



Office of the
Privacy Commissioner
of Canada

Privacy

ANNUAL REPORT TO PARLIAMENT

2007-2008

Report on the *Privacy Act*



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

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

© Minister of Public Works and Government Services Canada 2008
Cat. No. IP50-2008
ISBN 978-0-662-05790-1

This publication is also available on our website 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
Téloc. : (613) 947-6850
1-800-282-1376
www.privcom.gc.ca



December 2008

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, 2007 to March 31, 2008.

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



December 2008

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

Dear Mr. Speaker:

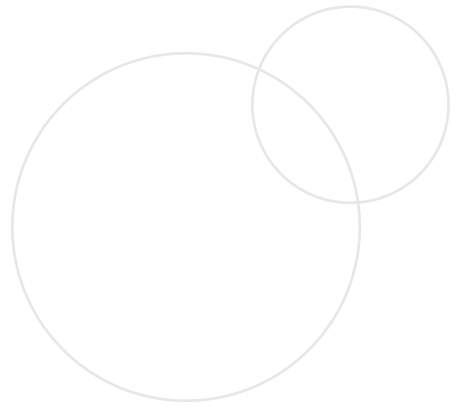
I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Privacy Act* for the period from April 1, 2007 to March 31, 2008.

Sincerely,

Original signed by

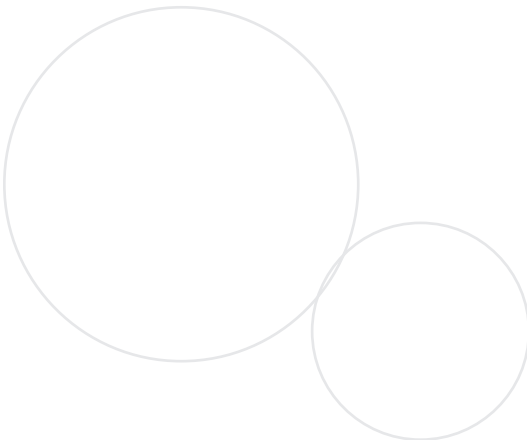
Jennifer Stoddart
Privacy Commissioner of Canada

TABLE OF CONTENTS



Message from the Commissioner	1
Key Accomplishments in 2007-2008	9
Privacy by the Numbers	13
Passport Canada Audit: <i>Significant Risk for Privacy</i>	15
Administrative and Quasi-judicial Bodies:	
<i>Balancing Openness and Privacy in the Internet Age</i>	23
Privacy Training in the Federal Public Service:	
<i>The Need for a Comprehensive Approach</i>	33
Update on <i>Privacy Act</i> Reform: <i>First Steps Toward a Legislative Overhaul</i>	41
Proactively Supporting Parliament	51
Law Enforcement and National Security Initiatives	51
Other Legislation and Initiatives with an Impact on Privacy	57
Responding to Complaints and Privacy Incidents	59
Other OPC Activities	77
Audit and Review	77
In the Courts.....	84
Access to Information and Privacy Unit	86
International Conference.....	87
The Year Ahead	89

Appendix 1	91
Definitions of Complaint Types	91
Definitions of Findings and other Dispositions under the <i>Privacy Act</i>	92
Appendix 2	94
Investigation Process under the <i>Privacy Act</i>	94
Appendix 3	96
<i>Privacy Act</i> Inquiry and Investigation Statistics	96
Inquiries Statistics	96
Complaints Received by Type	97
Top 10 Institutions by Complaints Received	97
Complaints Received by Institution	98
Complaints Received by Province/Territory	99
Closed Complaints by Finding	100
Findings by Complaint Type	100
Complaints (All Types) Closed	100
Access and Privacy Complaints Closed	101
Time Limits Complaints Closed	101
Time Limits Closed by Institution and Finding	102
Access and Privacy Complaints Closed by Institution and Finding	103
Complaint Investigations Treatment Times	105
By Finding	105
By Complaint Type	105







MESSAGE FROM THE COMMISSIONER

The doors of the Office of the Privacy Commissioner of Canada opened for business 25 years ago.

Canada's first Privacy Commissioner, John Grace, summarized the deep significance of his new mandate to protect the privacy of Canadians in his first annual report:

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

The source for a concern with privacy is an innate respect for personhood. Privacy is the ultimate minority protection. That is why the claim of privacy is so much more than a cry to be left alone or a fashionable obsession.

A quarter-century later, those eloquent words remain as true as ever. Privacy continues to be a deeply held value. However, it is also an increasingly fragile value.

Even that first annual report observed “it has become trite to say that personal privacy is threatened as never before in human history.... The confluence of new technologies with ever-insistent claims of the state to know, to be efficient, or both, has changed the quantitative and qualitative nature of the problem.”

Since then, the power of computers has multiplied many times over.

So too have governments' appetites for personal information about their citizens. In Canada and elsewhere, the rationale of safety and national security has been used to justify a dramatic expansion in the amount of personal information governments collect, analyze and share about us.

The potent combination of state interest in personal information and technological advances making it possible to gather and exploit this data on a massive scale is a theme highlighted – once again – in this 2007-2008 annual report on Canada’s public sector privacy law. (Our work related to private sector organizations is described in our annual reports on the *Personal Information Protection and Electronic Documents Act*, or PIPEDA.)

New Threats to a Fragile Value

This year, for example, our Office, along with our provincial and territorial counterparts, sounded the alarm about Canada’s Passenger Protect program – also known as the no-fly list – and the secretive use of personal information to determine who may and may not board aircrafts. The program raises profound concerns about privacy and other rights, such as mobility, access to information and due process – yet we have seen no evidence demonstrating the effectiveness of no-fly lists.

We also pointed out potential privacy and security risks related to the development of enhanced driver’s licences as an alternative to the Canadian passport.

Our Office, along with our counterparts in every other provincial and territorial office responsible for privacy protection, have concerns about the personal information of participating drivers leaving Canada and the potential that RFID chips in the licences could permit surreptitious location tracking. We also have concerns about our inability, in practice, to oversee how U.S. authorities receive and use this information.

Both the no-fly list and enhanced driver’s licences are well-intentioned initiatives – one is aimed at preventing terrorist incidents on planes; the other at providing Canadians with an alternative form of identification for crossing the Canada-U.S. border.

We are *not* arguing that the government has any malicious or intrusive intentions, even as it develops programs that result in increased surveillance of Canadians.

However, there needs to be a greater acknowledgement of the fact that our privacy rights are fragile in the face of government. They falter each time we trade away the personal and private for promises of more safety, greater efficiency or faster service.

There must also be a wider recognition of the reality that with each well-intentioned promise comes an increased erosion of privacy, risk of data security, diminished intellectual freedom and less personal autonomy.

The Orwellian dystopia was predicated on a totalitarian society. In our democracy, benevolent intentions appear to be pushing us toward a surveillance society.

Building Respect for Privacy Rights

Privacy, like any other freedom, is not an absolute right. It is conditional, limited by other rights we have recognized in our laws. And it is contextual – other laws may override it. There may be some cases where privacy protections must give way to protect a greater good, be it public health, consumer safety or national security.

However, we should *only* be asked to make this sacrifice when it is clear that the promised outcome – such as safer air travel – will actually be achieved *and* that there is no other less privacy-invasive option that would allow us to reach the goal.

The state must consider: Is there really a need that clearly outweighs the loss of privacy? Is the proposed measure likely to be effective in achieving the intended purpose? Is the intrusion on privacy proportional to the benefit to be gained? Is there some other less privacy-invasive way to achieve the same goal?

Unfortunately, recent federal initiatives are not always meeting this privacy test.

Technological advancements continue with no sign that governments recognize that amassing and analyzing mountains of personal data – virtually all of it from perfectly ordinary people – may not be the most effective way to protect us.

The threats to privacy have grown dramatically since the Office of the Privacy Commissioner opened its doors – with ever-growing databases, network computing, consumer profiling, and national security concerns. The list of issues has been daunting.

I can only imagine the challenges that a Privacy Commissioner will face a mere 15 years into the future with ubiquitous computing, handheld devices, nanotechnologies and more powerful surveillance techniques.

Despite challenges, our efforts to protect privacy in the public sector are not as effective as they could be given that the privacy law governing federal government programs is desperately outdated.



I can only imagine the challenges that a Privacy Commissioner will face a mere 15 years into the future with ubiquitous computing, handheld devices, nanotechnologies and more powerful surveillance techniques.

Privacy Act Reform

The *Privacy Act* needs to be overhauled.

Our hopes for better privacy protection for Canadians were revived in the spring of 2008, when the House of Commons Standing Committee on Access to Information, Privacy and Ethics announced a review of the *Privacy Act*.

Following this, our strategy was to provide the Committee with proposals that have a realistic chance of being adopted relatively soon. We put forward ten “quick fixes” – simple, straightforward suggestions for improving the legislation. Experts from across Canada, including members of our External Advisory Committee, testified in support of the needed reform.

The changes would go some way to improving privacy protections, but in no way eliminate the need for a highly detailed review and complete overhaul.

We look forward to seeing the Committee’s recommendations. Hopefully there will be some good news to report on legislative reforms in our next annual report.

Privacy Red Flags

The importance of strong protections for personal information held by governments – and the potential risk to citizens if such safeguards are not in place – was vividly demonstrated with a huge data breach in the United Kingdom in late 2007.

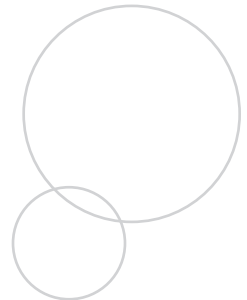
An administrative error – sending two unencrypted computer disks through an internal government mail system – compromised the personal information of 25 million people.

Strong privacy legislation can help prevent these sorts of simple but catastrophic mistakes, which leave people at serious risk for identity theft or other harms.

In this annual report, we focus on similarly dramatic shortcomings in how some federal institutions here in Canada are handling the personal information of the citizens they were established to serve.

Audits conducted by our Office uncovered serious problems with the privacy practices of three organizations that hold a great deal of highly sensitive personal information – the

Strong privacy legislation can help prevent these sorts of simple but catastrophic mistakes, which leave people at serious risk for identity theft or other harms.



Royal Canadian Mounted Police (RCMP), Passport Canada, and the Department of Foreign Affairs and International Trade (DFAIT).

RCMP Audit

The privacy issues we discovered while conducting an audit of the RCMP's exempt data banks – designed to prevent public access to the most sensitive national security and criminal intelligence files – were significant enough to prompt us to use our powers to table a special report to Parliament for the first time in the history of my Office.

The audit found that tens of thousands of files sheltered in RCMP exempt data banks should not have been there – raising questions about government transparency and accountability. Canadians should be able to see their personal information unless the disclosure could threaten national security, international affairs or lawful investigations.

The repercussions of such poor information management are potentially grave. People named in an exempt bank file could face serious harms.

Passport Audit

With this annual report, we are releasing the findings of an audit which identified serious flaws in privacy practices and procedures related to Canada's passport operations.

The audit uncovered a worrying series of problems in the way in which personal information is handled by Passport Canada and DFAIT. These problems may put at risk the privacy of Canadians applying for passports.

Training for Public Servants

One of the issues identified in our passport audit was the fact that some of the employees handling applications did not have a clear understanding of their obligation to protect privacy.

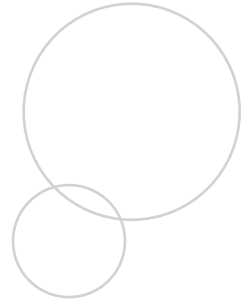
Training is essential to ensure all public servants understand their important responsibilities under both the *Privacy Act* and related Treasury Board Secretariat guidelines. Privacy training must be a requirement for public servants who handle significant amounts of personal information.

International Efforts

Our Office is also – by necessity – looking beyond Canada’s borders to develop privacy solutions for Canadians.

Transborder data flows and the Internet have transformed privacy into a global issue. Given the speed at which our personal data zips around the globe, assuring Canadians’ privacy requires strong international approaches to data protection.

Given the speed at which our personal data zips around the globe, assuring Canadians’ privacy requires strong international approaches to data protection.



Privacy protection can no longer be done on a country by country basis. The only way to succeed is by working collectively on privacy and security issues.

Canada is well-positioned to contribute to this effort. Over the years, we’ve developed a flexible, collaborative approach to data protection in the global context. Traditional close ties to the United States and membership in both the Asia Pacific Economic Cooperation (APEC) and the Organisation for Economic Cooperation and Development (OECD) place Canada in an excellent strategic position to help facilitate cooperation between countries.

I’ve been honoured to be able to work with the OECD Working Party on Information Security and Privacy. This group’s work is key to ensuring that global flows of information are adequately protected. The OECD Recommendation on Cross-border Privacy Co-operation adopted last year was a positive step, but we still have a ways to go.

We have also participated in the work of APEC, which is now implementing the APEC Privacy Framework.

In September, we hosted privacy advocates and experts from around the world at the 29th International Conference of Data Protection and Privacy Commissioners in Montreal, following a 2002 commitment. This conference was an important opportunity to discuss global privacy concerns and solutions. Commissioners resolved to increase cooperation and to help develop universally accepted international privacy standards in the area of information technology.

We will continue our work to encourage the development of global standards which will benefit people around the world.

Farewell to an Assistant Commissioner

Finally, on a more personal note, my Office is bidding *au revoir* to Raymond D'Aoust, Assistant Privacy Commissioner responsible for the *Privacy Act*.

Raymond arrived at the OPC at a very challenging time in the Office's history. A Commissioner and a handful of senior officials had just resigned amid a very public scandal.

Raymond brought the ideal personal attributes to help rebuild morale and resolve an organizational crisis – kindness, sensitivity and a passion for people. He encouraged a balanced approach to work and life – even introducing lunchtime yoga in the office boardroom.

A long career of committed public service provided Raymond with extensive experience in areas such as program evaluation, review, public consultation, strategic planning, business planning and quality management. He used all of this knowledge to make a major contribution to institutional renewal at the OPC.

Gifted with remarkable analytical skills, Raymond was consistently brilliant at identifying all the components of a given situation so he could assess it fairly and properly. A man of principle and a consummate professional, his tireless efforts and effective, firm diplomacy were instrumental to his many successes.

Raymond also brought with him a deep commitment to protecting privacy rights. His efforts have been driven by a strong notion of what the work of this Office means for individual Canadians. He was front and centre on a number of key files, including the protection of DNA, electronic health records, enhanced driver's licences and the no-fly list – to name but a few. I must also congratulate him for his stalwart endeavours to push *Privacy Act* reforms forward. He successfully conducted a number of governmental policy studies and helped found the Association of Francophone Data Protection Authorities.

The Office of the Privacy Commissioner has greatly benefited from his work and we are pleased that he will continue to work with us as Special Advisor to the Commissioners until his retirement.

Un très grand merci Raymond.

A Strong Team

I would also like to thank the rest of the wonderful team in my Office for their dedicated service over 2007-2008. As this annual report illustrates, the issues we work on each day are varied, complex and challenging. We've been lucky enough to attract an exceptionally talented new generation of privacy protection experts to our ranks over the past year.

I offer a special word of thanks to everyone working so hard on our initiatives related to *Privacy Act* reform, international data protection and investigation re-engineering – all of which are critical to ensuring our Office will be a strong, effective guardian of Canadians' privacy rights well into the future.

Jennifer Stoddart
Privacy Commissioner of Canada



KEY ACCOMPLISHMENTS IN 2007-2008

Our Office serves three key client groups – Parliament, federal government departments and agencies, and individual Canadians – under the *Privacy Act*.

Some of our key accomplishments in 2007-2008 include:

Proactively Supporting Parliament

- Tabled the Privacy Commissioner's first special report to Parliament, which outlined the findings of an audit of the RCMP's exempt data banks
- Prepared a submission and appeared before the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182
- Appeared six times before parliamentary committees on such issues as identity theft and the *Canada Elections Act*
- Worked with the Standing Committee on Access to Information, Privacy and Ethics on the statutory review of PIPEDA; responded to Industry Canada's consultation on PIPEDA review
- Joined provincial and territorial privacy oversight officials in passing joint resolutions on the privacy risks associated with enhanced driver's licences, as well as the need for comprehensive changes to the no-fly list program

Serving Canadians

- Responded to 4,258 *Privacy Act*-related inquiries and 2,367 general inquiries
- Investigated hundreds of privacy complaints in the public and private sectors
- Created a blog to help stimulate a discussion with Canadians on privacy issues

- Began work on a social marketing campaign aimed at encouraging awareness and prompting action on children's privacy online
- Participated in court cases in order to help develop privacy-conscious jurisprudence in Canada

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
- Reviewed 93 Privacy Impact Assessments

International Highlights

- Hosted the 29th International Conference of Data Protection and Privacy Commissioners, honouring a 2002 commitment
- Joined other international data protection authorities in passing resolutions on the need for global standards for safeguarding passenger data; greater international cooperation on privacy issues; and active involvement in the development of universally accepted international privacy standards in the area of information technology
- Chaired an OECD group working to enhance cooperation between data protection authorities and other privacy rights enforcement agencies around the world; the OECD adopted a recommendation on cross-border cooperation based on the volunteer group's work
- Contributed to an APEC data privacy group's efforts to implement a new privacy framework for APEC members
- Worked with the Standards Council of Canada on the development of international privacy standards
- Joined the International Standards Organization (ISO) and became a member of an important ISO Working Group tasked with developing and maintaining standards and guidelines addressing security aspects of identity management, biometrics and the protection of personal data
- Participated in the International Working Group on Data Protection in Telecommunications, which has recently focused on Internet privacy

- Played a lead role in the creation of an international association of data protection authorities and other enforcement agencies from francophone states
- Became a member of the Asia Pacific Privacy Authorities Forum

Encouraging Research and Debate

- Commissioned 22 research projects related to emerging privacy issues
- Issued a consultation paper seeking feedback on the implications of using RFID technology in the workplace
- Published a discussion paper on the role of identity in society and the privacy issues related to identity

PRIVACY BY THE NUMBERS IN 2007-2008



Average number of <i>Privacy Act</i> inquiries per month:	354
Average number of new <i>Privacy Act</i> complaints received per month:	63
Average number of investigations closed per month:	73
Total investigations closed during the year:	880
Privacy Impact Assessments reviewed:	78
Privacy Impact Assessments closed:	93
Parliamentary appearances:	6
Bills/acts reviewed for privacy implications:	19
Research papers issued:	16
Public events organized:	7
Formal visits by external privacy stakeholders:	39
Research activities commissioned:	22
Speeches and presentations delivered:	86
Media requests:	417
Interviews provided:	268
News releases issued:	37
Average hits to our website per month:	128,091
Average hits to our blog per month (September 2007 to March 2008):	17,345
Litigation decisions under <i>Privacy Act</i> :	1

CANADA



PASSPORT
PASSEPORT

PASSPORT CANADA AUDIT: *SIGNIFICANT RISK FOR PRIVACY*



Lack of adequate safeguards leaves the personal information of passport applicants vulnerable to misuse

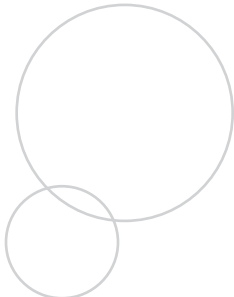
Privacy and security problems in Canada's passport operations add up to a significant risk for Canadians applying for passports, an OPC audit has found.

