continued support on election day.

The woman became concerned when she asked the canvasser how she had obtained her phone number and knew which party she was supporting and was told Elections Canada provided the information.

The *Canada Elections Act* allows registered political parties to obtain the electoral list from each polling division. These lists include the name and address of individuals but *not* the political party they supported in the last election. This information, which is provided to every candidate, Member of Parliament and registered political parties by Elections Canada, can be used for communicating with voters.

The *Canada Elections Act* allows individuals to delete their personal information from these electoral lists. Deleting a name in no way affects that person's right to vote.

The complaint was not well-founded. The complainant was satisfied that Elections Canada had not provided information about her party affiliation. She was pleased to discover her name could be deleted from the electoral list sent to political parties – a step other Canadians may not be aware is available.

RCMP says too much about family's troubles

A woman complained the RCMP disclosed too much information about the difficulties she was having in controlling her son's behaviour.

The complainant, a school teacher from another country, was taking part in an exchange program with a teacher in British Columbia. As part of the exchange, the teachers' families traded homes.

The complainant told an RCMP constable who came to her home that she was concerned that, since arriving in Canada, her 16-year-old son had dropped out of school, was taking drugs and was having house parties while she was away. She added her son had broken the lock in a room in the house where the owners had stored their valuables. The mother also said her son was stealing from her and she was locking her wallet in her car to stop him from taking her money.

One week later, the constable received a call from the Canadian owners of the house. They had heard from neighbours that police had been to their home in B.C. after someone complained of loud parties.

The RCMP officer told the Canadian homeowner about the loud party complaint and broken lock. He also recounted how the mother was locking her purse in the car and was becoming increasingly frustrated with her son's behaviour.

The OPC concluded the RCMP was obligated to disclose information to the homeowners with respect to the security of their home, including the parties, the broken lock and the property damage. However, the information should not have included the mother's efforts to protect her money from her son or reference to her growing frustrations.

While there was no indication of any malice on the part of the RCMP, this part of the complaint was well-founded.

RCMP takes precautions to protect identity of gun owners

Complainants worry gun owners will be identified after RCMP releases gun registry database to a newspaper.

The *Ottawa Citizen* obtained information related to the Canadian Firearms Registry through an *Access to Information Act* request to the RCMP. The newspaper then included the following statement on its Web site: “Tap into the gun registry database.” As a result, a number of people contacted the OPC to complain about the RCMP’s actions and express concern that they could be identified. Businesses complained their gun inventories would become publicly available, leaving them vulnerable to thieves.

The complaint was not well-founded. The OPC concluded the RCMP had taken precautions to ensure gun owners would remain anonymous. The RCMP had released information about registered firearms as well as the registration date, client type and the first two digits of the individual’s postal code. This was not considered personal information under the *Privacy Act*, which consists of information about an “identifiable individual.” The OPC also concluded the RCMP had not violated the privacy rights of business owners as it did not release the names of businesses or their owners.

Information collected without consent in suspected fraud case

A woman complained that Human Resources and Skills Development Canada (HRSDC) violated her privacy rights when it investigated an overpayment of benefits without first approaching her. She said HRSDC staff collected joint bank account statements and banking information and contacted her former employer.

The complainant was receiving maternity and parental benefits under the Employment Insurance program. HRSDC was notified the complainant had been hired by a company and determined she was working, but continuing to collect Employment Insurance benefits because she had not disclosed her income. HRSDC decided the complainant’s actions warranted prosecution for an overpayment of \$5,000 in benefits. As part of an investigation, the department asked the woman’s bank for records showing she had been receiving EI payments and wages at the same time. An investigator also asked her employer for payroll and employment information.

The complainant admitted to the allegations but claimed hardship due to the medical condition of her spouse. She argued HRSDC should have notified her before collecting her personal information. The department stated it acted within its legislated authority and added that notifying people prior to an investigation could result in the collection of inaccurate information.

The complaint was not well-founded. HRSDC had the legal authority to collect the information without the complainant's knowledge or consent in an investigation of that nature.

Informant complains identity disclosed to ex-wife

An individual alerted the Canada Revenue Agency (CRA) that his ex-wife, a CRA employee, had disclosed tax information and had viewed his tax information and that of others. He complained to the OPC that the tax agency had revealed to his former wife that in fact, he had made the accusations.

The complainant said he had been promised anonymity as an informant when he reported his ex-spouse's actions to the CRA. The CRA, however, said it had informed the complainant on three separate occasions it could not withhold his identity and that if his former spouse requested the information under the *Privacy Act*, it could be released.

The CRA concluded the complainant's ex-wife had, without authorization, accessed his tax records and had disclosed taxpayers' information. She was disciplined for her actions. During the disciplinary process, she received a report indicating her ex-husband had informed the CRA about her alleged wrongdoing.

The complaint was not well-founded. Under the *Privacy Act*, the disclosure of the complainant's name could not be withheld from the CRA employee. She was entitled to access that information because it was considered personal information about her under the Act.

Canada Revenue Agency justified in opening mail in alleged tax evasion case

An individual being investigated for alleged tax evasion complained CRA auditors opened the sealed mail found on his desk.

The complainant argued auditors had violated the provisions of a search warrant which allowed them to search for and seize information relating to transactions from 1996 to 2001. The mail on his desk was postmarked after that period. The complainant also stated auditors opened mail belonging to family members.

The CRA acknowledged it had opened mail postmarked after the dates specified in the search warrant, stating this was done to determine whether there were any documents relevant to its tax evasion investigation. The agency argued mail with a later postmark could relate to transactions under investigation. The CRA also stated the search warrant specifically referred to family members who were part of the investigation.

The complaint was not well-founded. CRA officials had the legal authority to enter the complainant's premises and conduct a search for and seize documents relevant to their investigation. The search warrant did not restrict the CRA from opening mail that was postmarked beyond the dates specified.

CRA Review

In 2006-2007, the OPC commissioned an independent review of more than 800 complaints directed at the Canada Revenue Agency from 2002-2003 to 2005-2006 to determine whether there were any overriding concerns. The goal was to allow the OPC to report more accurately on the causes and consequences of *Privacy Act* breaches and to see whether there were any trends.