The audit at Passport Canada and the Department of Foreign Affairs and International Trade (DFAIT) unfortunately found weaknesses in every step of the application process; the way in which personal information is collected and stored; how it can be accessed; and how it is ultimately disposed.

For example, passport applications and supporting documents were kept in clear plastic bags on open shelves; documents containing personal information were sometimes tossed into regular garbage and recycling bins without being shredded – and some documents that had been shredded by a private contractor could easily be put back together. Meanwhile, computer systems allowed too many employees to access certain passport files and controls, such as audit logs and encryption, were missing.

These privacy and security shortfalls are particularly worrying given the high sensitivity of the personal information involved in processing passport applications. There is a risk that this information could be used for nefarious purposes if it wound up in the wrong hands.

We are pleased that Passport Canada and DFAIT have indicated they will take action on our recommendations.



These privacy and security shortfalls are particularly worrying given the high sensitivity of the personal information involved in processing passport applications.

Background

Passport Canada processed more than 3.6 million passport applications in 2006–2007. It currently has more than 30 million passport records under its control. The information people provide on their application forms, supporting documentation, as well as passports include highly sensitive personal information.

Passport Canada is an agency of DFAIT, which has a mandate to issue passports. It also provides guidance to DFAIT missions issuing passports abroad.

Missions issued approximately 136,000 passports in the 2006–2007 fiscal year. While that represents only 3.5 per cent of the total number issued, DFAIT has acknowledged that the delivery of passport services abroad is “exposed to a high degree of inherent risk.”

There is a risk of consequences – identity theft, for example – to individual passport holders if their personal information goes missing or is stolen. It’s clear that stronger safeguards are required to protect this data.

Unfortunately, while the passport agency has adopted some good privacy and security features, the audit identified shortcomings. There are a number of opportunities to strengthen the privacy management framework and practices for the passport program.

Privacy Management Framework

Passport Canada does not have a Chief Privacy Officer. In fact, DFAIT has not delegated full authority to Passport Canada for privacy matters. As a result, key privacy responsibilities for the passport program are dispersed and, in our opinion, have not been given sufficient attention.

While the appointment of a Chief Privacy Officer is not a legislated requirement, it is increasingly becoming a practice among federal departments and agencies with significant personal information holdings.

The appointment of a Chief Privacy Officer helps ensure that privacy issues have a champion at the corporate decision-making table. It also ensures accountability for an organization’s privacy management practices.

Collection Issues

Our Office's list of other concerns begins with the passport application itself. Passport Canada concentrates a large amount of sensitive personal information on one application form. Credit card information is collected along with other identifying information, such as names, addresses, phone numbers, birthdates and sometimes Social Insurance Numbers.

Financial information and other personal information – particularly a Social Insurance Number – are key information ingredients sought by identity thieves.

Because an applicant's credit card information is combined with other application form information (both physically and electronically), virtually any employee involved in the passport process can access credit card numbers – even if they don't need this information to process the application.

Too Much Access

Too many DFAIT employees are able to see completed passport documents and the personal information they contain.

Access to personal information on passport applications is not adequately controlled to ensure that only employees who require this information can see it.

For example, consular officials at missions around the world – including locally hired staff – had computer access to passport files processed by any other mission abroad even though the need to access this information was infrequent and the information could be provided by other means on a need to know basis. As a further example, mission staff in one city can access completed passport records from other cities – and vice versa.

Our audit found a case where a former mission employee still had access to the passport management system even though she had left that employment six months earlier. One employee responsible for protocol and official visits had full access rights to the system – though it had nothing to do with his job. Other employees were included on the access list, although they no longer had access to passport records.

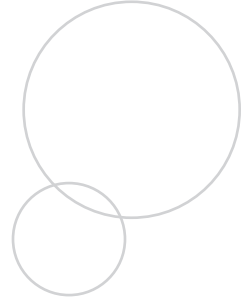
Passport Canada has been raising the security level it requires for employees handling passports to the "Secret" level. However, many consular employees, including most locally hired staff, still only have a basic "reliability" security level. In many countries around the world, difficulties in obtaining criminal and intelligence records pose a challenge for raising the security level of locally hired, non-Canadian staff.

DFAIT could mitigate the inherent risk associated with locally hired staff by using better access controls and also keeping track of who is accessing passport files.

We were surprised to find that IT systems for completed passport application files at both Passport Canada and DFAIT lacked a computer safeguard to track who had viewed these records.

The lack of such an audit trail flags a privacy risk in Canada's passport system that – if left unchecked – could lead to undetected security risks and data breaches.

The lack of such an audit trail flags a privacy risk in Canada's passport system that – if left unchecked – could lead to undetected security risks and data breaches.



Security Shortfalls

In some passport offices and missions abroad, passport records and supporting documents were stored in clear plastic bags and left on open shelves on their premises.

Use of portable memory devices, and the lack of encryption for stored personal information, and the transmission of e-mails with passport information outside DFAIT and Passport Canada, all pose a further risk to the protection of personal information.

Neither Passport Canada nor DFAIT has an organization-wide policy restricting employees' use of portable memory devices such as memory sticks and cell phones at work. Such devices are small, easy to use and hold large quantities of data. Anyone with access to passport information systems could photograph or download and copy personal information onto a portable device without being detected.

While our audit was not designed to detect privacy breaches, and none came to our attention during the audit (other than a breach of the Passport On-Line system), it is clear that a great deal of trust is placed in the employees who process passport applications, including locally employed staff. While we recognize the need for trust is inherent in the process, enhanced controls support trust and mitigate risk.

We also found that Passport Canada archives electronic passport records for up to 100 years – even though the reasons for keeping this personal information for such a long period of time are unclear.

The risk that this personal information will be compromised is heightened by the fact that personal information stored on both Passport Canada's main database and DFAIT's passport system is not encrypted. Another information technology concern is that e-mails containing personal information sent outside of secure internal networks may not be protected by encryption and are, therefore, vulnerable to interception and improper use by hackers. Many employees we interviewed were unaware that such e-mails may not be protected.

Our Office also has a number of concerns about the way in which Passport Canada is disposing paper and electronic passport records.

A number of Passport Canada offices and Canadian missions abroad disposed of passport administration forms containing personal information, such as names and dates of birth, in ordinary garbage and recycling bins.

At one private-sector shredding facility under contract with Service Canada, we found that – even after the documents had apparently been shredded – entire passport photos remained intact and documents could be pieced together with little effort.

Finally, the design of consular areas in some missions does not offer adequate privacy for clients. Applicants' sensitive conversations with consular officials can be overheard by other people in public waiting areas.

Online Risks

While our audit was underway, the OPC learned through the media about a breach of Passport Canada's online passport system. An Ontario man using the system had discovered he could access other applicants' sensitive passport information by randomly changing one number in the Uniform Resource Locator, or URL, which appears at the top of each page on every Internet site.

Passport Canada shut down the system and corrected the programming problem.

The agency told us that the incident was the only breach of this type it was aware of. Given that the man who had seen other people's personal information had immediately reported the breach to Passport Canada, the risk to Canadian's passport information was considered minimal by the agency. Passport Canada is investigating further and we are awaiting a full report.

Passport Canada has plans to replace the online system within a year with a new method to encrypt and protect personal data.

Recommendations and Next Steps

Our Office provided Passport Canada and Foreign Affairs with 15 recommendations to strengthen the privacy management framework for passport operations.

These include:

- Hiring a Chief Privacy Officer at Passport Canada
- Providing ongoing privacy and security training programs to staff
- Introducing better controls on access to passport information
- Reassessing the current 100-year retention period for passport information
- Providing essential safeguards, including: more restricted access to areas where passports are processed; privacy for clients discussing passport applications; re-evaluating adequacy of security screening for employees; policies on portable memory and recording devices, such as cell phones; and expanded use of encryption

Further to our audit report, both Passport Canada and DFAIT have agreed with most of our recommendations.

We will follow up with Passport Canada and DFAIT on our recommendations with a post-audit.

We would like to thank Passport Canada and DFAIT employees for their professionalism, cooperation and responsiveness during our audit.

The full audit report, including management responses, is available on the OPC website.





ADMINISTRATIVE AND QUASI-JUDICIAL BODIES: *BALANCING OPENNESS AND PRIVACY IN THE INTERNET AGE*

Complaints to the OPC highlight concerns about federal administrative and quasi-judicial tribunals posting highly sensitive personal information to the web

Highly personal information about Canadians fighting for government benefits and taking part in other federal administrative and quasi-judicial proceedings is being posted to the Internet – exposing those people to enormous privacy risks.

In 2007–2008, the OPC investigated 23 complaints regarding the disclosure of personal information on the Internet by seven bodies created by Parliament to adjudicate disputes. (We received three more similar complaints in May 2008.)

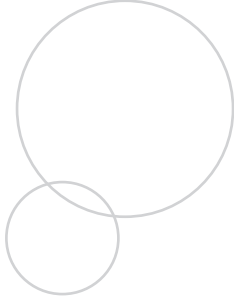
These administrative and quasi-judicial bodies consider issues such as the denial of pension and employment insurance benefits; compliance with employment and other professional standards; allegations of regulatory violations; and irregularities in federal public service hiring processes.

The adjudication process often involves very intimate details related to people's lives, including their financial status, health, job performance and personal history.

Few would question the fundamental importance of transparency in tribunal proceedings.

But is it in the public interest to make considerable amounts of an individual's sensitive personal information indiscriminately available to anyone with an Internet connection?

Why should a law-abiding citizen fighting for a government benefit be forced to expose the intimate details of her personal life to public scrutiny?



Why should a law-abiding citizen fighting for a government benefit be forced to expose the intimate details of her personal life to public scrutiny?

The Human Impact

The decisions of administrative and quasi-judicial decision-makers are routinely packed with personal details that not many people would be comfortable sharing widely: salaries, physical and mental health problems as well as detailed descriptions of disputes with bosses and alleged wrongdoing in the workplace.

In addition to the types of personal information legitimately needed in these bodies' reasons for decision, seemingly irrelevant information is often included – the names of participants' children; home addresses; people's place and date of birth; and descriptions of criminal convictions for which a pardon has been granted, for example.

Many complainants told us they were distressed to discover – typically with no prior notice – that this type of information about them was available on the Internet for neighbours, colleagues and prospective employees to peruse.

The following are some of the comments we heard:

“By posting my name, I feel violated in my privacy and this could adversely affect my prospects for jobs, business and my image in the community. I have never given consent.”

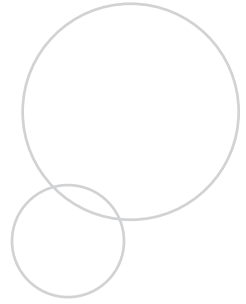
“Anybody, anywhere in the whole world, who types my name comes immediately to this personal information.... this situation leaves me open to criticism and mockery.”

“I’m at a loss to understand why this would have been done, except to think that this is further punitive measures taken against me.”

The potential for embarrassment, humiliation and public ridicule is significant. A long-ago legal transgression or temporary lapse in judgment could continue to haunt an individual for many, many years into the future.

Individuals whose personal information, particularly financial information, is disclosed on the Internet may be at greater risk of identity theft. They also face a risk of discrimination, harassment and stalking. The information could also be used by data brokers that compile profiles of individuals.

“Anybody, anywhere in the whole world, who types my name comes immediately to this personal information.... this situation leaves me open to criticism and mockery.”



A list of the bodies whose practice of posting personal information online have resulted in complaints investigated by the OPC in 2007-2008:

Canada Appeals Office on Occupational Health and Safety

The Canada Appeals Office on Occupational Health and Safety (CAO), now known as the Occupational Health and Safety Tribunal Canada, is a quasi-judicial administrative tribunal that determines appeals of decisions and directions issued by health and safety officers. It operates under the auspices of Human Resources Development Canada. Decisions rendered by this tribunal may include an individual's name, coupled with that person's personal opinions or views and place of employment.

Military Police Complaints Commission

The Military Police Complaints Commission is an independent federal body that oversees and reviews complaints about the conduct of Military Police members. The Commission is empowered to: review the Provost Marshal's handling of complaints concerning the conduct of Military Police; deal with complaints alleging interference in military police investigations; and conduct its own investigations or hearings related to complaints when the Commission believes that doing so is in the public interest.

All of the Military Police Complaints Commission decisions are vetted by the Commission with a view to the standards expressed in the *Privacy Act*. Most decisions rendered by the Military Police Complaints Commission are published on the Internet in summary and depersonalized form. Where decisions are not depersonalized, they may contain extensive personal information about military police members.

Pension Appeals Board

The Pensions Appeal Board is responsible for hearing appeals flowing from decisions of the Canada Pension Plan Review Tribunals. A hearing before the board may be initiated by an individual seeking Canada Pension Plan (CPP) benefits or by the Minister of Social Development. The board has the authority to determine, among other things, whether benefits under the CPP are payable to an individual.

Board decisions reveal a considerable amount of sensitive personal information about individuals seeking benefits, including dates of birth, detailed family, education and employment histories, extensive personal health information and personal financial data.

Public Service Commission

The Public Service Commission is a quasi-judicial tribunal that may conduct investigations and audits on any matter within its jurisdiction, including safeguarding the integrity of appointments and in overseeing the political impartiality of the federal public service. Its decisions may include information relating to individuals' education or medical or employment history.

Public Service Staff Relations Board

The board, which has been replaced by the Public Service Labour Relations Board, was a federal tribunal responsible for administering the collective bargaining and grievance adjudication systems in the federal public service.

Decisions may include descriptions of individuals' conduct and issues at work as well as disciplinary sanctions they've faced.

RCMP Adjudication Board

An RCMP Adjudication Board conducts formal disciplinary hearings respecting RCMP members' compliance with the Code of Conduct adopted under the *Royal Canadian Mounted Police Act*. Decisions include information about alleged misconduct, and, in some cases, other personal information such as an officer's marital situation and medical information. Adjudication Board decisions, which include the names of individuals, are published on the RCMP intranet, although the Board has advised that it intends to post its decisions on the Internet.

Umpire Benefits Decisions (Service Canada)

The *Employment Insurance Act* permits claimants and other interested parties to appeal to an umpire certain decisions rendered under that Act. An umpire is empowered to decide any question of fact or law that is necessary for the disposition of an appeal.

Decisions by an umpire tend to reveal detailed information about the employment history of claimants. A typical decision might also reveal information about a claimant's place of residence, marital status and sources of income.

Access to Justice

Another concern we have is that access to justice could suffer if tribunals, boards and other administrative decision makers continue to post decisions on the Internet.

The risk of having one's personal details made public may make people increasingly reticent to assert their rights in administrative and quasi-judicial proceedings. People trying to obtain benefits required to provide food and shelter for themselves and their families may feel that participation in tribunal proceedings is essentially mandatory – and that they have no option other than to give up their right to privacy.

In some cases, however, individuals have declined to exercise their legal right to appeal administrative decisions that significantly impacted them because of the loss of privacy this would entail.

“Open Court” Principle

The widespread practice of posting reasons for decisions on the Internet appears to be based on the assumption by decision makers that the rules – or lack of rules – which apply to judicial proceedings apply equally to administrative and quasi-judicial proceedings.

Many of the institutions investigated argued that the “open court” principle required the online publication of decisions.

The open court principle is an important part of our legal system and exists to ensure the effectiveness of the evidentiary process, encourage fair and transparent decision-making, promote the integrity of the justice system and inform the public about its operation. Opening decision-making processes up to public scrutiny assists to further these goals.

However, there is an important distinction between the courts and the institutions we investigated. The *Privacy Act*, which does not apply to the courts, applies to many administrative tribunals and quasi-judicial bodies and imposes specific rules on them regarding the disclosure of personal information. Through the *Privacy Act*, Parliament may be said to have set express limits on the extent to which the open court principle could authorize publication of decisions of the administrative tribunals subject to its provisions via the Internet.

Striking a Reasonable Balance

Respect for the open court principle can co-exist effectively with government institutions' statutory obligations under the *Privacy Act* through reasonable efforts to depersonalize any decisions posted online by replacing names with random initials.

It is beyond debate that the public requires access to the information necessary to maintain confidence in the integrity of a tribunal's proceedings, to enhance the evidentiary process, to promote accountability and to further public education. Yet in most cases, these important goals may be accomplished without disclosing the name of an individual appearing before a tribunal.

The identity of individuals appearing before tribunals is not obviously relevant to the merits of any given tribunal decision. As the open court principle is intended to subject *government institutions* to public scrutiny, and not the lives of the *individuals* who appear before them, the OPC has taken the position that the public interest in accessing information about tribunals' proceedings does not obviously or necessarily extend to accessing identifying information about individual participants.

Furthering the values that the open court principle promotes will not be hindered if, consistent with government institutions' obligations under the *Privacy Act*, only de-personalized decisions that do not reveal the identities of participants are made available to the public. It is, of course, also open to tribunals to redact all personal information that would otherwise be found in reasons for decision made available to the public. However, simple suppression of direct and obvious identifiers such as names is likely to represent the most efficient and effective means of complying with the *Privacy Act*. This method of protecting privacy poses no significant threat to tribunals' independence and ensures that the facts and issues in individual cases may be fully and transparently debated in an open and accessible manner.

Where there is a genuine and compelling public interest in disclosure of identifying information that clearly outweighs the resulting invasion of privacy, institutions have the legal authority to exercise their discretion to disclose personal information in identifiable form in their decisions. For example, where the public has a compelling interest in knowing the identity of an individual who has been found guilty in disciplinary proceedings, or of someone who poses a potential danger to the public, a tribunal may exercise its discretion to disclose personal information, including that individual's name, to the public.

Likewise, where Parliament or a body empowered to make regulations has drafted a law or regulation that authorizes the disclosure of personal information, the *Privacy Act* permits disclosure of personal information in accordance with such a provision. In this way, the Act recognizes the right of lawmakers to craft disclosure regimes that are responsive to particular tribunals' mandates and the associated demands of the open court principle.

There is, thus, no intractable conflict between the rights and interests protected by the open court principle and compliance with the *Privacy Act*.

It is also noteworthy that courts, too, are increasingly recognizing the need to limit the disclosure of personal information in judgments. The Canadian Judicial Council has published a Recommended Protocol for the use of personal information in judgements. This protocol recognizes it can be appropriate for judges to omit some personal information from a judgment in the interests of protecting privacy. Where appropriate, these guidelines encourage the judiciary to omit from judgments personal data identifiers, highly specific personal information and extraneous personal information with little or no relevance to the conclusions reached.

Privacy Act Limits

During our investigation, we found there is a significant lack of consensus among administrative and quasi-judicial decision-makers on the limits that the *Privacy Act* places on the Internet disclosure of personal information in their decisions.

The decisions of most, if not all, institutions subject to the *Privacy Act* contain personal information to which the protections of the legislation apply.

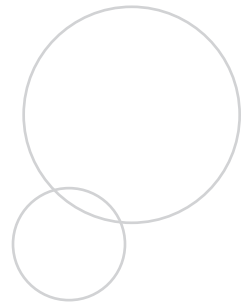
The *Privacy Act* says that personal information under the control of a government institution may be disclosed for the purpose for which it was obtained or compiled, or for a use consistent with that purpose.

The OPC concluded that the blanket electronic disclosure of these bodies' reasons for decision on the intranet or Internet is not the purpose for which the information was obtained. Rather, tribunals collect personal information for the purpose of making a decision on the facts of each specific case before them.

Moreover, disclosing administrative or quasi-judicial decisions with identifiable personal information on the Internet as a matter of course was not found to be reasonably necessary for the accomplishment of the investigated institutions' mandates. It was not a disclosure for a use that was consistent with the purpose for which the personal information was obtained – particularly when the uses to which sensitive personal information would be put could not be identified in advance or controlled in any way.

Under the *Privacy Act*, limits on the disclosure of personal information do not

... disclosing administrative or quasi-judicial decisions with identifiable personal information on the Internet as a matter of course was not found to be reasonably necessary for the accomplishment of the investigated institutions' mandates.



apply to publicly available information. Some of the institutions investigated argued that the publicly accessible nature of administrative and quasi-judicial proceedings rendered the personal information discussed during those proceedings publicly available for the purposes of the Act.

However, none of those institutions presented any evidence to indicate there was any record, in any form, of the personal information disclosed during the course of proceedings that is available in the public domain. Our Office found that disclosure of personal information during a proceeding did not in itself render that information available in the public domain.

The *Privacy Act* also allows for disclosure of personal information in accordance with any Act of Parliament or regulation authorizing such a disclosure.

Some institutions argued that the disclosure of personal information was permissible due to the fact that relevant legislation or regulations did not prohibit or address disclosure. We rejected this argument. There must be some specific indication in an Act or regulation that Parliament intended to permit disclosures of personal information outside of the quasi-constitutional regime created by the *Privacy Act*. Legislative silence on the issue does not constitute a legal authority to disclose personal information.

Recommendations

In the well-founded complaints we investigated, our Office made a number of recommendations to government institutions:

- Reasonably depersonalize future decisions that will be posted on the Internet through the use of randomly assigned initials in place of individuals' names; or post only a summary of the decision with no identifying personal information.
- Observe suggested guidelines respecting the exercise of discretion to disclose personal information in any case where an institution proposes to disclose personal information in decisions in electronic form on the Internet.
- Remove decisions that form the basis of the complaints to the OPC from the Internet on a priority basis until they can be reasonably depersonalized through the use of randomly assigned initials and re-posted in compliance with the *Privacy Act*.
- Restrict the indexing by name of past decisions by global search engines through the use of an appropriate "web robot exclusion protocol;" or remove from or reasonably depersonalize all past decisions on the Internet through the use of randomly assigned initials, within a reasonable amount of time.

Response to OPC Concerns

Even after being advised of privacy issues, most government institutions were reticent to change their policies and practices.

Notwithstanding the growing number and severity of privacy threats to individuals whose personal information is posted indiscriminately on the Internet, some government institutions told us they plan to continue posting sensitive personal information as they always have.

Others took important but incomplete steps towards improved compliance with the *Privacy Act*. As a result of our investigations, some institutions have implemented technical measures to prevent the names of individuals who participate in their decision-making processes from creating “search hits” when typed into major search engines. Others have agreed to use initials in place of individuals’ names.

Notably, Service Canada and Human Resources Development Canada agreed to fully implement our recommendations.

The OPC has relayed the results of its investigation to the complainants. In cases where these results were disappointing, the OPC remains committed to working with the bodies involved with a view to improving privacy protections for those who participate in administrative and quasi-judicial processes.

The varying degrees of responsiveness to the OPC’s recommendations means that, even among those institutions investigated, there remains inconsistent privacy protection for Canadians who participate in these institutions’ administrative and/or quasi-judicial proceedings.

It is also worth noting that many other administrative and quasi-judicial bodies post online reasons for decisions that link identifiable individuals with a great deal of sensitive personal information, but the OPC has not received complaints about them.

Next Steps

Under the *Privacy Act*, this is not a matter that we are empowered to bring before the courts for further guidance.

However, our Office is committed to continuing to work with the government institutions which have been reluctant to implement all of the recommendations. We hope that by maintaining a constructive dialogue, we will be able to persuade these organizations to take the steps necessary to protect Canadians’ privacy.

We also see a need for a new government-wide policy on this privacy issue. Given the complexity of the issues involved, recommendations flowing from our investigation of a small number of institutions are not the best instruments around which to build government-wide compliance with the *Privacy Act*. A comprehensive policy document based on consultations with a wider range of government institutions is required.

We have already conveyed to the Treasury Board Secretariat our view that centralized policy guidance is required. This guidance will ensure consistency in the privacy protection available to Canadians who participate in administrative and quasi-judicial proceedings.

Many institutions we investigated agreed with our view that centralized policy guidance is required and would welcome the same. They were willing to participate in consultations with Treasury Board to develop policy guidance and comply with this guidance when it took effect.

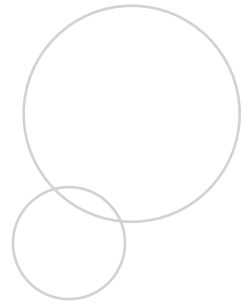
Treasury Board has advised our Office that its officials continue to work on developing guidance for federal institutions subject to the *Privacy Act* with respect to the posting of personal information on government websites. Treasury Board has also indicated that it will consult with our Office on any draft guidance that is developed.

Electronically publishing personal information contained in the administrative and quasi-judicial decisions of government institutions is risky privacy business. We look forward to working with Treasury Board on this important issue to ensure Canadians' privacy will be better protected by strong policy guidance in the future.

The trend to put more and more federal government information online raises important questions about how to balance the public interest and individual privacy rights.

While the use of the Internet to promote transparency and accountability in the federal government – posting contracts and travel expenses, for example – is a welcome development, it is clear there must be limits when it comes to the disclosure of personal information.

We hope that by maintaining a constructive dialogue, we will be able to persuade these organizations to take the steps necessary to protect Canadians' privacy.







PRIVACY TRAINING IN THE FEDERAL PUBLIC SERVICE: *THE NEED FOR A COMPREHENSIVE APPROACH*

Providing all employees who handle personal information with privacy training is one of the key ways in which governments can prevent data breaches

In late 2007, a relatively simple mistake by a British civil servant led to one of the biggest data breaches in history.

The incident compromised the personal information of 25 million people receiving a child benefit – and stands as a cautionary tale for governments around the world about the need to take data protection, including employee privacy training, extremely seriously.

An official in the U.K.'s Revenue and Customs Office had placed two computer disks containing details about families registered in a child benefit database into an envelope to be couriered to another government department.

The CDs did not arrive at their destination and have yet to be recovered.

The breach, which exposed families across Britain to the risk of identity theft, resulted in the resignation of the chairman of the Revenue and Customs Office and led to a major police investigation.

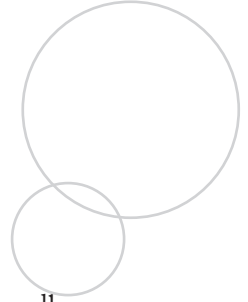
After its investigation, the British Independent Police Complaints Commission concluded that individual staff members were not to blame. Instead, it said “woefully inadequate” data handling practices and procedures, including a lack of training for staff, led to the breach.

“There was: a complete lack of any meaningful systems; a lack of understanding of the importance of data handling; and a ‘muddle through’ ethos,” the Commission said. “Staff found themselves working on a day-to-day basis without adequate support, training or guidance about how to handle sensitive personal data appropriately.”

Following the breach, the British government introduced mandatory annual training for all civil servants who deal with personal data.

Here in Canada, the OPC has for some time been urging the federal government to provide better training for public servants on the fundamental principles of personal information management. This privacy training should be mandatory for all managers and all public servants who handle personal information.

Privacy training should be mandatory for all managers and all public servants who handle personal information.



Unless adequate learning programs are put in place, a regrettable incident could lead to a breach of personal data held by a federal department or agency. Such a breach could affect thousands – if not millions – of Canadians.

Over the last few years, we have seen a number of significant breaches of personal information occurring all over the world, in both private and public sector organizations.

These breaches often take the form of the inadvertent or negligent loss of personal data by employees or the theft of equipment containing such data. In many of these cases, the breaches could have been avoided if employees handling the personal information had received training on the fundamental principles of secure and responsible information management.

Audit Concerns

Recent OPC audits underscored the need for comprehensive privacy training for employees who handle personal information in federal government departments and agencies.

In October 2007, our Office published the results of an audit assessing the effectiveness and outcome of Privacy Impact Assessments (PIAs) conducted by federal government departments and agencies for new or redesigned programs and services.

One of the audit's principal conclusions was that more training is needed to ensure that program managers understand their responsibilities under the Treasury Board Policy on Privacy Impact Assessments, and have the privacy knowledge and skills necessary to conduct effective PIAs.

While some government institutions have made a serious effort to apply the policy, the audit found more is required to ensure PIAs are having the desired effect – namely to establish and enshrine privacy protection as a core consideration in government program

and service delivery. The audit also discovered an uneven application of the policy, including a number of performance failures. Our auditors attributed these disappointing results to many causes, including a lack of training.

Another major audit, described in detail in our 2005-2006 annual report, examined the management practices of the Canada Border Services Agency (CBSA) with regards to trans-border data flows and found similar challenges with regards to training needs of key personnel.

Generally, the audit identified significant opportunities for the CBSA to better manage privacy risks and achieve greater accountability, transparency and control over the trans-border flow of personal information.

The audit called for providing regular and ongoing training sessions on the administration of, and compliance with, the *Privacy Act*. It recommended designing and implementing a privacy management framework for the CBSA, a component of which would be the creation of a committee of senior managers mandated with ensuring that privacy guidance and training are provided.

Finally, the audit recommended the development of specific training modules to combat problems with verbal exchanges of personal information between Canadian and U.S. border officials.

An audit of Canada's passport operations, detailed earlier in this report, also highlighted how a lack of adequate training can lead to privacy and security risks.

A Core Curriculum

Some federal government departments and agencies have recognized the need for better privacy training for employees. Statistics Canada and Citizenship and Immigration have introduced training regimes and formal instruction to raise awareness of privacy issues and legislation. The Treasury Board Secretariat has also been providing training for some years to the ATIP community. In addition, the Secretariat provides ongoing advice to individual institutions - both ATIP and program officials - on specific privacy-related issues.

Despite these success stories, on the whole we feel the federal government could be doing much more.

Part of the problem lies in the fact that there is no mandatory core curriculum for educating public servants who process or manage personal information about their basic duties and responsibilities under the *Privacy Act*.

Nor is there a mandatory core curriculum for training these employees on widely recognized privacy fair information principles, which govern the appropriate collection, use, disclosure, and disposal of personal information within government.

The Canada School of Public Service offers two training modules on privacy and access laws. However, these are not mandatory. (The two current courses will be merged into one new course beginning in early 2009.)

Many departments and agencies have designed their own training programs, but in most cases this training is insufficient.

The Public Service Commission of Canada (PSC), for example, runs information sessions to provide advice and training to its managers about the impact of the *Privacy Act* on various programs. The sessions are so popular that the PSC turned some of its managers away in 2007 for lack of resources to provide training. The PSC has since expanded the program in an attempt to meet the demand.

The Department of Foreign Affairs and International Trade has built a permanent policy, process, and training regimen to ensure that all access to information and privacy analysts receive the training they need to do their jobs. However, the department is of the view that there is a pressing need for more widespread training.

Clearly, some departments are willing to meet that need with proactive programs that formalize privacy training. What they need is additional training support to get the job done.

A Comprehensive Approach

The OPC is of the view that a coordinated and comprehensive strategy needs to be developed and implemented by key players in the federal government: the Canada School of Public Service (CSPS); Treasury Board Secretariat (TBS); and ATIP offices in every federal government department and agency.

The Role of the Canada School of Public Service

The Canada School of Public Service's key mandate is to ensure all public service employees have the knowledge and skills they need to develop policy and deliver services for Canadians.

We believe that the School should develop a core, mandatory privacy training curriculum to be used by all government departments and agencies in training employees who handle significant amounts of personal information. The target audience for the core curriculum should be employees up to and including supervisors. Teaching modules and a trainers'

guide should be developed in consultation with the key government institutions in Ottawa that handle significant amounts of personal information.

The School should also develop a distinct mandatory training module for all middle- and senior-level government managers, acquainting them with the fundamentals of privacy and personal information management. This module could be integrated into existing courses for managers, or offered as stand alone courses, as required. (While the School currently offers two training modules on privacy and access laws, these are not mandatory and their target audience consists of functional specialists and supervisors as well as managers.)

Development of the core curriculum, teaching module and trainers' guide should be done in consultation with the Offices of the Privacy Commissioner and the Information Commissioner.

The Role of ATIP Units

We believe that individual ATIP units should play the lead role in dispensing privacy training to employees and supervisors within their respective departments and agencies.

The foundation of the training provided would be the core curriculum and trainers' guide developed by the CSPS, described above. We recognize, however, that training needs may vary from one department or agency to another. Indeed, federal government institutions that handle large amounts of personal data—such as the Canada Revenue Agency or the Canada Border Services Agency—will have different training requirements than a department that handles comparatively little personal information, such as the Department of Finance. That is why we believe that departments and agencies should be free to adapt the core curriculum and trainers' guide to their particular needs and situations.

Treasury Board Secretariat's Role

TBS is responsible for government-wide administration of the *Privacy Act*. The Secretariat coordinates the administration of the Act by preparing and distributing policies and guidelines to help institutions interpret the law and to assist them in their application on high profile issues.

We believe TBS should make mandatory the training we have described above throughout the federal public service. Indeed, TBS needs to continue to play a leadership role in promoting and overseeing privacy training and awareness across the entire federal public service. Its role and importance in ensuring a culture of privacy within the public service cannot be understated.

The Creation of “Privacy Training Champions”

Every department and agency should consider appointing a “privacy training champion” whose mandate would be to oversee and promote privacy training and learning across that institution. This individual should be a member of the senior management team, possibly the organization’s chief privacy officer.

In keeping with the recommendation the OPC made in its audit of the Canada Border Services Agency, every government institution should consider creating a committee of managers mandated with ensuring that requisite guidance and training are provided to programs areas on privacy issues.