The review found that denials of Access to personal information requests were the most common type of complaints. Individuals complained exemptions under the *Privacy Act* were not well applied. Time Limits complaints were also common. Delays in responding to access requests in the timeframe prescribed by law were likely due to limited resources.

As for use, collection and disclosure complaints, which represent a small fraction of the total number of complaints, there were no significant cases except when employees inappropriately accessed or used taxpayer information. There was evidence the CRA dealt with these cases with diligence and resolve by disciplining employees.

The review found the number of complaints against the CRA had dropped significantly in the last few years. The trend was also on a downward slope in 2006-2007. The specific reasons for the decline have not been identified. But the numbers suggest the agency may have taken innovative steps to address privacy concerns. The review did not detect any systemic personal information-handling issues. Overall, the OPC was pleased to find there appeared to be no widespread personal information management deficiencies at the CRA.

INCIDENTS UNDER THE *PRIVACY ACT*

In addition to individual complaints, the OPC also reviews cases of mismanagement of personal information brought to our attention through media reports and by government institutions. Incidents such as these often highlight a systemic issue that needs to be corrected as soon as possible.

INCIDENT INVOLVING IDENTITY THEFT

Canada Savings Bond accounts robbed of \$100,000 at Bank of Canada

The Bank of Canada notified the OPC that criminals had stolen a total of \$100,000 from the Canada Savings Bond payroll accounts of eight clients. In other cases, fraudsters gained access to accounts in order to obtain fraudulent credit cards and cellular phone accounts.

The Bank of Canada became aware of suspicious activity in several Canada Savings Bond accounts in late 2005. The central bank launched an internal investigation and contacted police. The bank notified all affected individuals and clients were reimbursed. A press release asking clients to contact the bank if they noticed any account inaccuracies was also issued.

The RCMP and Ottawa police completed their investigation in April 2006. Charges were laid. The bank reviewed its security processes and procedures relating to bondholder information. It also enhanced authentication measures and revised its redemption and change of address procedures. In May 2006, the bank informed all affected individuals that their accounts had been flagged and were being monitored on a daily basis to detect any inappropriate activities.

The OPC is satisfied that swift corrective measures were taken to secure bondholders' savings.

INCIDENT INVOLVING HUMAN ERROR

Employment history forms sold along with filing cabinet

The media contacted the OPC to report that documents containing the personal information of census employees were found in a filing cabinet sold at a Crown Assets sale.

During a census, Statistics Canada hires temporary staff and opens offices across the country. Once the census is complete, the offices are closed and Statistics

Canada sends the furniture to Crown Assets for disposal. Before sending the furnishings to Crown Assets, all cabinets are checked by one employee and then verified empty by a second employee. Stickers are then placed to indicate that a cabinet is ready for disposal.

An investigation showed that verification procedures were followed. The problem occurred when a census pay supervisor – who had moved to a new office – tried to print employment history forms. The documents wound up being printed at the old office, which was being closed. It appears somebody picked up the papers and put them away in a surplus filing cabinet which had already been emptied. The cabinet was then sold.

Following this incident, Statistics Canada introduced an additional step to its disposal procedures. Staff now place tape across every drawer once a filing cabinet has been inspected and labelled for disposal. If the tape is broken, the process is repeated. And for any future moves, the agency will ensure all printers and computers are disconnected at the same time.

PUBLIC INTEREST DISCLOSURES UNDER THE *PRIVACY ACT*

Heads of government institutions have the discretion to disclose personal information without consent when the disclosure benefits the individual or when a compelling public interest outweighs the invasion of that person's privacy. Unless an emergency dictates otherwise, the Privacy Commissioner must be notified of such disclosures in advance. The OPC reviews proposed disclosures and, if deemed necessary, the Commissioner notifies the individual. The OPC also advises institutions when we feel the amount of personal information slated for release goes beyond the public interest. We then make recommendations to minimize privacy intrusions.

The OPC reviewed 90 public interest disclosure notices in 2006-2007. The large majority of these were decisions by the RCMP to disclose personal information concerning offenders about to be released from prison after serving their sentences. They were all considered to be high-risk offenders who posed a danger to the community. In other cases involving the RCMP, personal information was made public in order to locate a suspect or warn people about a violent or sexual offender's actions.

A significant number of other disclosure notices from several departments, such as National Defence and Correctional Service Canada, concerned the release of information about the nature of an individual's death to family members. In most cases, the nature of the death of military personnel and offenders was disclosed for compassionate reasons.

WHAT HAPPENS WHEN YOU FILE A COMPLAINT WITH THE OPC? A STEP-BY-STEP APPROACH

Protecting your Privacy: How to file a complaint with the Privacy Commissioner

Your Social Insurance Number has been disclosed to an unknown party by a government agency without your consent.

You panic.

Your greatest fear is that a con artist has his hands on your personal information and will drain your bank account and ruin your credit rating.

You file a complaint with the Office of the Privacy Commissioner of Canada. First piece of advice: Put your complaint in writing and do not forget to mention that you are invoking your rights under the *Privacy Act*. It is preferable to send everything to the OPC by mail. A faxed document can always be intercepted, and, unfortunately, we cannot accept complaints via e-mail.

A case will then be opened and assigned to an investigator to determine whether the allegations contravene the *Privacy Act*. The investigator will interview the complainant as well as officials from the department involved, and any witnesses, gather evidence, and provide his or her recommendations to the Commissioner.

Investigators have *carte blanche* to conduct investigations

This is the general process followed by the 14 investigators who investigate complaints under the *Privacy Act*. They routinely take an in-depth look at a host of issues: Was an individual's personal information disclosed by a federal department? If so, for what purpose? Why was an individual denied access to his or her personal information records? Were the established time limits for sending documents met?

Investigators have extensive powers delegated to them by the Commissioner. They have the right to enter any office of a federal institution. Except for Cabinet documents, investigators can have access to any document they deem necessary for their investigation. They have *carte blanche* to go up the chain of command as far as a deputy minister or head of a federal institution if need be.

Unexpected turns

Investigations can last several months and sometimes take unexpected turns.

“I actually had to go to a port to see where the surveillance cameras were located,” says an experienced investigator. In another case, documents sought from a specific department mysteriously disappeared ... twice. Because of the lack of evidence, the case fell apart.