Training Content

The key objective of a privacy training program should be to provide public servants with grounding in federal government requirements respecting the protection of personal information holdings, and the knowledge of best practices for managing personal information.

In order to accomplish this, a privacy training program for public servants would need to address certain key themes and subject matters:

- **Knowledge of Statutory and Policy Requirements:** Public servants must understand their duties and responsibilities under the *Privacy Act*, attendant regulations, and other statutory instruments germane to privacy. (Individual departments and agencies may also need to tailor their training programs to take into account special requirements under the legislation they administer, as well as internal policies respecting data management.)
- **Knowledge of What Constitutes Personal Information:** Public servants who manage personal information need a solid grounding in the definition of personal information – recorded information about an identifiable individual – and what this can include.
- **Knowledge of Basic Principles:** Federal public servants need to know what personal information they can collect, use and disclose in the course of their duties. And they need to know how to maintain personal information in a secure manner. Knowledge of the basic principles of privacy – often referred to as “fair information principles” – is essential.
- **Knowledge of Best Practices:** Some techniques, methods and processes are better than others at delivering positive privacy promotion and protection outcomes.

Providing public servants with a strong knowledge of these techniques will help ensure the personal information of Canadians held by government institutions is managed with limited problems or unforeseen complications. Best practices from federal government institutions, as well as those from other jurisdictions – the provinces, foreign governments and the private sector – should be built into the training program.

Conclusion

The federal government needs to address the privacy training and learning needs of its employees head on. And it needs to do so immediately, before a regrettable incident similar to the one in the U.K. occurs.

Public servants who manage the personal information of Canadians are stewards of a public trust that underpins our system of government.

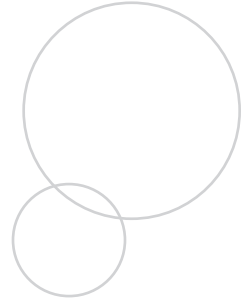
Public servants require sound knowledge of the laws, rules, regulations and policies governing privacy and the management of personal information in the federal government. They need a firm understanding of what constitutes personal information; the basic principles of privacy protection and fair information practices; and an appreciation of the best practices for managing personal information.

This specialized knowledge can only be acquired through a comprehensive and coordinated training program for all federal public servants who manage personal information. The Treasury Board Secretariat and the Canada School of Public Service have a leadership role to play in this regard. ATIP units within individual government departments and agencies also have a key role to play, as they are best placed to dispense the knowledge that staff in their institutions require.

The OPC remains ready to help all of these key players with the development of a privacy training curriculum for the federal government.

A comprehensive approach to privacy training and learning is one of the key elements required to safeguard the personal information of Canadians.

Public servants who manage the personal information of Canadians are stewards of a public trust that underpins our system of government.





UPDATE ON *PRIVACY ACT* REFORM: *FIRST STEPS TOWARD LEGISLATIVE OVERHAUL*

OPC proposes a series of “quick fixes” to improve Canada’s public sector privacy legislation in the short term

Privacy Commissioners have been calling for reform of the *Privacy Act* for many years now and the increasingly urgent need for modernization of the legislation has become a regular theme of our annual reports.

This year is no different. Our current legislation does not adequately protect the personal information of Canadians held by government departments and agencies.

In 2006, our Office issued a comprehensive report detailing recommended changes to the *Privacy Act*.

Since then, we have consulted with external stakeholders on this issue. For example, we asked the Public Policy Forum to organize two roundtable discussions on reform of the federal privacy regime in June and October 2007. These discussions involved senior government officials who have a stake in privacy promotion and protection.

As we were working on this annual report, we received word from the House of Commons Standing Committee on Access to Information, Privacy and Ethics that its members planned to take a look at the *Privacy Act*.

The committee heard from a number of witnesses. Our Office hopes the committee members will return to this work in the fall of 2008.

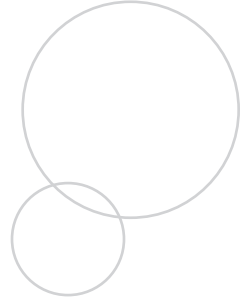
Given that there seems to be little appetite in government for a major rewrite of the legislation, the Commissioner proposed a list of 10 “quick fixes” when she appeared before the committee in April 2008. These relatively straightforward changes would address some of the legislation’s shortcomings – basics such as introducing a “necessity test” for the collection of personal information by government departments.

However, the proposals are most emphatically *not* meant to be the definitive statement on *Privacy Act* reform. Our Office sees these 10 recommendations as a first step in modernizing the legislation while we wait for a comprehensive modernization initiative.

Some of the proposed changes would simply incorporate into the law existing federal government policies and practices. Treasury Board Secretariat has done some good work on privacy matters by providing guidance to line departments, for example, on signing information-sharing agreements and the outsourcing of personal data processing. However, amending the legislation would provide clearer guidance in this regard.

Other proposed changes would correspond to provisions that already exist in or are being contemplated for PIPEDA.

Our Office sees these 10 recommendations as a first step in modernizing the legislation while we wait for a comprehensive modernization initiative.



10 *Privacy Act* “Quick Fixes”

- 1 “Necessity test” requiring government institutions to demonstrate need for personal information they collect.
- 2 Broaden grounds for an application for Court review under section 41 of the *Privacy Act*; give Federal Court the power to award damages against offending institutions.
- 3 Requirement to assess privacy impact of programs prior to implementation and to publicly report assessment results.
- 4 Clear public education mandate.
- 5 Greater discretion to report to Canadians on government institutions’ privacy management practices.
- 6 Discretion to refuse/discontinue complaints where investigation is not in public interest.
- 7 Eliminate restriction that *Privacy Act* applies only to recorded information.
- 8 Require government institutions to report annually on a broader spectrum of privacy-related activities.
- 9 Require ongoing five-year Parliamentary review of *Privacy Act*.
- 10 Stronger provisions governing disclosure of personal information by Canada to foreign states.

The following is a description of the OPC’s proposed “quick fixes”:

- 1 Create a legislative “necessity test” which would require government institutions to demonstrate the need for the personal information they collect.

Background

This “necessity test” is already included in Treasury Board policies as well as PIPEDA. It is an internationally recognized privacy principle found in modern privacy legislation around the world. For example, the provinces and territories have adopted a model in their public sector legislation requiring that one of three conditions be met: the collection is expressly authorized by statute; the information is collected for the purpose of law enforcement; or the information relates directly to *and is necessary* for an operating program or activity.

The *Privacy Act* currently states: “No personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution.” This sets a disproportionately low standard for the fundamental rights at the heart of the *Privacy Act*.

What difference would it make?

By building in better controls at the collection point, there is less potential for misusing and disclosing personal information.

- 2 Broaden the grounds for which an application for Court review under section 41 of the *Privacy Act* may be made to include the full array of privacy rights and protections under the *Privacy Act* and give the Federal Court the power to award damages against offending institutions.

Background

Currently, the Federal Court may only review a refusal by a government institution to grant access to personal information requested by an individual under the *Privacy Act*.

Although the Commissioner can investigate complaints concerning the full array of rights and protections under the legislation and make recommendations, if the response of the institution is not satisfactory, neither the individual nor the Privacy Commissioner may apply to the Federal Court for enforcement and remedy. This means there are no effective remedies for violations of privacy rights, such as the wrongful disclosure of personal information or the inappropriate collection of information.

This is a far lower standard than in the private sector, where PIPEDA provides such remedies for Canadians.

What difference would it make?

Broadening Federal Court review would ensure government institutions respect individuals' rights to have their personal information collected, used and disclosed in accordance with the *Privacy Act*. It would also put the *Privacy Act* on par with PIPEDA.

Every right needs a remedy in order to have meaning.

- 3 Enshrine a requirement for heads of government institutions subject to the *Privacy Act* to assess the privacy impact of programs or systems prior to their implementation and to publicly report assessment results.

Background

A 2002 Treasury Board Secretariat policy on Privacy Impact Assessments (PIAs) was designed to assure Canadians that privacy principles would be taken into account during the development and implementation of programs and services that raise privacy issues.

Unfortunately, the way in which institutions are implementing this policy has been uneven. As reported in our 2006-2007 annual report, an OPC audit found that PIAs are not always conducted when they should be and are frequently completed well after program implementation, or not at all.

What difference would it make?

A legal requirement for PIAs would ensure they are done on a consistent and timely basis.

As well, PIAs should be submitted to the OPC for review prior to program implementation – allowing our Office to offer recommendations on how privacy could be better protected.

- 4 Amend the *Privacy Act* to provide the Office of the Privacy Commissioner of Canada with a clear public education mandate.

Background

While the OPC's central function under the *Privacy Act* is the investigation and resolution of complaints, the OPC also needs to advance privacy rights by other means – through research, communication and public education. The Commissioner lacks a clear legislative mandate under the *Privacy Act* to educate the public about their privacy rights with respect to information held by federal government institutions.

What difference would it make?

A clear public education authority would allow the OPC to publish public advisories and education material on significant policy and legislative measures with “personal information” components.

PIPEDA contains such a mandate and it is only logical that the *Privacy Act* contain a similar mandate for the public sector.

- 5 Provide greater discretion for the Office of the Privacy Commissioner of Canada to report publicly on the privacy management practices of government institutions.

Background

As it now stands, our Office reports to Parliament and Canadians through annual or special reports. There is no specific section in the legislation authorizing the Commissioner to make public interest disclosures.

The OPC has been hampered in its ability to speak with the press, the public, and even Members of Parliament, due to the existing confidentiality constraints in the *Privacy Act*.

Waiting until the end of the reporting year to tell Canadians about privacy issues related to federal institutions means the information has sometimes become moot, stale or largely irrelevant. A clear discretion for public interest disclosures would allow for more timely and relevant public discussions about privacy issues important to Canadians.

What difference would it make?

This discretion would be an important tool for advancing public understanding, providing public assurances, and restoring public confidence where required.

Canadians would have timely information about how the federal government is handling their personal information.

- 6 Provide discretion for the Privacy Commissioner to refuse and/or discontinue complaints the investigation of which would serve little or no useful purpose, and would not be in the public interest to pursue.

Background

At the moment, valuable resources are still being disproportionately consumed by having to open and investigate all individual complaints on a first-come, first-serve basis. Examples of complaint types where relatively little is gained by investigating include:

- Repetitive issues that have already been clearly decided in past cases (e.g. legitimate collection and use of Social Insurance Numbers.)
- Moot time complaints where the individual has since received the information requested (e.g. where access was already provided, though technically out of

time and at no disadvantage to the individual.)

- Frequent complaints brought forward by the same individual against an institution (e.g. where contentious labour or employment issues constitute the real dispute.)
- Multiple complaints brought by many individuals about the same incident (e.g. a large data breach.)
- Issues that have already been recognized and addressed by a government institution.

Many data protection authorities in Canada and elsewhere face similar challenges in having to treat all complaints received indiscriminately, with no ability to dismiss or discontinue some of them early on where no public interest would be served by investigating or continuing to investigate them.

What difference would it make?

This discretion would allow our Office to focus more investigative resources on privacy complaints which are of broad systemic interest and affect the interests of a significant number of Canadians.

- 7 Amend the *Privacy Act* to align it with the *Personal Information Protection and Electronic Documents Act* by eliminating the restriction that the *Privacy Act* applies to recorded information only.

Background

Unrecorded information – such as surveillance cameras that are used to monitor people, but do not record images – is beyond the scope of the *Privacy Act*. Personal information contained in deoxyribonucleic acid, known better as DNA, and other biological samples is not explicitly covered.

Under PIPEDA, personal information includes personal information in any form.

What difference would it make?

Expanding the definition of personal information would ensure the *Privacy Act* is responsive to the digital imagery and biometric applications of contemporary law enforcement surveillance and monitoring activities. It would also offer protection for DNA and other biological samples.

- 8 Strengthen the annual reporting requirements of government departments and agencies under section 72 of the *Privacy Act*, by requiring these institutions to report to Parliament on a broader spectrum of privacy-related activities.

Background

The *Privacy Act* requires the head of a government institution to submit an annual report to Parliament on the administration of the Act. Our experience in reviewing these reports over the years indicates that, on the whole, they have rarely contained substantive information. Rather, they've tended to be a patchwork of statistics about the number of *Privacy Act* requests received; dispositions taken on completed requests; exemptions invoked or exclusions cited; and completion times.

Treasury Board Secretariat issued comprehensive privacy reporting guidelines for government institutions in 2005, and updated these in early 2008. The *Privacy Act* should be amended to integrate these guidelines into legislation in order to provide them with added weight and authority.

What difference would it make?

A more comprehensive coverage of privacy management issues would provide Parliamentarians with relevant information to evaluate the extent to which government institutions are addressing privacy challenges, and whether new initiatives may pose a threat to the privacy rights of citizens. Individuals would also be better informed on how government departments and agencies are handling their personal information.

- 9 Introduction of a provision requiring an ongoing five-year Parliamentary review of the *Privacy Act*.

Background

The privacy landscape is dynamic and constantly evolving. It is not unreasonable to expect that Parliament should review the *Privacy Act* on a regular basis, in light of new technologies or government measures that may impact on the right to privacy of Canadians.

By contrast, PIPEDA requires that the first part of that Act be reviewed every five years. A number of provinces have a similar requirement for regular legislative review of their public sector privacy law.

What difference would it make?

A five-year review requirement would help synchronize the Canadian data protection framework across jurisdictions. It would also keep the privacy practices of both private and public sector organizations on the minds of Canadian decision-makers and industry. Finally, it would ensure federal law keeps pace with rapidly evolving technologies and international trends.

10 Strengthen the provisions governing the disclosure of personal information by the Canadian government to foreign states.**Background**

Technological advances have made it much easier and less expensive for governments to collect and retain personal information about citizens. At the same time, information sharing between nations has increased dramatically as governments have adopted more coordinated approaches to regulating the movement of goods and people and to combating trans-national crimes and international terrorism.

For example, the Canadian Border Services Agency shares customs information and information about travellers entering Canada with other countries, while the Financial Transaction and Reports Analysis Centre (FINTRAC) has over 40 agreements with other financial intelligence units to share information about suspected money launderers and terrorists.

The *Privacy Act* does not reflect this increase in international information sharing. It places only two restrictions on disclosures to foreign governments: an agreement or arrangement must exist; and the personal information must be used for administering or enforcing a law or conducting an investigation.

The *Privacy Act* does not even require that an information-sharing arrangement be in writing, let alone impose any requirements concerning the content of such agreements.

The consequences of sharing personal information without adequate controls were dramatically highlighted in the Maher Arar case.

During the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, Justice O'Connor concluded it was very likely that, in making the decisions to detain and remove Mr. Arar to Syria, U.S. authorities relied on inaccurate information about Mr. Arar provided by the RCMP. Justice O'Connor made a series of recommendations to strengthen RCMP policies and practices when sharing information with other government authorities.

The Government of Canada and Parliament should consider specific provisions to define the responsibilities of those transferring personal information to other jurisdictions and to address the adequacy of protection in those jurisdictions.

What difference would it make?

Good controls on information sharing would minimize the risks to Canadians. Better control would serve to ensure that information being shared is relevant and accurate,

that appropriate caveats are given, circumscribing the use of the information only for the purpose for which it was shared.

Conclusion

These 10 straightforward changes would begin the process of aligning the *Privacy Act* with modern data protection legislation around the world.

Our Office hopes that Canada will one day regain the leadership role in privacy promotion and protection it once held, when the *Privacy Act* was first adopted some 25 years ago.





PROACTIVELY SUPPORTING PARLIAMENT

A key part of the OPC's mandate under the Privacy Act is to support Parliament's work by providing information and advice on privacy issues

National security initiatives continued to raise privacy concerns in 2007-2008 and were a key focus of our work with Parliamentarians and officials in many government departments.

National security issues of particular note were Canada's new no-fly list, the government's lawful access consultations and plans for enhanced driver's licences in some provinces.

From our Office's point of view, one of the bright spots in the area of law enforcement was the introduction of legislation aimed at tackling identity theft.

The OPC also provided input on a number of other issues during the year, including possible amendments to copyright legislation and the development of electronic health records.

LAW ENFORCEMENT AND NATIONAL SECURITY INITIATIVES

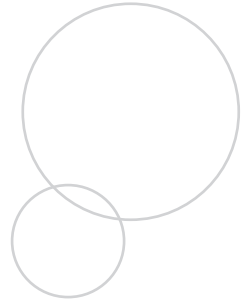
It is impossible to overstate how privacy rights around the world have been rolled back since the terrorist attacks of Sept. 11, 2001. Governments everywhere – Canada included – have responded with a wide range of national security initiatives, which often focus on gathering more and more information about the routine, day-to-day activities of ordinary people.

Governments appear to believe that the key to national security and public safety is collecting, sorting and analysing mountains of personal data – without demonstrating the effectiveness of doing so.

Privacy often receives short shrift as new anti-terrorism and law enforcement initiatives are rolled out. This trend continues several years after the 9-11 tragedies.

Canadians expect the government to take measures to protect them; equally, they expect these measures will respect their rights, including their right to privacy, and also conform to the rule of law. This includes legal standards, such as due process, the right to consult counsel, the right to see evidence held against you and other elements of procedural fairness that underpin our justice system.

Privacy often receives short shrift as new anti-terrorism and law enforcement initiatives are rolled out. This trend continues several years after the 9-11 tragedies.



The following is a summary of some of the top national security and law enforcement issues of 2007-2008:

No-Fly List

Much of the post 9-11 focus has been on air travel security. In Canada, the federal government created a no-fly list which raises profound concerns about not only privacy, but other related human rights, such as freedom of association and expression and the right to mobility.