In short, a day in the life of an investigator is far from typical. Investigators have to keep their ears open, arm themselves with courage and patience, and be flexible.

The OPC’s Investigation branch employs people from all walks of life: a former RCMP officer who led criminal investigations, an archivist and a nurse, to name a few.

“You must have good judgment and it is critical that you understand the legislative requirements of a specific department,” says one seasoned investigator.

It is also useful to have been on both sides of the fence. An analyst for a government department whose job was to go through access to information and privacy requests with a fine tooth comb, now conducts investigations for the OPC.

“I know how to find information ... it speeds up the process and prevents us from running around in circles,” says another investigator.


Investigations are conducted with vigour, keeping in mind the Privacy Commissioner’s ombudsman role.

“We take a co-operative approach,” says an investigator who has been around the block. “We negotiate instead of forcing things.”

Branch Activities

POTENTIAL PRIVACY RISKS: MONITORING FEDERAL GOVERNMENT PROGRAMS

Privacy Impact Assessments (PIAs) are tools that help federal departments and agencies ensure that privacy protection is a core value when a new program or system is planned and implemented. An ongoing responsibility of the Audit and Review Branch is to evaluate PIAs to determine whether there are potential privacy risks associated with government programs and services.




PIAs should offer safeguards against the inappropriate disclosure of personal information.

PIAs: Are they Measuring Up?

PIAs are designed to identify and mitigate privacy risks. They are meant to document what personal information is collected and why, how it is collected, used, transmitted, stored and retained. PIAs should also offer safeguards against the inappropriate disclosure of personal information.

In 2006-2007, we reviewed 22 individual PIAs for projects ranging from the implementation of a health indicators survey involving collection of blood and urine samples to an RCMP information-sharing project.

We have been monitoring the RCMP's National Integrated Information Initiative (N-III), an integrated information-sharing system that involves courts, prosecution offices, border control services, parole, probation and correctional agencies.



In an earlier section of this annual report, we summarized the results of our government-wide audit of the PIA function. Essentially, we found that the PIA function is not working as well as it should. This section describes some of our PIA review work.

This data sharing, when fully integrated, is expected to involve personal information collected not only by law enforcement bodies, but also by other government departments during special departmental and administrative investigations, such as those carried out by the Canada Border Services Agency and Citizenship and Immigration Canada into suspected fraud, smuggling, or other infractions of border control or immigration legislation. This kind of database has the potential to become a huge electronic information warehouse that could be used for increased surveillance and profiling.

The RCMP initiative includes several components: the Law Enforcement Information Portal, Police Records Information Management Environment of British Columbia, Integrated Query Tool, the Police Reporting and Occurrence System, and Computer-Assisted Dispatch applications.

These components were developed separately and, therefore, their privacy risks have been considered separately. However, these various initiatives – when considered collectively – will have a major impact on personal information sharing among national, provincial, and municipal police forces, as well as government departments and international partners.

The OPC has asked the RCMP to conduct a Privacy Impact Assessment of the initiative as a whole. An information-sharing network of this size and sensitivity should be subject to a high standard of scrutiny, transparency, and accountability. While the RCMP responded positively to our suggestion, more than one year later we had still not received the comprehensive assessment but were advised it was forthcoming. The program was being implemented without the benefit of a completed comprehensive PIA. The OPC continues to urge the completion of this PIA.



**Some of our Audit and Review
Accomplishments in 2006-2007 Include:**

- Completion of four audit projects started in the prior year and launch of six new audit projects, three of which were in their final stages at the end of the fiscal year;
- Completion of 22 PIAs and 13 other projects involving information, assessment or advice on privacy practices; and
- Consultations with departments and agencies about the privacy implications and risks of new programs or systems.

Canada Revenue Agency - Time Limits Review

In 2005, we received a request from the Union of Taxation Employees to audit the Canada Revenue Agency's use of Time Limits extensions when processing *Privacy Act* requests. The union makes such requests on behalf of members involved in grievances.

The *Privacy Act* gives Canadians the right to access their personal information held by government institutions. Institutions must respond within 30 days, but, under certain circumstances, the limit can be extended by an additional 30 days.

The OPC received a total of 35 extension notice complaints against the CRA from April 2000 to March 2006 – 15 of them from one individual. We found 60 per cent of these were well-founded, often in cases where the agency claimed extensions due to summer staff shortages.

In 2006 – after the union requested the audit – the agency processed all requests filed on behalf of union members without a Time Limits extension. In previous years, roughly 85 per cent of requests were processed during the extension period. Our review did not suggest a full audit was necessary since the CRA had remedied the problem during the period of our intervention.

IN THE COURTS

Overall, there were very few court actions proceeding under the *Privacy Act* in 2006-2007. As noted earlier, the *Privacy Act* provides for only limited judicial recourse in the case of improper denials of access. There is no judicial recourse available for the improper collection, use or disclosure of personal information by a government institution.

Complainants can obtain no further relief under the *Privacy Act* beyond the Commissioner's non-binding report and recommendations. Because of the lack of well-entrenched remedies available under the *Privacy Act*, individuals have little choice but to resort to other less direct, and less accessible judicial means.

One vivid example concerns a case that was brought before the Ontario courts in 2006-2007. In this particular case, prison guards' personal information was not sufficiently safeguarded. The situation resulted in the improper disclosure of their information to the prison population.

The OPC's involvement in the matter began when a prison guard complained to our office and ended when we issued a well-founded report and non-binding recommendations. The plaintiffs had no other option but to pursue their claims before the Ontario Superior Court under such causes of action as breach of a common law right to privacy and breach of their *Charter* rights. The Ontario Court of Appeal recently dismissed the Crown's motion to strike the plaintiffs' claim. It ruled their case could move forward on the grounds raised. (See *Jackson v. Canada (Attorney General)*, 2006 CanLII 32311 (ON C.A.))

Ideally, individuals should be able to pursue redress before the courts through the *Privacy Act* but our calls to amend the Act have not been heeded. As a result, individuals must continue to take other means to seek remedy.

Judicial Review

The following judicial review and other cases of interest were filed in 2006-2007. In keeping with our mandate, we have chosen not to publish the plaintiff's name in order to protect the privacy of the complainants. Only the court docket number and the name of the government institutions are listed.

X. v. Privacy Commissioner of CanadaFederal Court File T-1628-06

In this case, a plaintiff submitted an application for judicial review under section 18.1 of the *Federal Courts Act* to challenge a decision by the Office of the Privacy Commissioner.

The OPC informed the applicant in a letter that his complaint would not be immediately assigned to an investigator, since the investigators' workload at the time was unusually high.

The applicant complained that the Canada Post Corporation had refused to reveal the identity of the person who was allegedly attacking his reputation. That person had used Canada Post's distribution system to vilify him by sending 800 letters to the inhabitants of a reserve where the applicant held a key position. The mailing method led the complainant to believe Canada Post had information about the author of the letters.

The applicant tried to obtain a court order requiring the OPC to immediately assign an investigator to investigate his complaint which he had filed against the Canada Post Corporation in April. The complaint was subsequently assigned to an investigator in September, which led to the withdrawal of proceedings before the Federal Court.

X. v. Privacy Commissioner of CanadaFederal Court File 07-T-22

The applicant, a Health Canada employee, underwent a "fitness to work evaluation" to assess her capacity to return to work following a period of sick leave and long-term disability. She complained to the Privacy Commissioner that the Health Canada physician who examined her had disclosed her medical information in a letter to her employer without her consent. The complaint centered around one sentence which said there had been "significant improvement" in the employee's medical condition.

The Privacy Commissioner investigated the matter and concluded the complaint was not well-founded. The Commissioner also found the physician's letter did not disclose the nature of the illness of the Health Canada employee or other personal information in breach of the *Privacy Act*. The findings were communicated to the applicant in October 2006.

Seven months after the Commissioner's report was released, the applicant filed a motion in court against the Office of the Privacy Commissioner, requesting an extension of the time limit as set out in the *Privacy Act* to review the Commissioner's findings. The OPC opposed this request on various grounds. On May 17, 2007, the Federal Court dismissed the applicant's motion. The court ruled that she had not proven "an active and continued interest" to pursue the case against Health Canada after the release of the OPC's report.

Intervention in a Matter Involving the *Access to Information Act*

X. v. Minister of Health Canada

Federal Court File T-347-06

The Commissioner was granted intervener status in a case filed under the *Access to Information Act*, which involves important new and emerging privacy issues. This case raises the issue of possible re-identification of individuals when government information is combined with information which is already available to the public.

X v. Minister of Health Canada was initiated in February 2006. Under the *Access to Information Act*, the applicant tried to obtain an order forcing the Minister to provide him with certain information fields contained in a departmental database. This database contained information on the adverse side effects of medication.

The Minister refused to allow the applicant's request on the grounds that the disclosure of these information fields could lead to the possible identification of individuals if this information were to be combined with other information accessible to the public.

This case raises an important question: To what extent does "personal information" as defined in the *Privacy Act* include information that could, when combined with other information, potentially identify the individuals concerned? In other words, at what point does information become information concerning an "identifiable individual" as defined in the *Privacy Act*? The OPC received intervener status in this case and submitted a brief to the Federal Court. The hearing in this case is scheduled for November 15, 2007.

The Year Ahead

We have identified several key priorities for the coming year. These include:



Improve and expand service delivery

- The OPC will reduce backlogs and improve response times of complaint investigations and Privacy Impact Assessment reviews.
- We will continue to increase the number of audits and follow-up audits of privacy systems and practices in both the public and private sectors.




Engage with Parliament on privacy issues

- We will continue to support Parliamentarians through the provision of useful and timely submissions and policy positions relating to potential privacy implications of proposed legislation and government initiatives.




Continue to promote *Privacy Act* reform and *PIPEDA* review

- The OPC will continue to promote *Privacy Act* reform by engaging Parliament and encouraging federal institutions to respect the privacy rights of individuals.
- The OPC will continue to take an active role in a mandated parliamentary review of *PIPEDA*.


**Host and evaluate the 29th International Conference
of Data Protection and Privacy Commissioners**

- The OPC will intensify efforts to ensure the September 2007 conference is a success.


Build organizational capacity

- Review and finalize OPC organizational structures, including the creation of regional offices; create and classify new positions and recruit staff.
- Provide training and development opportunities for new and existing staff.
- Implement aspects of the new *Federal Accountability Act* affecting the OPC, namely the creation of an office to handle access to information and privacy requests.
- Improve the OPC's infrastructure (e.g. Information Management / Information Technology, accommodations, policies and procedures).

Appendix 1

DEFINITIONS OF COMPLAINT TYPES

Complaints received in the OPC are categorized into three main groups:

Access:

- **Access** – All personal information has not been received, either because some documents or information are missing or the institution has applied exemptions to withhold information.
- **Correction/Notation** – The institution has failed to correct personal information or has not placed a notation on the file in the instances where it disagrees with the requested correction.
- **Language** – Personal information was not provided in the official language of choice.
- **Fee** – Fees have been assessed to respond to a *Privacy Act* request; there are presently no fees prescribed for obtaining personal information.
- **Index** – Infosource (a federal government directory that describes each institution and the banks of information – groups of files on the same subject – held by that particular institution) does not adequately describe the personal information holdings of an institution.

Privacy:

- **Collection** – Personal information collected is not required for an operating program or activity of the institution; personal information is not collected directly from the individual concerned; or the individual is not advised of the purpose of the collection of personal information.
- **Retention and Disposal** – Personal information is not kept in accordance with retention and disposal schedules (approved by the National Archives and published in Infosource): either destroyed too soon or kept too long. In addition, personal information used for an administrative purpose must be kept for at least two years after the last administrative action unless the individual consents to its disposal.

- **Use and Disclosure** – Personal information is used or disclosed without the consent of the individual and does not meet one of the permissible disclosures without consent listed in section 8(2) of the Act.

Time Limits:

- **Time Limits** – The institution did not respond within the statutory limits.
- **Extension Notice** – The institution did not provide an appropriate rationale for an extension of the time limit, applied for the extension after the initial 30 days had been exceeded, or applied a due date more than 60 days from date of receipt.
- **Correction/Notation - Time Limits** – The institution has failed to correct personal information or has not placed a notation on the file within 30 days of receipt of a request for correction.