Fundamental flaws in the program were highlighted within days of the no-fly list, or Passenger Protect Program, coming into force in June 2007.

Two Canadian boys with the same name became entangled by North America's no-fly lists because they share the name of someone on one of these lists.

Their stories were similar: Alarm bells went off when each boy arrived at an airline check-in counter to try to catch a flight. The boys' families were told there was a security issue because of a name match with a no-fly list. (It was unclear which list they were on.) Both boys were allowed to fly after lengthy delays, apparently because their ages – 10 and 15 – made it clear they posed no threat.

An airline official warned one of the families there would be trouble each time their son tried to fly in the future and proposed a dramatic solution – changing his name.

The Passenger Protect Program involves the secretive use of personal information and, despite this significant intrusion on our privacy rights, Canadians have no legally enforceable rights to independent adjudication, compensation for out-of-pocket

expenses or other damages, or to appeal. Canadians also have no right to ask whether they are even on the list.

The government has said the list includes up to 2,000 names. There is clearly a significant risk for false positives – a problem we have seen in the US, where children and public figures such as Senator Edward Kennedy have faced questioning or been denied boarding.

Our Office has been clear that it will not stand in the way of initiatives which will protect the lives of Canadians. However, despite our repeated requests, Transport Canada has provided no evidence demonstrating the effectiveness of no-fly lists.

Some security experts suggest that improving physical screening at our airports – including thorough luggage and cargo checks – would be a more realistic and effective way to enhance aviation security.

An audit of the privacy management practices of the Passenger Protect Program is planned.

Shortly after the no-fly list came into effect, Canada's federal, provincial and territorial privacy commissioners and ombudsmen united to call for extensive reforms to the program. In a joint resolution, we called for the program to be suspended, or, at a minimum, to operate under strict ministerial scrutiny with regular public reports to Parliament while a comprehensive public Parliamentary review is completed.

NOTE: Information about our review of the Privacy Impact Assessment of the Passenger Protect program is included on page 82.

Privacy officials around the world share similar concerns about the widespread use of no-fly lists, as well as the collection and sharing of passenger data.

Data protection authorities attending the 29th International Conference of Data Protection and Privacy Commissioners in Montreal hosted by our Office supported a resolution calling for international standards for the use and disclosure of personal information collected by a travel carrier about its passengers.

The no-fly list was also a major focus when the Privacy Commissioner appeared before the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 in November 2007. We urged the Inquiry to consider the need for clear legal remedies, enforceable safeguards, and effective oversight as it assesses the adequacy of air travel security measures.

Lawful Access

In October 2007, Public Safety Canada issued a brief consultation paper on lawful access and difficulties faced by law enforcement agencies in obtaining customer information such as name, address, telephone number or IP address from telecommunications service providers.

Some companies provide this information voluntarily, while others require a warrant before providing any information, regardless of its nature or the nature of the situation.

The Public Safety Canada consultation document says this is making the job of police officers challenging because they may have no means to compel the organizations to provide the information they are seeking.

“For example, law enforcement agencies may require the information for non-investigatory purposes (e.g., to locate next-of-kin in emergency situations) or because they are at the early stages of an investigation. The availability of such building-block information is often the difference between the start and finish of an investigation,” the consultation paper said.

The consultation document does not provide any sense of the scope of the difficulties mentioned in the document. Are 20 per cent or 80 per cent of companies providing information voluntarily? Do companies respond differently depending on the situation – in a next-of-kin emergency situation versus a request involving suspected violent crimes? We don’t have the answers to these key questions.

In our Office’s opinion, requiring all telecommunications service providers to disclose customer information on request is an overly broad, one-size-fits-all response to a problem that has not been clearly defined or measured.

Neither this consultation paper, nor previous consultation documents has presented a compelling case based on empirical evidence that the inability to obtain customer data in a timely way has created serious problems for law enforcement and national security agencies.

Assuming there is a well-documented and empirically demonstrated problem in obtaining access to customer information, we are not convinced that requiring telecommunications service providers to disclose this information without a warrant is the only, or most appropriate, solution.

It is our view that there is a reasonable expectation of privacy in customer data – making any mandatory disclosures or seizures of dubious constitutional validity.

Although the consultation paper identified the “absence of explicit legislation” as a problem to be addressed, PIPEDA is, in fact, an explicit legislative code which permits lawful access by law enforcement and national security agencies while protecting the privacy and other rights and freedoms of Canadians.

PIPEDA allows telecommunications service providers and other organizations to disclose personal information without consent to law enforcement agencies without a warrant for the purpose of enforcing a law or carrying out an investigation. It also allows disclosures without consent in emergencies which threaten someone’s life, health or security.

Lawful access was the subject of considerable discussion during a five-year review of PIPEDA conducted by the House of Commons Standing Committee on Access to Information, Privacy and Ethics. In its response, the government indicated there is a need to clarify the concept of lawful authority. The government noted that PIPEDA currently allows organizations to collaborate with law enforcement and national security agencies without a subpoena, warrant or court order.

Before considering legislation which would make the disclosure of customer information mandatory on request, we would strongly recommend that the government determine whether clarification to PIPEDA, together with any guidance that may be appropriate, could address the perceived problem.

Lawful access raises fundamental issues for rights such as privacy and the ability to communicate freely. Our Office will continue to monitor this issue and to raise our concerns with government officials and Parliamentarians.

Enhanced Driver’s Licences

Plans to consider or implement enhanced driver’s licences (EDLs) in several Canadian provinces have prompted our Office as well as provincial and territorial privacy guardians to express their concerns about privacy and security risks.

The moves toward enhanced driver’s licences are a provincial response to the U.S. government’s requirement that travellers provide proof of identity and citizenship to comply with the Western Hemisphere Travel Initiative.

These developments have raised concerns among federal, provincial and territorial commissioners and ombudsmen responsible for privacy.

A key concern is that personal information of participating drivers should remain in Canada and that there is meaningful and independent oversight of how the U.S. Customs and Border Protection receives and uses Canadians’ personal information.

As well, RFID technology in enhanced driver's licences poses a potential privacy threat because it may permit the surreptitious location tracking of individuals carrying an EDL. The technology may not encrypt or otherwise protect the unique identifying number assigned to the holder of the EDL and would not protect any other personal information stored on the RFID.

In February 2008, we issued a unanimous joint resolution outlining the steps that will need to be taken to ensure the privacy and security of any Canadian's personal information accessed as part of EDL programs.

In the resolution, we emphasized that Canadian citizens already have access to a well-established, highly-secure travel identification document in the form of the Canadian passport, but acknowledged that some may want an alternative.

Identity Theft

New legislation aimed at addressing identity theft represents a significant step forward in tackling this growing crime.

A central notion of privacy is that people should be able to control how, when and for what purposes their personal information is used. Victims of identity theft have clearly lost control over their personal information – with often serious and long-lasting consequences. Their privacy has been violated in a very significant way.

Identity theft is a complex problem, with many contributing factors.

Bill C-27 focused on the early stages of identity theft and addressed a number of different ways in which criminals gather personal information. For example, it:

- Makes it an offence to possess or traffic in identity information when this information is to be used for a fraudulent purpose;
- Tackles a common technique used by identity thieves – mail re-direction – by making it an offence to fraudulently redirect anything sent by post; and possess a mail key;
- Addresses credit card fraud by creating a new offence dealing with the possession of instruments for copying credit card information; and
- Makes the obtaining, selling or possessing of “identity documents” that relate to another person an offence, punishable by up to five years in prison.

These changes will provide police officers with important new tools to stop identity thieves or fraudsters *before* Canadians suffer actual financial harm.

Another praiseworthy element of the legislation is the possibility that offenders will be required to pay restitution to victims. This is significant in that it recognizes the serious financial impact identity theft can have on individuals.

It is our view, however, that this identity theft bill is only a beginning and that other types of legislative changes are also necessary.

For example, a key issue not addressed in Bill C-27 is pretexting – where an individual obtains personal information, such as telephone or financial records, by pretending to be someone authorized to have it. We also need to legislate against spam – often used by identity thieves to trick people into providing personal information online. Canada is the only G-8 country without anti-spam legislation.

OTHER LEGISLATION AND INITIATIVES WITH AN IMPACT ON PRIVACY

Copyright

The federal government has been studying changes to the *Copyright Act* for the last few years.

In January 2008, the Privacy Commissioner wrote to the Minister of Industry and the Minister of Canadian Heritage regarding possible amendments to the Act.

In particular, our Office is concerned about possible changes authorizing the use of technical mechanisms to prevent copyright infringement that could have a negative impact on the privacy rights of Canadians. In some cases, such mechanisms to protect copyrighted material result in the collection, use and disclosure of personal information without consent.

Technological protective measures can be embedded in various media to control copying and prevent copyright infringement, or they can be built into electronic devices to prevent the reading of unauthorized content.

Digital rights management is the general term for the varied technologies used to enforce pre-defined limitations on the use of digital content. These include any means by which publishers or manufacturers control use of data or hardware.

If digital rights management technologies only controlled copying and use of content, we would have few concerns. However, they can still collect detailed personal information from users, who often access the content on a computer. This information is transmitted back to the copyright owner or content provider, without the consent or knowledge of the user.

Although the means exist to circumvent these technologies and thus prevent the collection of this information, previous proposals to amend the *Copyright Act* contained anti-circumvention provisions.

Technologies that report back to a company about the use of a product reveal a great deal about an individual's tastes and preferences. Indeed, such information can be extremely personal.

Our Office will carefully assess the privacy implications of any legislation to amend the *Copyright Act*.

Electronic health records

The federal government is encouraging the development of a system of electronic health records through the Federal Healthcare Partnership.

We are monitoring the progress of this group, which would impact the health care services provided to First Nations and Inuit populations, eligible veterans, members of the Canadian Forces, RCMP, federal inmates and refugee protection claimants.

As well, our Office is an active participant in the new Canada Health Infoway Privacy Forum, which brings together representatives of the health ministries and privacy oversight offices across Canada. The Forum is discussing fundamental privacy and governance issues that must be addressed to ensure the successful implementation of electronic health records.

Infoway's goal is to ensure that, by 2010, half of Canadians will have their electronic health record readily available to health care providers.

While electronic health records offer significant benefits, such as rapid access to complete patient information for health professionals, they also raise a number of privacy risks.

The protection of privacy must be a key factor as we consider how these highly sensitive records are managed. It is crucial that patients know what is happening to their health information and feel confident that they can exercise a measure of control over it.

Electronic health records will require extremely strong security measures, including safeguards to ensure only authorized people can access the information. Careful attention must also be given to potential secondary uses for the information, including health research.



RESPONDING TO COMPLAINTS AND PRIVACY INCIDENTS

How the OPC dealt with complaints and incidents under the Privacy Act in 2007-2008

The complaints we receive show Canadians have a wide range of concerns about how the government is handling their personal information.

Canadians are uneasy about the sharing of information between departments; the use of e-mail to record and/or share information; and the problems associated with institutions maintaining and properly allowing individuals a right of access to personal information stored on computers.

We have also noticed a growing concern about how government institutions are protecting their information. Headlines about personal information being lost or stolen when public servants telework or bring home work on laptops do not inspire public confidence.

The cases we investigated over the year also highlighted how human error can jeopardize personal privacy. Some of the breaches we looked at show how problems with computers and use of other mechanized equipment designed to improve government processes can result in the disclosure of personal information. It is also clear that government institutions must continue to emphasize to employees the importance of safeguarding personal information and privacy.

Another issue which continues to concern our Office is ongoing delays in processing individuals' requests for access to their personal information. While some departments have improved their response times, many federal Access to Information and Privacy (ATIP) units are overwhelmed.

NOTE: Detailed statistical charts; definitions of each type of complaint and findings; and a chart describing the course of a *Privacy Act* investigation are included in the Appendices.

Snapshot: Inquiries, Complaints and Investigations

Inquiries

<i>Privacy Act</i> inquiries received:	4,258
General privacy inquiries:	2,367
Total (excludes PIPEDA inquiries):	6,625

Complaints

Total new complaints received:	759
--------------------------------	-----

Top 10 institutions by complaints received

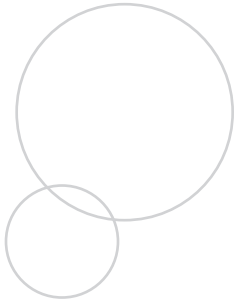
Correctional Service Canada	248
Royal Canadian Mounted Police	84
Canada Border Services Agency	54
Service Canada	52
National Defence	48
Canadian Security Intelligence Service	45
Canada Revenue Agency	38
Canada Post Corporation	28
Foreign Affairs and International Trade	27
Justice Canada	18
Others	117
Total	759

Inquiries

Our Office received a total of 4,258 inquiries related to the *Privacy Act* and another 2,367 more general inquiries about privacy in 2007-2008. These figures do not include the 7,636 inquiries related to PIPEDA, the legislation applying to the private sector, received in 2007. The average daily number of inquiries we receive about all privacy issues is close to 60.

Our inquiries unit provides an extremely important service to Canadians, who are able to obtain a timely response to questions touching on a wide array of privacy issues.

Our inquiries unit provides an extremely important service to Canadians, who are able to obtain a timely response to questions touching on a wide array of privacy issues.



Complaints

We received 759 new complaints, down slightly from the previous year's 839.

The number of complaints filed against institutions does not necessarily mean that these institutions are not compliant with the *Privacy Act*.

Some institutions – because of their mandate – hold a substantial amount of personal information and are more likely to receive numerous requests for access to that information. There is also a higher likelihood of complaints about the institution's collection, use and disclosure, retention and disposal of personal information, and the manner in which it provides access to that information.

Correctional Service Canada and the RCMP have been the top two institutions receiving complaints over the past few years. It is noteworthy that there has been a steady drop in the number of RCMP complaints, but a fairly significant increase in Correctional Service Canada complaints – from 190 in 2005-2006 to 248 in 2007-2008. The rise in the number of complaints against Correctional Services Canada may be directly proportional to the additional access to personal information requests it received.

A complete list of complaints received by institution can be found in Appendix 3.

The majority of all new complaints were from individuals who claimed that federal government institutions denied them a right of access to their personal information. The second most common type concerned the 30-day statutory time limit (extended to 60 days in some circumstances) for institutions to respond to a personal information request.

Detailed information about complaints received by type can be found in Appendix 3.

Closed Complaints in 2007-2008

Total	880
--------------	------------

Top 3 Categories of Closed Complaints

Denial of access	318
Time Limits Exceeded	301
Improper use / disclosure of personal information	134

Disposition of Closed Complaints

Discontinued	117
Early resolution	32
Settled during the course of investigation	114
Resolved	6
Not well-founded	275
Well-founded	319
Well-founded and resolved	17
Total	880

Individuals may discontinue their complaints because they have resolved the issue with the institution before the active investigation has begun. Our Office may also discontinue complaints due to a lack of information necessary to complete our investigations. When a complaint is resolved through early resolution or by settling, this indicates the individual is satisfied with the actions taken by the institution as a result of our intervention.

Obtaining Access to Personal Information

Obtaining access to personal information held by a government institution is a basic privacy right that is afforded to individuals under the *Privacy Act*. However, it is clear many Canadians are having difficulties exercising this right. More than 70 per cent of the complaints filed with this Office related to individuals expressing concern about being denied access to their personal information or because institutions failed to provide that information within the statutory time limit.

Our Office is pleased to see that the total number of complaints in both these categories has declined over the last few years. This may be because individuals are dealing directly with institutions to resolve their concerns, a practice that our Office encourages.

Time limit complaints are opened when an individual notifies this Office that an institution has failed to respond to his or her *Privacy Act* request within 30 days. In some cases a year had passed without the institutions responding to individuals' requests. One complainant had been waiting for more than two years for a response to his request.

Investigations and Inquiries Challenges

Our Office is facing its own challenges in responding to complaints in a timely way. We are strongly committed to improving our complaint treatment times.

In 2007-2008, we received 759 complaints and closed 880. We had a backlog of 370 complaints that were unassigned because of a lack of investigators. On average, it took 14.5 months to complete a complaint investigation. We know this is unacceptable and are undertaking a number of measures to remedy the situation.

A detailed breakdown of the treatment times by finding and complaint type can be found in Appendix 3.

We are challenged by the fact that, under the wording of the *Privacy Act*, we need to deal with every complaint we receive. Other data protection authorities around the world and in Canadian provinces are also finding similar challenges with the need to address all complaints received – regardless of their nature or seriousness.

Our Office has asked the federal government for legislative amendments to provide us with this flexibility, a step that would allow us to better focus our investigative resources. (See page 45 for more detailed information.)

Another major challenge is attracting and retaining seasoned investigators and managers in this area. People with *Privacy Act* and investigation experience are in high demand across government and there are not enough qualified individuals to go around. An older generation is retiring and the new generation is extremely mobile in a competitive job market. Turnover rates in this area have been higher than elsewhere in the OPC due to retirement and external demand.

We are continuing to revitalize our investigations unit by focusing our efforts on recruitment, as well as looking at innovative means to improve service delivery to Canadians.

Our strategy includes re-engineering our investigative process by streamlining inquiries, complaints and investigations. We will triage complaints and identify those which could likely be resolved early in the process. A new case-management system will help us to better identify trends and focus resources where they can have the most impact.

We anticipate it will take a year to build capacity, diminish the backlog, continue hiring and training more staff to investigate in innovative ways. Our goal is to complete the re-engineering initiative in the spring of 2009.

Training and Inter-jurisdictional Cooperation

Training will play an important role in our continuous efforts to improve how we investigate and attempt to resolve complaints about privacy breaches.