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

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

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

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

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

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

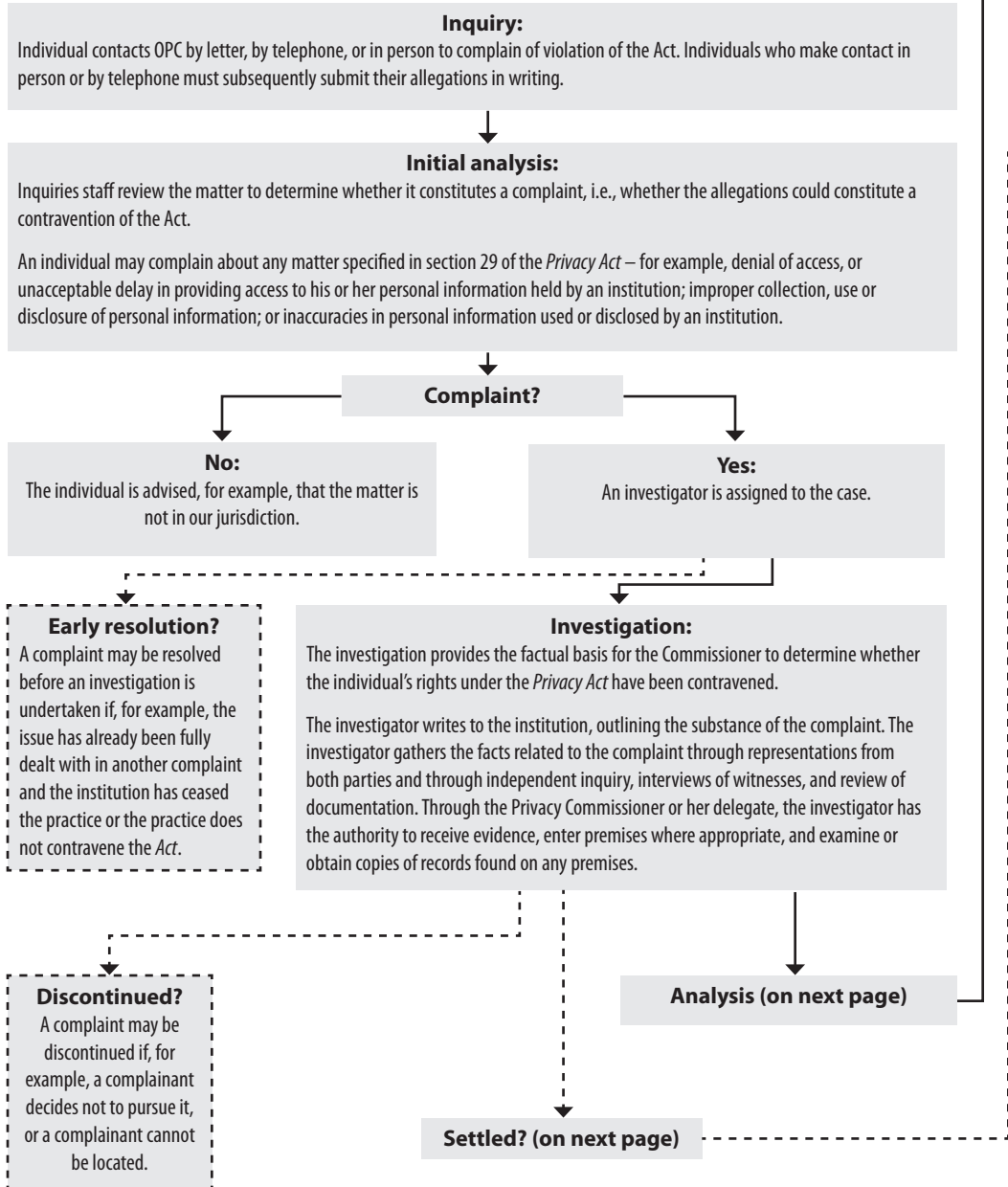
Resolved: After a thorough investigation, the OPC helped negotiate a solution that satisfies all parties. The finding is used for those complaints in which well-founded would be too harsh to fit what essentially is a miscommunication or misunderstanding.

Settled during the course of the investigation: The OPC helped negotiate a solution that satisfies all parties during the investigation, but issues no finding.