In February 2008, we hosted our fourth annual investigators conference. We welcomed more than 90 participants at this Ottawa event, including representatives from 12 of the 13 provincial and territorial privacy offices, and, for the first time, members of the Office of the Information Commissioner of Canada. The conference allowed investigators to share experiences and best practices. Open and frank discussions increased awareness of common issues.

Complaints – Examples of Cases the OPC Investigated

Passport Canada apologizes for “unacceptable error”

The complainant mailed his passport renewal application to Passport Canada. As required, he provided his expiring passport, photocopies of his driver’s licence and health card, and his original birth certificate. When he received his new passport in the mail, the envelope contained another person’s expired passport and other personal documents.

The individual notified Passport Canada of the error. The agency asked him to return the other individual’s documents, which he did, and said that it would search for his documents. Passport Canada contacted the other individual and learned that he had destroyed the complainant’s documents.

Our investigation determined that a passport employee had mixed up the contents of two files and then failed to check that the labelled envelope, new passport and other documents all matched the intended recipient.

Passport Canada apologized for what it acknowledged was an “unacceptable error” and said it had taken steps to ensure it did not happen again. Managers now hold monthly briefings with staff to verify that proper procedures are being followed. In addition, the agency posts the procedures and all new employees are trained and instructed on the importance of verifying documentation prior to it being placed in an envelope and mailed to a recipient.

The complaint was well-founded.

Inmate report discovered in prison gym garbage can

A report containing pictures, names, birthdates and cell locations of 96 inmates, as well as other personal information, was found in an offender's cell at an Alberta prison. Fourteen affected inmates complained to our Office.

An offender had discovered the report in a garbage can in the prison's gym. Correctional Service Canada's investigation determined that this report was routinely updated and posted for correctional officers in an office next to the gym. Out-of-date reports were being regularly discarded in the gym's garbage can.

To ensure that such a disclosure does not occur again, Correctional Service Canada instructed the institution to stop posting this type of information in the office next to an area used by offenders and to take greater care with personal information.

The complaint was well-founded.

Canada Revenue Agency employee misuses information

A woman complained that her former neighbour, who worked for the Canada Revenue Agency, improperly gained access to her tax files in order to identify her place of employment and then used this information to make harassing and threatening phone calls.

The complainant had a history of problems with the Canada Revenue Agency employee. She stated that the employee and her family had threatened and harassed her for years. The complainant moved and obtained an unlisted telephone number. After her move, she began receiving harassing calls at her place of work. She determined that these originated from the Canada Revenue Agency employee.

The agency confirmed that its employee had used her position to gain access to the complainant's personal information. This included the complainant's address, Social Insurance Number, place of employment, income and deductions. The agency confronted the employee about her actions and she confirmed she had viewed the complainant's tax information. She was disciplined for the unauthorized access to the complainant's personal information.

The CRA has an extensive audit trail process allowing it to maintain the security of taxpayers' information.

The complaint was well-founded.

Identity of information requester revealed

A Foreign Affairs and International Trade Canada (DFAIT) employee complained the institution improperly disclosed his personal information to co-workers. The co-workers then disclosed it to the Public Service Alliance of Canada.

In addition to being a DFAIT employee, the complainant's union work had been criticized by the local's executive and some members. The complainant submitted *Privacy Act* requests seeking all personal information held by five co-workers, who were also his fellow union members and the ones who had criticized him.

When DFAIT received his requests, the ATIP unit asked the co-workers to provide all personal information they held about the complainant. ATIP staff alerted the co-workers of the sensitivity of the request and informed them of the restriction for further dissemination of that information on a "need-to-know" basis within the institution.

The first issue our Office reviewed was the complainant's concern about being identified as the requester. We concluded this complaint was not well-founded. In order to obtain the information held by the co-workers, the ATIP unit needed to disclose his identity.

As for the complainant's concern about the co-workers notifying the union that he had submitted *Privacy Act* requests, our investigation confirmed that four of the five had informed the Public Service Alliance of Canada of his actions. The co-workers believed that the complainant had submitted his requests in an effort to harass them. All four confirmed they had read the ATIP unit's reminder about the sensitivity of his request, but considered the matter union business, not departmental business.

While the disclosure of the complainant's identity to his co-workers was not well-founded, the fact that four co-workers notified the union that he had submitted *Privacy Act* requests violated his privacy rights.

The complaint was well-founded.

Monitoring of employee's e-mails was appropriate

An Indian and Northern Affairs employee complained that the institution did not have the authority to restore 35 months of the employee's e-mails and then review all of the messages contained in the departmental account. The employee alleged that as a result of the department's actions, the employee's personal information was improperly accessed.

The employee was the subject of an administrative investigation into allegations that the employee was misusing the department's network.

During the course of its investigation into the complainant's actions, the institution restored the complainant's e-mail account and found pornographic e-mails.

Later, the employee received a copy of the Terms of Reference for the administrative investigation and noted that it was not signed. The employee contended that, as the document was not signed, the institution had no authority to restore or read the e-mails. The employee also contended that there should have been notification of the institution's actions.

Treasury Board's policy states that if an institution reasonably suspects that an individual is misusing a department's network it must refer the matter for further investigation and action which may involve special monitoring and/or reading the contents of an individual's e-mails.

Indian and Northern Affairs policy states that management is permitted to have access to an employee's e-mail in the course of any investigation relating to impropriety, security breaches, violation of a law or infringement of departmental policies.

Although the Terms of Reference were not signed and the employee was not advised of the institution's actions, Indian and Northern Affairs did not violate Treasury Board's policy on network use or the employee's privacy rights. Under the *Privacy Act*, institutions may use personal information for the purpose for which it was obtained or compiled or for a use consistent with that purpose. In this case, the information gathered from the employee's e-mail account was used solely for the purpose of the institution's administrative investigation.

The complaint was not well-founded.

Reporter identified in response to access request

A journalist complained that his name had been improperly released in a response to a request made under the *Access to Information Act* (ATIA). The name of the journalist appeared in an e-mail message prepared by a Privy Council Office employee.

The e-mail came to light after another reporter requested access to all e-mails and communications sent or received by the director of communications in the Prime Minister's Office.

The response to that request included an e-mail from an employee of the Privy Council Office (PCO) to 19 government officials in both the PCO and the Prime Minister's Office.

The e-mail was written after a multi-department conference call during which an official with Public Safety Canada discussed the pending release of information about a sensitive issue in response to an ATI request. In the e-mail, the PCO official discussed the possibility of another article being written by the complainant about a sensitive issue that he had previously reported on. Other reporters' names were also mentioned in the e-mail, primarily concerning stories that had already appeared in print. While their names were blacked out, the complainant's name had been overlooked and released in error.

The Privy Council Office subsequently apologized to the complainant.

As the complainant's name was released to the other reporter in response to an ATI request, the OPC concluded that his privacy rights had been violated. The complaint was well-founded.

A related complaint alleged that the PCO official disclosed that the journalist had filed an ATI request to Public Safety Canada during the multi-department conference call.

However, our investigation confirmed that the ATI requestor's identity was never disclosed outside of the ATIP office of Public Safety Canada.

The PCO official stated he had simply made an assumption about who had made the request based on the fact that the journalist had written a number of articles on the subject.

The Assistant Commissioner was satisfied that the journalist's identity as the person making the access request was not under the control of PCO. This complaint was not well-founded.

A third complaint from the same journalist against Public Safety Canada that it had disclosed his name as an ATI requester was also not well-founded. That complaint was closed in the previous reporting year.

Improper disclosure of information to prospective employer

A man contended that Human Resources and Skills Development Canada (HRSDC, now Service Canada) improperly provided his Social Insurance Number, address, birth date, income information and employment insurance application details to a prospective employer.

While receiving employment insurance (EI) benefits, the complainant turned down a job offer from a company. As a result, HRSDC disqualified his EI benefits. The

complainant appealed its decision to the Board of Referees. He claimed that he had refused the job because of working conditions.

In accordance with the *Employment Insurance Act*, when an individual appeals a decision to the Board of Referees, HRSDC may share that individual's information with interested parties such as employers and any person with a vested interest. The disclosure of information to these parties is necessary to establish the validity of an individual's request for continuation of EI benefits.

In this case, HRSDC deemed that the prospective employer was a party to the complainant's appeal and gave the company a complete package of information. HRSDC did not review the complainant's file and released his Social Insurance Number, birth date and information relating to his past employment record, including rates of pay and overtime. As the complainant's appeal to the Board of Referees was based on refusing the job offer because of working conditions, the information released by HRSDC to the parties should have been limited to what was required to establish the validity of his decision to refuse that job offer.

HRSDC agreed that it had released too much information, calling the incident an "honest mistake made in good faith by an employee." As a result of this complaint, it reviewed its policies and procedures and changed the definition of employer to include "a current or former person or organization for whom the claimant worked." A prospective or potential employer is no longer considered an interested party in the appeal process.

The complaint was well-founded.

Incidents under the *Privacy Act*

Our Office also reviews cases involving the mismanagement of personal information which come to our attention through media reports, affected individuals or breach notifications from government institutions.

Data breaches

Treasury Board Secretariat published privacy breach guidelines for institutions subject to the *Privacy Act* at the end of March 2007. The guidelines "strongly recommend" that government institutions notify the OPC if a breach involves sensitive personal information such as financial or medical information or Social Insurance Numbers or if there is a risk of identity theft or some other harm or embarrassment which could have an impact on an individual's reputation, financial position or safety.

During the first year in which the guidelines have been in place, we have noticed an increase in the number of reported incidents (57 in 2007-2008 as compared to 43 for 2006-2007). The fact that the number of incidents is relatively low, when one considers the large amount of personal information held by government institutions, is encouraging news.

Most incidents occurred as a result of human error or theft, for example, when documents containing someone's personal information were lost, or when a government employee's briefcase was stolen from a hotel room or a laptop was taken from a vehicle. In one instance, employees gained unauthorized access to personal information stored on government computer systems.

The following are some typical incidents we reviewed:

Technology glitch results in disclosure of sensitive information

A failed effort by Public Works and Government Services Canada (PWGSC) to remove exempted information when it respond to *Access to Information Act* (ATIA) requests using CDs rather than paper format compromised a number of individuals' personal information.

Over the last number of years, institutions have been responding to some *Access to Information Act* and *Privacy Act* requests by sending the information on CDs rather than in paper format. At PWGSC, the CDs were scanned in "Tagged Image File Format" (TIFF), which is a picture copy of the document. The imaging program was changed to "Portable Document Format" (PDF) when requesters complained about having difficulties in opening TIFF files.

The recipient of one of the CDs that contained the information in PDF format informed the institution he was able to read the information that had been exempted. He said that he simply selected the severed portions and pasted them into another document.

Before this problem was brought to its attention, the institution had responded to 123 ATIA requests and one *Privacy Act* request using the PDF format. As a result, people who received the CDs were able to read the names and home addresses of government employees being investigated for fraud involving government credit cards, the names and birth dates of people undergoing security clearances, the results of second language evaluations and employee leave information.

In an effort to minimize any further disclosure, PWGSC attempted to retrieve the CDs from requesters. Some requesters did return the CDs, while others said they had

destroyed or lost them. Individuals whose personal information was at risk were notified by the institution of the potential breach.

It was determined that the problem was a flaw in an imaging system. The manufacturer of the software was contacted and confirmed that PWGSC was the only institution with a flawed version. That being said, to ensure that this did not occur in another institution, Treasury Board prepared a general security bulletin warning institutions not to release information on CDs until they received certification that their programs were secure.

Stolen laptop contains household survey information

An encrypted laptop stolen from a Statistics Canada employee's home contained the personal information of several Canadians who had taken part in surveys. Unfortunately, the employee had written down the two passwords required to access the laptop's information on a Post-it note stored in the computer's case.

The laptop contained a total of six Labour Force Survey and Canadian Community Health Survey cases. The labour surveys contained contact information, household information, rent, employment and income and demographic information, while the health surveys contained highly sensitive personal information including height, weight, sleep patterns, sexual behaviours, chronic conditions, stress, use of tobacco and alcohol, illicit drug use and mental health information.

The employee immediately reported the theft to police. Statistics Canada officials visited each of the affected households and informed the residents that their personal information had been compromised.

The department addressed the issue in an appropriate manner with the employee whose laptop was stolen. The department also sent out a newsletter to all field employees reminding them of their obligations to secure laptops and control the use of their passwords, user identification, and computer accounts. Our Office was satisfied with the measures implemented by Statistics Canada.

Human error compromises taxpayers' information

After using the Canada Revenue Agency's telephone service to inquire about information related to his Registered Retirement Savings Plan, an individual received an envelope containing the Notices of Assessment of nine other taxpayers.

The man called the agency to report the problem, but had trouble communicating with the telephone agent. He asked to speak to a supervisor, but was initially refused. A supervisor called back, asking him to return the documents. The man was left with

the impression that the agency was not taking the matter seriously and contacted two television stations.

Camera crews recorded the man personally returning a Notice of Assessment to one individual who lived nearby and bringing the other documents to a Canada Revenue Agency office.

Following the incident, Canada Revenue Agency reviewed its procedures and policies involving documents prepared for faxing and mailing and made corrections. The agency also apologized to the affected taxpayers.

Our Office concluded the incident was the result of human error.

Failure to reset envelope-stuffing machine leads to privacy breach

An employee of a private company which administers the Veterans Independence Program for Veterans Affairs Canada forgot to reset an automated envelope stuffing machine, a mistake which meant 122 cheques were double-stuffed into 61 envelopes.

The company investigated the incident and put in place a new quality assurance system. It now documents the number of cheques handled each day and it reconciles the number of cheques printed against the number of envelopes prior to their mail-out. Any discrepancies in the numbers will result in immediate investigation and correction. In addition, it implemented a policy whereby it now individually stuffs envelopes containing reimbursement cheques.

Veterans Affairs Canada telephoned the affected veterans to check on the status of their cheques, and the company sent out apology letters. Cheques were either redirected to the proper recipients or new cheques were issued.

Our Office reviewed Veterans Affairs' report on this incident and was satisfied with the action it took to notify the affected individuals and the measures it implemented to ensure that this type of error isn't repeated.

Public Interest Disclosures under the *Privacy Act*

When there is a compelling public interest that outweighs an individual's personal privacy, the heads of government institutions may, under the *Privacy Act*, use their discretion to disclose personal information without an individual's consent.

Unless the situation that arises is an emergency, institutions disclosing personal information in the public interest must notify the Privacy Commissioner in advance.

After reviewing the proposed disclosure, the Commissioner may, if she deems it necessary, notify an individual of the release of his or her personal information. The OPC will also recommend ways to minimize the amount of personal information being disclosed if we feel a department's proposal to release personal information goes beyond the public interest.

In 2007-2008, our Office reviewed 83 public interest disclosure notices. Most were from the RCMP and involved high-risk offenders being released from prison and who police believed were a danger to the community. In other instances, the RCMP released personal information to the public in order to locate suspects or provide a warning about the actions of a violent or sexual offender.

In other cases, the Department of National Defence and Correctional Service Canada released information about the death of individuals to family members. Information about the nature of those deaths is provided for compassionate reasons.

Other Examples of Public Interest Disclosures

Tuberculosis scare prompts identification of passenger

The Department of Foreign Affairs and International Trade informed our Office it had released to the Public Health Agency of Canada the identities and contact information for 27 people who had been seated close to an airline passenger with infectious tuberculosis for more than eight hours during an international flight.

The Public Health Agency was then able to contact passengers from the flight to advise them of the need to be tested for tuberculosis.

In this case, the disclosure in the public interest clearly outweighed any potential invasion of an individual's privacy.

Auditor General identifies Quebec's Lieutenant Governor's misuse of funds

The Office of the Auditor General of Canada informed our Office that it intended to release personal information about the Lieutenant Governor of Quebec's improper use of federal public funds.

The Auditor General based her decision on the opinion that releasing the information was in the public interest. Our Office concluded no further action was necessary.

Military Ombudsman releases report about Canadian Forces snipers

The office of the National Defence and Canadian Forces Ombudsman informed our Office that it intended to release a report entitled: *A Sniper's Battle – A Father's Concern – An Investigation into the Treatment of a Canadian Forces Sniper Deployed to Afghanistan in 2002 – Special Report to the Minister of National Defence and the Chief of the National Defence Staff*.

The report concerned allegations made by the father of one of six officers in a sniper unit. He alleged the officers were ostracized, treated unfairly, denied stress debriefings and subjected to unfounded criminal and other investigations.

Two individuals named in the report consented to the release of their personal information. The Ombudsman believed it was possible to identify other individuals mentioned, but not named. However, he believed that disclosing the report was in the public interest and outweighed any invasion of privacy.

The Ombudsman's office notified four people about the report's impending release and gave them each a copy. The OPC reviewed the matter and recommended the Ombudsman's Office inform the two other individuals about the report's release and the possibility they could be identified. The Ombudsman's office agreed.

Complaints Commission report reveals personal information

The Military Police Complaints Commission is an independent federal body that oversees and reviews complaints of conduct of members of the Military Police.

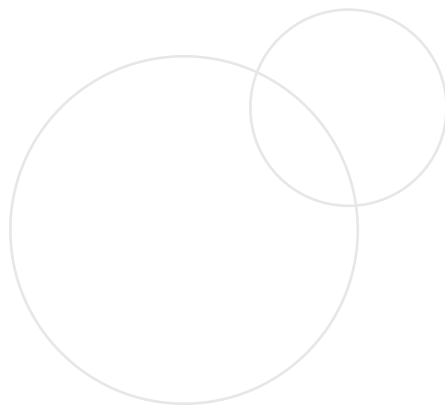
The Complaints Commission received a complaint from a member of a sniper unit deployed to Afghanistan expressing concern about the conduct of the Military Police. The Commission investigated the allegations made against the Military Police and notified the OPC that it intended to disclose personal information contained in its report by posting it on its website. The Complaints Commission argued the report contained information crucial to the public interest.