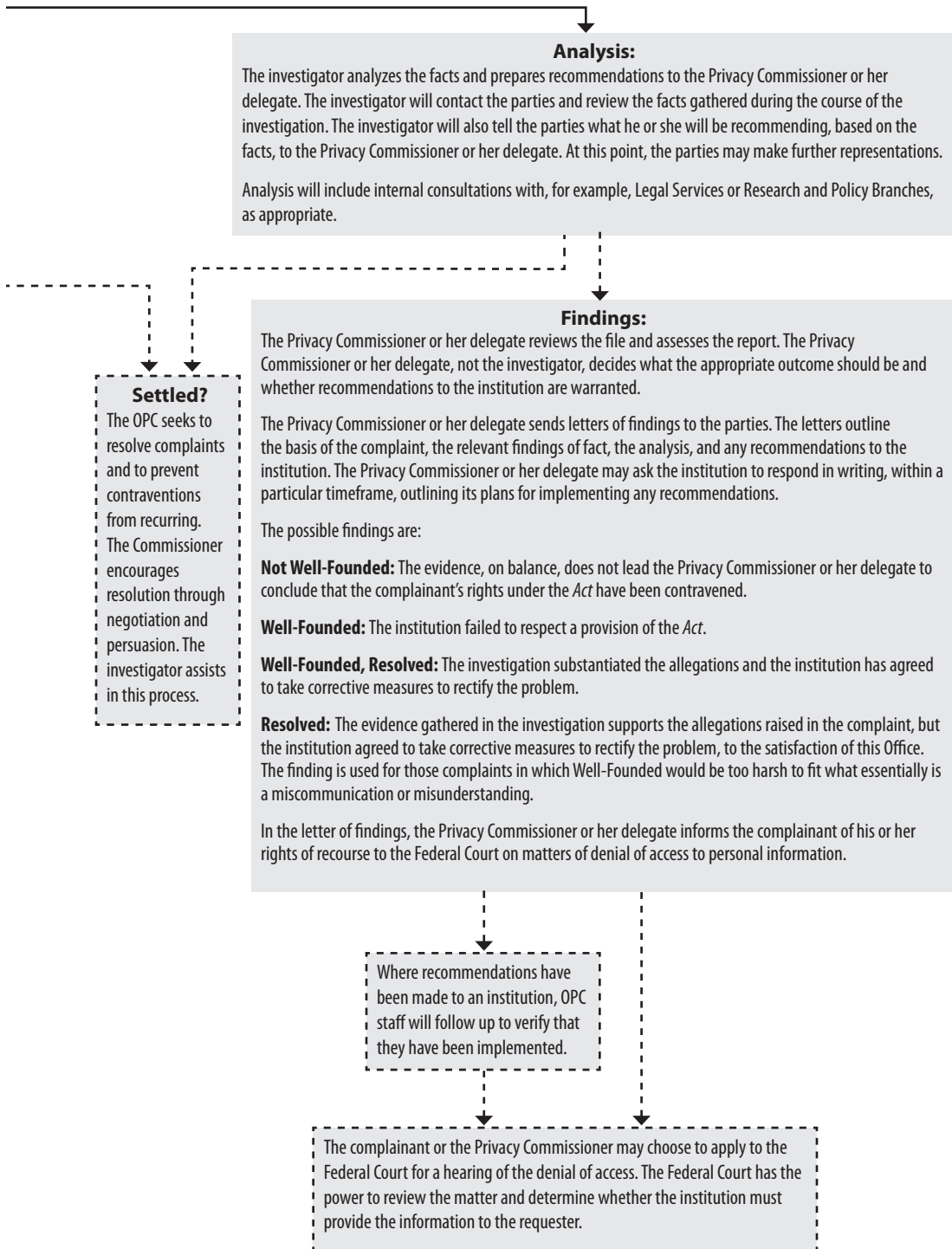
Discontinued: The investigation was terminated before all the allegations were fully investigated. A case may be discontinued for any number of reasons—the complainant may no longer be interested in pursuing the matter or cannot be located to provide additional information critical to reaching a conclusion.

Appendix 2

INVESTIGATION PROCESS UNDER THE *PRIVACY ACT*



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



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

Appendix 3

COMPLAINTS RECEIVED BY COMPLAINT TYPE

Complaints received between April 1, 2006 and March 31, 2007

Complaint Type	Total	Percentage
Access	317	38
Time Limits	292	35
Use and Disclosure	149	18
Extension Notice	29	3
Collection	28	3
Correction-Notation	11	1
Correction-Time Limits	8	1
Retention and Disposal	5	1
Total	839	100

The distribution of complaint types is similar to previous years with a few exceptions. The percentage of Time Limits complaints has dropped to 35 per cent from 40 per cent a year earlier. Use and Disclosure complaints have increased from 11.2 per cent to 18 per cent.

TOP 10 INSTITUTIONS BY COMPLAINTS RECEIVED

Institutions that received the greatest number of complaints for the fiscal year ending March 31, 2007

Organization	Total	Access to Personal Information	Time	Privacy
Correctional Service Canada	194	64	88	42
Royal Canadian Mounted Police	141	66	65	10
Canada Revenue Agency	86	30	28	28
National Defence	59	21	31	7
Citizenship and Immigration Canada	49	20	22	7
Canada Border Services Agency	40	11	24	5
Service Canada	38	14	7	17
Foreign Affairs and International Trade	26	11	9	6
Canadian Security Intelligence Service	25	17	8	0
Canada Post Corporation	24	9	6	9
Others	157	65	41	51
Total	839	328	329	182

Overall, two institutions, Correctional Service Canada and the RCMP, accounted for 40 per cent of complaints received for fiscal 2006-2007. However, a high number of complaints filed against an institution does not necessarily mean that institution is not complying with the *Privacy Act*. Because of their mandate, some government departments hold a substantial amount of personal information and are therefore more likely to receive requests for access to that information. This situation increases the likelihood of complaints about an institution's collection, use and disclosure, retention and disposal of personal information, and the manner in which it provides access to that information. There is some overlap between Time Limits and Access complaints. One request to a department for personal information can trigger two complaints to the OPC: one complaint for Time Limits if that request is not met within 30 days (or 60 days if there is an extension) and another for denial of access when there is failure to disclose all the information requested.

COMPLAINTS RECEIVED BY INSTITUTION

Complaints received against federal institutions for the fiscal year ending March 31, 2007

	Total
Correctional Service Canada	194
Royal Canadian Mounted Police	141
Canada Revenue Agency	86
National Defence	59
Citizenship and Immigration Canada	49
Canada Border Services Agency	40
Service Canada	38
Foreign Affairs and International Trade Canada	26
Canadian Security Intelligence Service	25
Canada Post Corporation	24
Fisheries and Oceans	15
Human Resources and Social Development Canada*	14
Agriculture and Agri-Food Canada	11
Justice Canada	11
Canada Firearms Centre	10
Health Canada	10
Transport Canada	10
National Parole Board	8
Environment Canada	7
Immigration and Refugee Board	7
Privy Council Office	6
Canadian Nuclear Safety Commission	4
Freshwater Fish Marketing Corporation	4
Public Service Commission Canada	4
Statistics Canada	4
Canada Economic Development for Quebec Regions	3
Industry Canada	3
Library and Archives Canada	3
Public Safety and Emergency Preparedness Canada	3
Atlantic Canada Opportunities Agency	2
Export Development Corporation	2
Indian and Northern Affairs Canada	2

Complaints received against federal institutions for the fiscal year ending March 31, 2007 (cont.)

	Total
Inspector General of CSIS, Office of the	2
Office of the Chief Electoral Officer	2
Treasury Board of Canada Secretariat	2
Canada School for Public Service	1
Canadian Radio-Television and Telecommunications Commission	1
Canadian Space Agency	1
Correctional Investigator Canada	1
Human Resources and Skills Development Canada*	1
Public Service Labour Relations Board	1
Public Works and Government Services Canada	1
Vancouver Port Authority	1
Total	839

* Note that the name of one department changed from Human Resources and Skills Development Canada to Human Resources and Social Development Canada. Complaints are listed under the name of the department at the time the complaint was made.