The Commission had determined the allegations against military police officers were unfounded.

The complainants, the members of the Military Police, the Minister of National Defence and other departmental officials received copies of the report before it was posted, and were told it would be made public. Other individuals named in the report as having been interviewed during the investigation were not notified.

The OPC recommended that the Commission consider notifying the interviewees of its intention to render the report public. We also recommended that the Commission depersonalize the report to protect the identities of the parties and interviewees.

OTHER OPC ACTIVITIES



AUDIT AND REVIEW

Our Office's audit work resulted in our first special report to Parliament this year. Problems uncovered during an audit of the RCMP's exempt data banks raised such significant concerns that the Commissioner decided to present the findings in a special report tabled in February 2008.

We also completed a comprehensive examination of passport operations. (See page 15.)

Other issues our Audit and Review branch worked on over 2007-2008 included the government's purchase of personal information from data brokers and the widespread use of Social Insurance Numbers.

We also conducted reviews of Privacy Impact Assessments for new federal initiatives, offering hundreds of recommendations to help protect Canadians' privacy.

RCMP Exempt Databanks – A Special Report to Parliament

An OPC audit found the RCMP's exempt data banks, which shelter national security and criminal intelligence files from public access, have been crowded with tens of thousands of records that should not have been there. This conclusion is particularly disturbing given that the RCMP was advised of compliance problems 20 years ago and made a commitment to properly manage such banks.

Exempt data banks serve to withhold the most sensitive national security and criminal intelligence information. Departments and agencies controlling such records will refuse to confirm or deny the existence of information in response to requests for access.

People whose names appear in the RCMP's exempt data banks could be at risk of harmful impacts. For example, they could have trouble obtaining an employment security clearance or crossing the border.

More than half of the files examined as part of our audit did not belong in the exempt banks. To illustrate, one seven-year-old file in the national security exempt bank detailed a resident's tip that a man had gone into a rooming house and drugs might be involved. Police investigated, but found the man had simply dropped his daughter off at a nearby school and stepped out of his car to smoke.

The Privacy Commissioner was satisfied the RCMP was taking her recommendations seriously and would take action to ensure its exempt banks comply with the *Privacy Act* and RCMP policy. Our Office will conduct a post-audit.

The complete audit report is available on the OPC website.

Project Shock

The RCMP's National Security Investigations Records exempt bank includes records related to "Project Shock" – the effort to coordinate tips related to the 9-11 terrorist attacks.

We examined a sample of records in 2002 and found tips generally related to suspected terrorist affiliations, suspicious persons or suspicious activity. However, some tips seemed to amount to little more than public hysteria during a time of crisis.

While these files were not part of our exempt bank audit, we asked questions in order to verify that each tip file had undergone an assessment to determine whether it warranted continued exempt bank status.

As we reported in our special report, a subsequent RCMP review of the Project Shock file, which contained records that touch on thousands of Canadians, found the records did not meet the criteria for continued inclusion in the national security exempt bank and were removed.

Data Mining and the Public Sector

Concerns about how data brokers collect, use and disclose personal information have been on our radar screen for a number of years. As well, privacy concerns have been highlighted in a number of studies and high-profile incidents involving data brokers.

In late 2006, the *Ottawa Citizen* published an article describing how the RCMP had been buying and storing personal information from commercial data brokers for a number of years. This revelation raised questions not only about how the RCMP was using the information, but also about whether other government departments were purchasing data broker information.

Data brokers collect and analyze personal information – for example, financial, credit or health information – for the purpose of developing and selling data products, often to marketers. From a privacy perspective, we have concerns about the accuracy of this kind of data as well as the possibility that incorrect assumptions about individuals may be drawn.

The RCMP advised our Office that it has contractual agreements with a number of data brokers which provide commercial reports for public and private companies, and contact information (address and telephone numbers) for consumers and businesses.

The extent of data broker use within the RCMP varies depending on the mandate of the operational unit. For example, RCMP Commercial Crime Units may prepare economic profiles on individuals and companies in the course of bankruptcy investigations.

The RCMP told us that information from data brokers complements the force's intelligence and investigative work, and is only considered as a secondary source of information of unknown relevance, accuracy and reliability. We understand no action is undertaken solely on the basis of such information.

Our Office also conducted a limited survey to assess the use of data brokers by other federal government departments. We concluded the use of data brokers does not appear to be widespread.

Treasury Board Secretariat has told us that it will consider the data broker issue as it reviews the Treasury Board Privacy Impact Assessment Policy, which is scheduled to be completed by April 2009.

Use of Social Insurance Numbers

A senior citizen wrote to the Privacy Commissioner in June 2007 to express concern about the inclusion of Social Insurance Numbers on Old Age Security identification cards. The citizen pointed out that this was forcing older Canadians to reveal sensitive personal information each time they used the card to obtain privileges such as seniors' discounts.

The letter prompted our Office to contact Human Resources and Social Development Canada to raise the concerns. A few months later, the department informed us that Social Insurance Numbers would no longer be printed on the cards.

This Social Insurance Number was created in 1964 to serve as a client account number for the Canada Pension Plan and various employment insurance programs. In 1967, what is now Canada Revenue Agency (CRA) started using Social Insurance Numbers for tax reporting purposes.

A recent OPC study found that over 70 federal departments and agencies use Social Insurance Numbers in one way or another. Meanwhile, approximately 170 pieces of provincial legislation deal with uses of Social Insurance Numbers.

Despite the efforts of governments, our Office, other privacy commissioners, privacy advocates and citizens to limit the use of Social Insurance Numbers, over many years, the use of this number has snowballed to the point where many see it as a *de facto* common client identifier, if not a national identifier.

At the same time, there is no legislated privacy protection related to the use of Social Insurance Numbers. This is a significant concern given that a Social Insurance Number is a key piece of information to unlock the door to an individual's personal information. For example, identity thieves use it to apply for credit cards and open bank accounts.

Treasury Board Secretariat recently issued a new policy governing the use of Social Insurance Numbers and whether this helps curtail the use of this number remains to be seen.

Privacy Impact Assessment Reviews

Privacy Impact Assessments (PIAs) are an important privacy management tool to help federal government institutions identify and mitigate privacy risks before implementing programs.

PIAs – which are mandated by Treasury Board Secretariat policy – are meant to help departments focus on privacy as a core consideration when implementing new programs and initiatives. Our Office believes PIAs should be mandated under the *Privacy Act*. (See page 44 for more detailed information.)

The OPC's Audit and Review Branch reviews submitted PIAs to evaluate the privacy risks of government programs and services, and offers advice where appropriate. In this way, the OPC can ensure that privacy safeguards are built in to programs and systems.

PIAs by the Numbers	
New PIAs sent to the OPC for review	60
PIAs reviewed and letters of recommendation sent to departments (includes PIAs received in prior years)	78
Recommendations made by OPC to departments	434
Requests made to departments for information missing from PIAs	239

Our Office was pleased to note that, increasingly, departments are inviting OPC officials to early consultation meetings during – or even before – the PIA development stage. This allows the OPC to provide ideas on best practices and offer early alerts about the privacy risks related to new programs and initiatives.

A key branch priority in 2007-2008 was to reduce a PIA review backlog. Over the year, the backlog of files waiting for review was significantly reduced from 50 files to 18.

We reviewed 78 PIAs for a wide range of government programs and initiatives. Some of these were for controversial and high-profile projects, such as Transport Canada's no-fly list and Canada Border Service Agency's Enhanced Driver's Licence initiative. Our Office also reviewed the privacy risks of lesser-known initiatives: a new benefits program for veterans; the recording of phone calls at Canada's ports; and the process for handling passport applications at Service Canada locations.

In most cases, we uncover privacy risks and make recommendations. Our advice is usually taken seriously.

Examples of Privacy Impact Assessment Reviews

Transport Canada – Passenger Protect Program (No-fly List)

While our Office continues to have significant concerns about the inherent privacy risks stemming from the no-fly list, our review of Transport Canada's PIA of the program did result in some improvements.

For example, in response to the OPC's recommendations, Transport Canada put in place our suggestions for passenger recourse; an audit of the program's effectiveness; confidentiality provisions in memoranda of understanding; and standard operating procedures for RCMP and CSIS to guide their actions when someone is denied boarding.

However, a recommendation that the personal information of individuals who are denied boarding not be shared with local police forces was not fully implemented.

Similarly, our proposal that the Passenger Protect Program, as well as other watch lists, be referred to a Parliamentary committee for review in an open and transparent forum was rejected.

Statistics Canada - Canada Health Measures Survey

Our review of the Canada Health Measures Survey – a national survey that will collect information from Canadians about their general health and lifestyles – initially recommended against the planned storage of survey participants' samples of blood, urine and DNA for unlimited lengths of time, to be used for unspecified future research.

Our Office felt this practice would render participants' consent to the collection of their samples somewhat meaningless.

The OPC recommended Statistics Canada store the biological samples, identified only by anonymous code, for a specific period of time, not exceeding 20 years. We also recommended the survey should not include the option of long-term storage for biological specimens from young respondents (aged 6 to 13 years) where consent was to be provided by a parent or guardian.

Statistics Canada decided to go ahead with the indefinite storage plan. It proposed that an oversight committee of interested parties such as the OPC could review the ways in which stored specimens may be used in the future. The plan to store children's biological samples will also proceed; however, those individuals will be contacted after their 14th birthdays to obtain explicit consent.

RCMP / Public Safety Canada – National Integrated Information Initiative

The National Integrated Information Initiative (N-III) is an electronic records-sharing program linking national, provincial and municipal police forces, with the capacity to expand access and sharing capabilities to federal government departments.

The initiative is a partnership involving the RCMP, Public Safety Canada and a number of departments and agencies such as the Canada Border Services Agency, Citizenship and Immigration Canada, the Canadian Firearms Centre, Correctional Service of Canada and the National Parole Board.

Given the significant number of institutions involved, the OPC asked Public Safety Canada to develop an over-arching PIA which would include a privacy management framework with measurable standards and limitations for all government agencies accessing and sharing information through systems, such as the Police Information Portal.

We had hoped such a PIA would: outline the overall business case defining and justifying the need for the proposed increased information sharing; articulate a Public Safety commitment to protect personal information; set measurable standards against which audits for compliance within each portfolio department could be accomplished; and include a communications strategy for informing Canadians about how the program may lead to their personal information being shared with a number of government institutions.

A year after the request was made, we have yet to receive an over-arching PIA, although our Office was informed in the spring of 2008 that work on a broad assessment had begun.

Canada Border Services Agency – Enhanced Drivers' Licences

Our Office has been working with the British Columbia Information and Privacy Commissioner during our review of the Enhanced Drivers' License (EDL) pilot project between British Columbia and Washington State. Canada Border Services Agency is encouraging and helping to coordinate the B.C. pilot as well as EDL projects in other provinces.

EDLs are being proposed as an alternative to a Canadian passport for travellers entering the United States at land borders. They are a response to new U.S. government rules requiring documentation of identity and citizenship.

Under the B.C. pilot, Canada Border Services Agency collects applicants' personal information from the province and transfers it to U.S. Customs and Border Protection.

Concerns raised during our PIA review include the duplication of personal information and data verification processes which already exist at Passport Canada. Other concerns include: unclear legislative authority for citizenship verification; meaningful consent; potential uses of personal information by the U.S. government; the use of EDLs for other purposes; and privacy risks related to the use of radio frequency identification (RFID) chips.

The OPC has pressed Canada Border Services Agency for assurances that subsequent EDL projects will not proceed on a permanent basis unless drivers' personal information remains in Canada, and that EDL information will only be used for crossing the border. While the way in which personal information will be disclosed to U.S. authorities was still under discussion as we prepared this report, Canada Border Services Agency has said the database itself will remain in Canada.

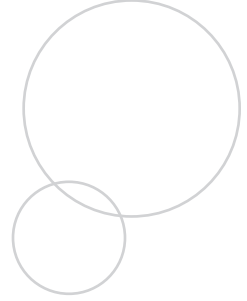
IN THE COURTS

As in previous years, there were only a few court applications proceeding under the *Privacy Act* in 2007-2008.

Under section 41 of the *Privacy Act*, the Federal Court may only review a government institution's refusal to grant access to personal information requested under the *Act*.

A section 41 application may *not* be made for wrongful collection, use or disclosure of an individual's personal information by a government institution.

Under section 41 of the *Privacy Act*, the Federal Court may only review a government institution's refusal to grant access to personal information requested under the *Act*.



Our Office has called on the federal government to broaden the grounds for which an application for court review under section 41 may be made to include the full array of privacy rights and protections under the *Privacy Act*. We also recommended giving the Federal Court the power to award damages against offending institutions.

Until the *Act* is amended, there will continue to be only a small number of court applications proceeding under the legislation.

The following cases of interest were before the Federal Court during 2007-2008.

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

X. v. Office of the Privacy Commissioner of Canada
Federal Court File T-1903-07

The Applicant filed a complaint against the Canadian Security Intelligence Service (CSIS) for failing to provide requested personal information. The Privacy Commissioner found the complaint was not well-founded.

The Applicant sought judicial review of the Privacy Commissioner's findings pursuant to section 41 of the *Act*. However, the purpose of a section 41 application is to ask the Court to determine whether the government institution against whom a complaint was filed respected the applicable provisions of the *Act* in refusing to provide access to personal information sought by the complainant. Section 41 does not provide for recourse against the Privacy Commissioner.

Mr. Justice Blanchard ruled that it is well established that the Privacy Commissioner has no decision-making authority and her findings and recommendations following an investigation under the *Act* are not binding on the government institution.

He also noted it is clear under the *Act* that it is not the Privacy Commissioner who is called upon to justify a refusal. That responsibility rests with the government institution refusing to grant access to requested personal information.

The Court therefore allowed the Privacy Commissioner's motion, ordering that the application proceed only on condition that the Applicant file an amended application directed at CSIS. The Applicant filed an amended application in March 2008.

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

X. v. The Minister of Health Canada

Federal Court File No.: T-347-06

As reported in the 2006-2007 annual report, the Privacy Commissioner was granted intervener status in a case filed under the *Access to Information Act* which raises important privacy issues. Our Office was concerned about the possible re-identification of individuals when government information is combined with publicly available information.

The Applicant, a CBC producer, had sought access to Health Canada's Canadian Adverse Drug Reaction Information System – a database containing information relating to suspected adverse reactions to health products marketed in Canada.

In response to his request, Health Canada released some information, but refused to reveal the provinces in which data about adverse drug reactions had been collected on the grounds that it constituted personal information under the *Privacy Act*.

In a February 2008 decision, Mr. Justice Gibson accepted a fundamental premise set out by the Supreme Court of Canada: In a situation involving personal information about an individual, the right to privacy is paramount over the right of access to information.

He also adopted the legal test proposed by our Office: "Information will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information."

Based on the evidence before him, Justice Gibson concluded that disclosure of the province would substantially increase the possibility that an individual could be identified based on the totality of data-fields already disclosed from the drug reaction

database, combined with other publicly available information, such as obituary notices. This is particularly the case for unique or quasi-unique individual reports, in smaller provinces or territories.

Therefore, in the circumstances, the province field does constitute personal information and was properly exempt from access.

Also of note, the judge emphasized the importance of ministerial discretion in deciding whether or not to exceptionally release this personal information in the public interest. In this case, the Minister had properly considered the facts before him and decided that, here, the public interest in disclosure did not clearly outweigh the violation of privacy that could result from the disclosure.

ACCESS TO INFORMATION AND PRIVACY UNIT

Our Office has now completed one full fiscal year subject to both the *Access to Information Act* and the *Privacy Act*. (The *Federal Accountability Act* extended both of these pieces of legislation so that they would cover our Office.)

We received 44 formal requests under the *Access to Information Act*. Fourteen of those requests were transferred to government institutions which had control of the records being sought, and we responded to 29 requests for access to information in our Office. One other request was carried over. All *Access to Information Act* requests were responded to within the statutory time frames.

Our Office received five complaints from two people under the *Access to Information Act* – three alleged denial of access and two concerned response time. The Information Commissioner concluded two access complaints were “not substantiated” and the third was “resolved.” The Information Commissioner further concluded that one time complaint was “not substantiated” and the other was “resolved.”

Our Office received 45 requests for personal information under the *Privacy Act*. We redirected 23 requests to government institutions which had the information being sought, and we responded to 22 requests for access to OPC information. All *Privacy Act* requests were responded to within the statutory time frames set out in the *Act*.

The OPC received two complaints under the *Privacy Act* from one individual alleging denial of access. The complaints were addressed under an arms-length process and were determined to be “not well-founded” in April 2008.

The *Federal Accountability Act* does not include a mechanism under which *Privacy Act* complaints against our Office would be investigated. Given the fact it would be entirely inappropriate for our Office to investigate its own actions with respect

to its administration of the *Privacy Act*, we have created the position of “Privacy Commissioner ad hoc” to conduct such investigations.

In September 2007, the Honourable Mr. Justice Peter Cory was engaged as Privacy Commissioner ad hoc. The Privacy Commissioner delegated to him the majority of her powers, duties and functions as set out in sections 29 through 35 and section 42 of the *Act*. Justice Cory completed his contract in March 2008. A new Privacy Commissioner ad hoc, Justice Andrew Mackay, has since assumed these duties.