COMPLAINTS RECEIVED BY PROVINCE/TERRITORY

Complaints received by province and territory for the fiscal year ending March 31, 2007

Province/Territory	Total	Percentage
British Columbia	235	28
Ontario	195	23
Quebec	116	14
National Capital Region	81	10
Alberta	77	9
Saskatchewan	44	5
Manitoba	34	4
New Brunswick	22	3
Nova Scotia	19	2
International	9	1
Newfoundland	4	<1
Prince Edward Island	2	<1
Northwest Territories	1	<1
Total	839	100

It should be noted that 65 per cent of complaints originated in the provinces of Quebec, Ontario, and British Columbia. This year, the number of complaints received from Ontario and Quebec declined, and British Columbia moved from third to first place. We have not identified any significant trends explaining the increase of complaints in B.C. or the reduction of complaints in Ontario and Quebec.

FINDINGS BY COMPLAINT TYPE

Findings, all complaint types, for fiscal 2006-2007

In total, 957 complaints were finalized

Complaints (All Types) Closed

	Discontinued	Early Resolution	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Well-founded-Resolved	Total
Time Limits	49	2	55	0	3	331	1	441
Access	41	17	91	12	41	2	36	240
Use and Disclosure	25	14	22	1	12	23	1	98
Extension Notice	2	0	45	0	0	14	0	61
Collection	5	2	45	0	3	0	0	55
Correction-Notation	4	2	30	0	1	0	8	45
Correction- Time Limits	3	0	1	0	0	4	0	8
Retention and Disposal	2	1	3	0	1	0	1	8
Language	1	0	0	0	0	0	0	1
Total	132	38	292	13	61	374	47	957

Access and Privacy Complaints Closed

	Discontinued	Early Resolution	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Well-founded-Resolved	Total
Access	41	17	91	12	41	2	36	240
Use and Disclosure	25	14	22	1	12	23	1	98
Collection	5	2	45	0	3	0	0	55
Correction-Notation	4	2	30	0	1	0	8	45
Retention and Disposal	2	1	3	0	1	0	1	8
Language	1	0	0	0	0	0	0	1
Total	78	36	191	13	58	25	46	447

As in previous years, there are clearly far more not well-founded complaints than well-founded Access and Privacy complaints: 191 and 71 respectively (includes well-founded resolved). In addition, a significant number of complaints, 185 of 447, or 41 per cent, were resolved in some way (discontinued, early resolution, resolved or settled in the course of investigation). Only 16 per cent of complaints to the OPC under the *Privacy Act* are well-founded. This is up from 10 per cent in 2005-2006. Overall, we believe this still speaks well for compliance with the Act.

Findings, all complaint types, for fiscal 2006-2007 (cont.)**Time Limits Complaints Closed**

	Discontinued	Early Resolution	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Well-founded-Resolved	Total
Time Limits	49	2	55	0	3	331	1	441
Extension Notice	2	0	45	0	0	14	0	61
Correction-Time Limits	3	0	1	0	0	4	0	8
Total	54	2	101	0	3	349	1	510

By their very nature, the majority of Time Limits complaints are well-founded. Organizations have 30 days from the date of receipt to respond to requests for access to personal information. Individuals do not complain unless there has been a delay in responding to their request. Some Time Limits complaints are not well-founded because Extension Notices have been appropriately applied. These notices allow for an additional 30 days to respond. There are also examples where the complainants did not allow for mailing time.

TIME LIMITS COMPLAINTS CLOSED BY INSTITUTION AND FINDING

Respondent	Discontinued	Early Resolution	Not well-founded	Settled in course of investigation	Well-founded	Well-founded Resolved	Total
Royal Canadian Mounted Police	13	0	1	1	114	1	130
Immigration and Refugee Board	0	0	51	0	40	0	91
Correctional Service Canada	11	0	9	2	43	0	65
Canada Revenue Agency	8	0	6	0	23	0	37
Canada Border Services Agency	2	0	0	0	30	0	32
Citizenship and Immigration Canada	3	1	3	0	23	0	30
National Defence	4	0	1	0	23	0	28
Justice Canada	5	0	5	0	12	0	22
Foreign Affairs and International Trade Canada	3	0	1	0	13	0	17
Health Canada	1	0	0	0	13	0	14
Agriculture and Agri-Food Canada	0	0	3	0	3	0	6
National Resources Canada	0	0	5	0	0	0	5
Canada Post Corporation	0	0	1	0	3	0	4
Environment Canada	2	0	2	0	0	0	4
Fisheries and Oceans	0	0	4	0	0	0	4
Human Resources and Skills Development Canada*	0	1	1	0	1	0	3
Atlantic Canada Opportunities Agency	2	0	0	0	0	0	2
Canada Firearms Centre	0	0	2	0	0	0	2
Canadian Security Intelligence Service	0	0	0	0	2	0	2
Industry Canada	0	0	2	0	0	0	2
National Parole Board	0	0	2	0	0	0	2
Transport Canada	0	0	1	0	1	0	2

* Note that the name of one department changed from Human Resources and Skills Development Canada to Human Resources and Social Development Canada. Complaints are listed under the name of the department at the time the complaint was made.

TIME LIMITS COMPLAINTS CLOSED BY INSTITUTION AND FINDING (cont.)

Respondent	Discontinued	Early Resolution	Not well-founded	Settled in course of investigation	Well-founded	Well-founded Resolved	Total
Export Development Corporation	0	0	0	0	1	0	1
Freshwater Fish Marketing Corporation	0	0	0	0	1	0	1
Human Resources and Social Development Canada*	0	0	0	0	1	0	1
Privy Council Office	0	0	0	0	1	0	1
Service Canada	0	0	0	0	1	0	1
Treasury Board of Canada Secretariat	0	0	1	0	0	0	1
Total	54	2	101	3	349	1	510

The OPC continues to be concerned about the number of Time Limits complaints filed against major institutions serving the public. We are pleased some institutions have taken steps to address staffing challenges. The OPC continues to monitor and assess compliance with the Time Limits requirements of the *Privacy Act*.

* Note that the name of one department changed from Human Resources and Skills Development Canada to Human Resources and Social Development Canada. Complaints are listed under the name of the department at the time the complaint was made.

ACCESS AND PRIVACY COMPLAINTS CLOSED BY INSTITUTION AND FINDING

Respondent	Discontinued	Early Resolution	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Well-founded - Resolved	Total
Correctional Service Canada	19	15	65	3	9	18	9	138
Canada Revenue Agency	11	3	13	1	14	0	6	48
Royal Canadian Mounted Police	9	3	14	0	7	2	7	42
Agriculture and Agri-Food Canada	0	0	29	2	0	0	6	37
National Defence	5	2	16	0	1	1	5	30
Citizenship and Immigration Canada	3	2	2	2	7	0	3	19
Immigration and Refugee Board	1	0	11	2	1	1	2	18
Justice Canada	6	0	2	0	1	0	1	10
Canada Post Corporation	4	1	3	0	1	0	0	9
Human Resources and Skills Development Canada*	4	1	2	0	1	0	1	9
Canadian Security Intelligence Service	0	0	6	0	2	0	0	8
Human Resources and Social Development Canada*	0	1	4	0	1	1	1	8
Canada Border Services Agency	5	1	1	0	0	0	0	7
Service Canada	0	3	0	0	3	1	0	7
Canada Customs and Revenue Agency	0	0	4	0	0	0	1	5
Export Development Corporation	0	0	4	0	0	0	1	5
Foreign Affairs and International Trade Canada	0	0	1	0	3	0	0	4
Health Canada	2	0	1	0	1	0	0	4
Industry Canada	1	1	2	0	0	0	0	4
Fisheries and Oceans	0	0	2	0	0	0	1	3
Office of the Chief Electoral Officer	1	0	0	0	2	0	0	3
Public Works and Government Services Canada	0	0	0	1	2	0	0	3
Social Development Canada*	0	0	1	1	1	0	0	3
Canada Economic Development for Quebec Regions	2	0	0	0	0	0	0	2

* Note complaints are listed under the name of the department at the time the complaint was made.

ACCESS AND PRIVACY COMPLAINTS CLOSED BY INSTITUTION AND FINDING (cont.)

Respondent	Discontinued	Early Resolution	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Well-founded - Resolved	Total
Canadian Nuclear Safety Commission	0	1	0	1	0	0	0	2
Canada Firearms Centre	0	1	1	0	0	0	0	2
Natural Resources Canada	1	0	1	0	0	0	0	2
Veterans Affairs Canada	1	0	1	0	0	0	0	2
Atlantic Canada Opportunities Agency	0	0	0	0	1	0	0	1
Canadian Heritage	0	0	1	0	0	0	0	1
Canadian Human Rights Commission	0	0	0	0	0	1	0	1
Canadian Radio-Television and Telecommunications Commission	0	1	0	0	0	0	0	1
Commission for Public Complaints against the RCMP	0	0	1	0	0	0	0	1
Correctional Investigator	0	0	1	0	0	0	0	1
National Gallery of Canada	0	0	0	0	0	0	1	1
National Parole Board	0	0	1	0	0	0	0	1
National Research Council Canada	1	0	0	0	0	0	0	1
Office of the Commissioner of Review Tribunals	1	0	0	0	0	0	0	1
Public Safety and Emergency Preparedness Canada	0	0	1	0	0	0	0	1
Public Service Human Resources Management Agency of Canada	0	0	0	0	0	0	1	1
Transport Canada	1	0	0	0	0	0	0	1
Total	78	36	191	13	58	25	46	447

* Note complaints are listed under the name of the department at the time the complaint was made.

COMPLAINT INVESTIGATIONS TREATMENT TIMES - *PRIVACY ACT*

The following tables show the average number of months to complete a complaint investigation, from the date the complaint is received to when a finding is made. The first table provides a breakdown by finding, the second by complaint type.

By Finding

For the period between April 1, 2006 and March 31, 2007

Disposition	Average Treatment Time in Months
Resolved	22.77
Well-Founded Resolved	21.53
Settled in the Course of Investigation	19.38
Not Well-Founded	17.20
Discontinued	14.33
Well-Founded	8.71
Early Resolution	4.13
Overall Average	13.39

Complaint treatment times continue to be a concern. The average time it takes from the day a complaint is filed to the day we make our findings has increased from ten and a half months in 2005-2006 to over 13 months in 2006-2007. This was anticipated and can be attributed to the loss of experienced personnel and a case backlog. It should also be noted that many complaint files now involve voluminous records, which take considerably more time to review and investigate. A number of complaints in multimedia formats such as CDs, video and audio tapes, have also been reviewed – a time-consuming process.

By Complaint Type

For the period between April 1, 2006 and March 31, 2007

Complaint Type	Average Treatment Time in Months
Access	19.32
Collection	17.69
Use and Disclosure	15.84
Language	15.00 **
Retention and Disposal	15.00 *
Extension Notice	11.75
Correction/Notation	10.00
Time Limits	9.73
Correction/Notation Time Limits	7.63 *
Overall Average	13.40

* The treatment time for this complaint type reflects eight cases.

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

INQUIRIES STATISTICS

Inquiries received and closed by the Inquiries unit For the period between April 1, 2006 and March 31, 2007

The OPC deals with a high volume of inquiries from the public. Frequently raised topics include identity theft, telemarketing, the no-fly list, the gun registry, and the misuse of Social Insurance Numbers.

	Privacy Act Inquiries Received	General Inquiries Received*	Total Inquiries Received
Telephone inquiries	2,399	3,301	5,700
Written inquiries (letter, e-mail, fax)	1,430	256	1,686
Total inquiries received	3,829	3,557	7,386

	Privacy Act Inquiries Closed	General Inquiries Closed*	Total Inquiries Closed
Telephone inquiries	2,399	3,301	5,700
Written inquiries (letter, e-mail, fax)	1,001	256	1,257
Total inquiries received	3,400	3,557	6,957

* These are privacy-related inquiries which cannot be linked to either the *Privacy Act* or the *Personal Information Protection and Electronic Documents Act (PIPEDA)*.