A substantial number of the requests we have received under both the *Access to Information Act* and the *Privacy Act* were for the contents of our investigation files. In a few cases, all file information was withheld as required by the *Access to Information Act* and the *Privacy Act* because the investigation or court proceedings were ongoing. Where an investigation was fully concluded, the file information was processed and access was granted subject to relevant exemptions.

INTERNATIONAL CONFERENCE

As reported in our 2007 PIPEDA Annual Report, the success of the 29th International Conference of Data Protection and Privacy Commissioners – held in Montreal in September and following through on our initial 2002 engagement – was beyond our highest expectations.

We welcomed more than 600 commissioners, academics, privacy professionals, advocates, government officials, IT specialists and others from around the globe – making it the largest-ever conference of its kind. Most importantly, the positive reviews and kudos from participants justified the time and resources invested in this event.

The conference theme was Privacy Horizons: *Terra Incognita*. Early cartographers marked unknown lands that had yet to be mapped with this Latin term. One of the earliest known terrestrial globes from Europe labels an uncharted edge of the ocean “*hic sunt dracones*” – or “here be dragons.”

This notion of an unknown landscape with lurking dragons seemed the perfect metaphor for the future of privacy. Privacy issues are changing rapidly, with powerful new technologies and the international war on terror acting as potent forces which threaten the privacy of people around the world.

The goal of our conference was to begin to chart what the privacy world of the future might look like and also to equip privacy advocates with some strong dragon-slaying tools. During a series of plenaries, workshops and information sessions, we considered the best strategies for defending privacy rights in the face of constant change.

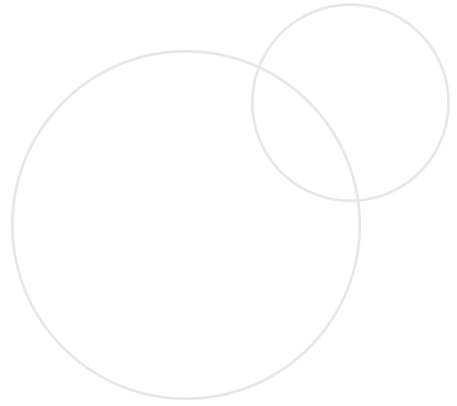
Participants heard from the who's who of the privacy world, including security technology guru and author Bruce Schneier; Simon Davies, a pioneer of the international privacy arena and founder of Privacy International; consumer privacy advocate Katherine Albrecht; Marc Rotenberg, executive director of the Electronic Privacy Information Center; Peter Fleischer, Google's global privacy counsel; Peter Hustinx, the European Data Protection Supervisor; as well as Peter Schaar, now past-chair of the EU Article 29 Data Protection Working Party and France's Alex Türk, who is now chair of the working party. Our guest of honour, who opened the conference, was the Honourable Peter Milliken, Speaker of the House of Commons.

The conference program underscored the wide range of issues which will have an impact on privacy in the coming years as well as the increasingly global nature of privacy issues.

We prepared 14 workbooks before the conference. Most included a commissioned paper by a subject-matter expert and a variety of other resources, such as research and bibliographical materials, to satisfy the curiosity of participants who might be new to a particular subject, as well as the more rigorous requirements of key policy and decision-makers to locate trustworthy information about the privacy implications of our conference topics. These are available on our conference website at www.privacyconference2007.gc.ca and are an important legacy of the conference.

We have posted details about the cost of the conference on our website. We stayed well within our overall financial targets.

THE YEAR AHEAD



The list of issues our Office deals with on a daily basis will always be a lengthy one. In an effort to focus our efforts on the most significant threats to the privacy of Canadians, we have identified four top strategic priorities: information technology, national security, identity integrity and protection, and genetic information.

A key objective for our Office over 2008-2009 will be to **provide leadership on our priority issues**. Our plans to address these privacy threats include the following steps:

- **Information Technology**
 - Build sufficient capacity to assess the privacy impact of new information technologies.
 - Increase public awareness of technologies with potential privacy impacts.
 - Provide practical guidance to organizations on the implementation of specific technologies.
- **National Security**
 - Ensure national security initiatives adequately protect privacy.
 - Ensure proper oversight and accountability of national security agencies' personal information management practices.
 - Raise public awareness of the privacy impacts of national security initiatives.
- **Identity Integrity and Protection / Identity Theft**
 - Improve organizations' personal information management practices.
 - Raise public awareness of identity protection.
 - Advocate for a coordinated federal government approach to identity protection.

- **Genetic Information**

- Advance research and knowledge to address new challenges posed by genetics in the context of traditional data protection regimes.
- Raise public awareness about the potential uses of genetic information.

Our Office has identified four other major corporate priorities. They are:

- Continue to **improve service delivery** through focus and innovation, including new investigative strategies to make our complaints resolution process more efficient;
- **Build a sustainable organizational capacity** by growing our Office and continuing an information management renewal project;
- **Support Canadians** to make informed privacy decisions with expanded public education initiatives such as a social marketing campaign on children's online privacy and outreach programs in partnership with provincial and territorial privacy commissioners; and
- Strategically **advance global privacy protection for Canadians** through work with organizations such as the OECD and APEC.

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 uses or disclosures without consent set out in sections 7 and 8 of the *Act*.

Time Limits:

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

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

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

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

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

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

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

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

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

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

APPENDIX 2

INVESTIGATION PROCESS UNDER THE *PRIVACY ACT*

Inquiry:

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



Initial analysis:

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

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



Complaint?



No:

The individual is advised, for example, that the matter is not in our jurisdiction.



Yes:

An investigator is assigned to the case.



Early resolution?

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



Investigation:

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

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



Analysis (on next page)



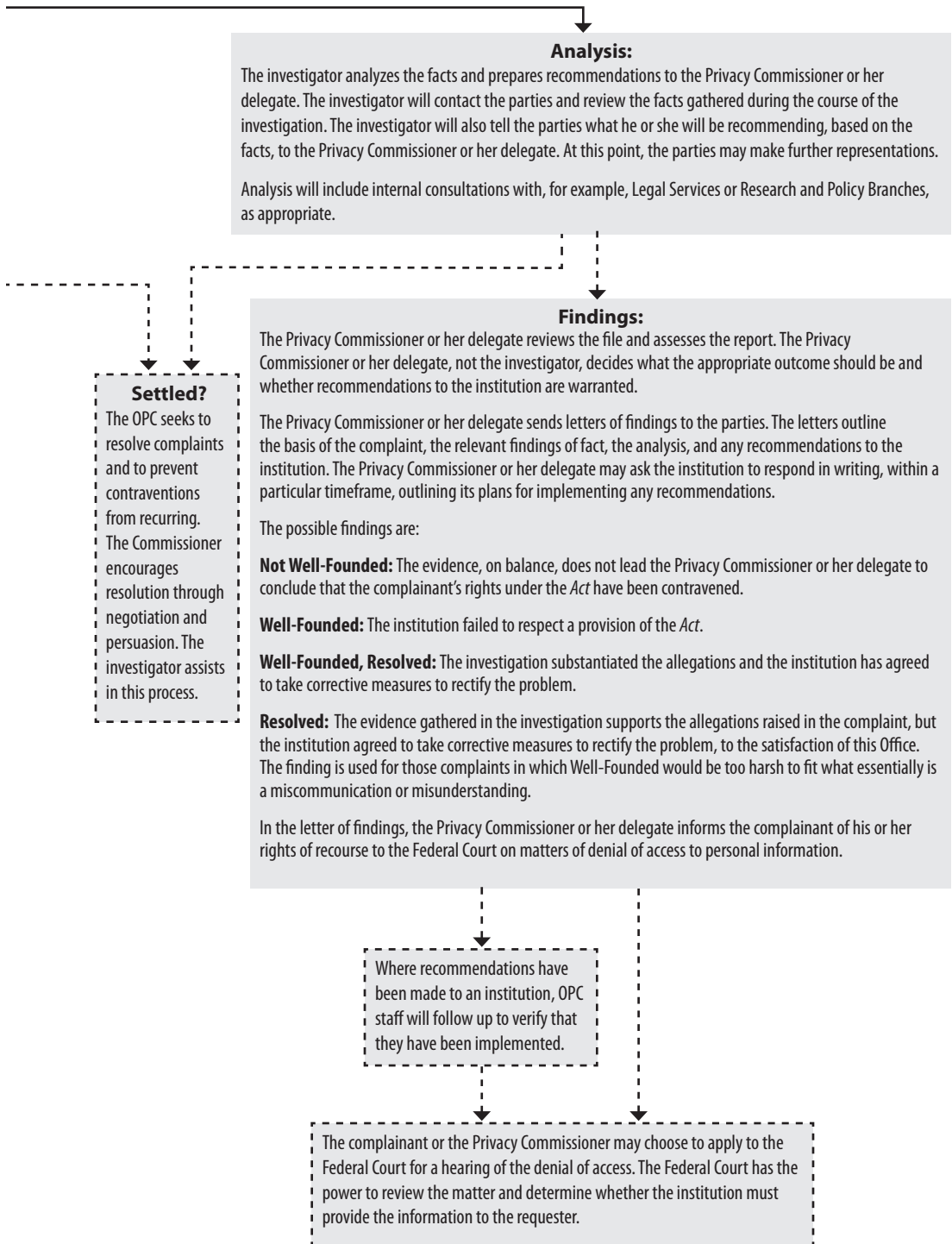
Discontinued?

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



Settled? (on next page)

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



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

APPENDIX 3

PRIVACY ACT INQUIRY, COMPLAINT AND INVESTIGATION STATISTICS FOR 2007-2008

Inquiries

Our Inquiries Unit received well over 4,000 *Privacy Act*-related inquiries between April 1, 2007 and March 31, 2008.

Some of the most frequently raised issues included ways in which to make formal requests for access to personal information; how to file complaints against government institutions that, for example, exceed statutory time limits and fail to comply with the *Privacy Act*. We also received inquiries from individuals seeking advice from our Office as a result of being affected by various privacy breaches.

Privacy Act inquiries received by the Inquiries Unit

Telephone inquiries	2,199
Written inquiries (letter, e-mail, fax)	2,059
Total number of inquiries received	4,258

Privacy Act inquiries closed

Telephone inquiries	2,221
Written inquiries (letter, e-mail, fax)	1,901
Total number of inquiries closed	4,122

General inquiries received *

Telephone inquiries	2,231
Written inquiries (letter, e-mail, fax)	136
Total number of inquiries received	2,367

General inquiries closed

Telephone inquiries	2,229
Written inquiries (letter, e-mail, fax)	140
Total number of inquiries closed	2,369

*These are inquiries related to privacy issues, but cannot be linked to either Act.

Complaints Received by Type

Complaint Type	Count	Percentage
Access	292	38
Time Limits	259	34
Use and Disclosure	124	16
Collection	33	4
Correction-Time Limits	26	3
Extension Notice	10	1
Retention and Disposal	9	1
Correction-Notation	5	1
Language	1	< 1
Total	759	

As in previous years, the most common complaints to our Office related to both access to personal information as well as the length of time government departments and agencies take to respond to access requests.

See Appendix 1 for definitions of complaint types.

Top Ten Institutions by Complaints Received

	Total	Access to Personal Information	Time Limits	Privacy
Correctional Service Canada	248	48	151	49
Royal Canadian Mounted Police	84	59	14	11
Canada Border Services Agency	54	18	31	5
Service Canada	52	13	14	25
National Defence	48	17	19	12
Canadian Security Intelligence Service	45	44	0	1
Canada Revenue Agency	38	18	9	11
Canada Post Corporation	28	16	8	4
Foreign Affairs and International Trade	27	6	7	14
Justice Canada	18	4	13	1
Others	117	49	29	39
Total	759	292	295	172

Some institutions – because of their mandate – hold a substantial amount of personal information and are more likely to receive numerous requests for access to that information and subsequent complaints.

See Appendix 1 for definitions of complaint types.

Complaints Received by Institution

	Total
Correctional Service Canada	248
Royal Canadian Mounted Police	84
Canada Border Services Agency	54
Service Canada	52
National Defence	48
Canadian Security Intelligence Service	45
Canada Revenue Agency	38
Canada Post Corporation	28
Foreign Affairs and International Trade Canada	27
Justice Canada	18
Human Resources and Social Development Canada	14
Citizenship and Immigration Canada	14
Health Canada	8
Transport Canada	7
Public Works and Government Services Canada	6
Fisheries and Oceans	5
Library and Archives Canada	5
Privy Council Office	5
Agriculture and Agri-Food Canada	4
Canadian Food Inspection Agency	4
Indian and Northern Affairs Canada	4
Treasury Board of Canada Secretariat	4
Commission for Public Complaints Against the RCMP	3
Environment Canada	3
Public Service Commission Canada	3
Canada Firearms Centre	2
Canada Mortgage and Housing Corporation	2
Canada Public Service Agency	2
Ombudsman National Defence and Canadian Forces	2
Canadian Broadcasting Corporation	1
Canadian Forces Grievance Board	1
Canadian Human Rights Agency	1
Canadian Transportation Agency	1
Correctional Investigator Canada	1
Export Development Corporation	1
Financial Transactions and Reports Analysis Centre of Canada	1
Immigration and Refugee Board	1
Industry Canada	1
Inspector General of the Canadian Security Intelligence Service, Office of the	1
National Museum of Science and Technology	1
National Parole Board	1
Natural Resources Canada	1
Pension Appeals Board Canada	1
Public Safety Canada	1
Public Service Labour Relations Board	1
Public Service Staffing Tribunal	1
Royal Canadian Mint	1
Statistics Canada	1
Veteran Affairs Canada	1
Total	759

Complaints Received by Province/Territory

	Total	Percentage
Ontario	195	26
British Columbia	179	23
NCR	112	15
Quebec	65	8
Alberta	60	8
Saskatchewan	44	6
Nova Scotia	28	4
Manitoba	26	3
International *	22	3
New Brunswick	15	2
Newfoundland	5	1
Prince Edward Island	4	1
Nunavut	3	<1
Yukon Territory	1	<1
Total	759	

* Canadians living abroad have the same access and privacy protection rights under the *Privacy Act* as those living in Canada, including the right to complain to this Office. Some of these Canadians living abroad have chosen to exercise those rights. (Note: the privacy protection rights, but not access rights, are also available to all individuals of any citizenship or country of residence.)

We have seen one significant change in the geographical distribution of complaints over the last few years: There has been a sharp drop in the number of Quebec complaints, which accounted for 24 per cent of total complaints in 2005-2006; 14 per cent in 2006-2007; and just 8 per cent in 2007-2008. While we can't be certain about the precise reason for this decrease, we are aware that Quebec has its own stringent privacy legislation. Most of our complainants living in Quebec who use our services, are located in the National Capital Region.

Closed Complaints by Finding

Finding	Count	Percentage
Early Resolution	32	4
Settled	114	13
Well-founded Resolved	17	2
Resolved	6	< 1
Well-founded	319	36
Not Well-founded	275	31
Discontinued	117	13
Total	880	

Roughly one in five of our closed complaints resulted in solutions that satisfied complainants, respondents and our Office – with an Early Resolution, Settled, Well-founded Resolved or Resolved finding. A significant number of closed complaints – more than one third – were well founded, which suggests that there is room for improvement in privacy management practices.

Findings by Complaint Type

Complaints (All Types) Closed

	Discontinued	Early Resolution	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Well-founded/Resolved	Total
Access	56	4	180	5	59	2	12	318
Time Limits	14	18	23	0	3	243	0	301
Use and Disclosure	32	4	51	1	31	42	3	164
Collection	6	5	11	0	11	0	0	33
Correction- Time Limits	3	1	0	0	5	22	0	31
Extension Notice	1	0	3	0	0	10	0	14
Retention and Disposal	3	0	4	0	4	0	1	12
Correction- Notation	2	0	3	0	1	0	1	7
Total	117	32	275	6	114	319	17	880

This table shows varying characteristics by Complaint Type. For instance, by their very nature, most Time Limits are well-founded; most individuals do not complain to us until the statutory deadline has passed. Seventy-five per cent of Access cases are either not well-founded or settled, meaning that the exemptions were properly claimed and/or individuals were satisfied with the explanation given of the reasons for exemptions or missing documentation. Interestingly, no Collection complaints were well-founded. This indicates several possible things: that the collection of personal information was indeed necessary and reasonable for the program or activity of the government institution;

that the individuals understood an explanation/rationale for the collection; or that discussions with the organizations were successful in reaching some compromise that was acceptable to both parties.

Access and Privacy Complaints Closed

	Discontinued	Early Resolution	Settled in course of investigation	Not well-founded	Well-founded	Well-founded-Resolved	Resolved	Total
Access	56	4	59	180	2	12	5	318
Use and Disclosure	32	4	31	51	42	3	1	164
Collection	6	5	11	11	0	0	0	33
Retention and Disposal	3	0	4	4	0	1	0	12
Correction-Notation	2	0	1	3	0	1	0	7
Total	99	13	106	249	44	17	6	534

As in previous years, not well-founded complaints outweigh those complaints that are well-founded. In addition, a number of complaints have been concluded using alternate resolution mechanisms, as is demonstrated by the number of settled complaints and early resolution findings.

See Appendix 1 for definitions of findings and other dispositions under the *Privacy Act*.

Time Limits Complaints Closed

	Discontinued	Early Resolution	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Well-founded/Resolved	Total
Time Limits	14	18	23	0	3	243	0	301
Correction- Time Limits	3	1	0	0	5	22	0	31
Extension Notice	1	0	3	0	0	10	0	14
Total	18	19	26	0	8	275	0	346

By their very nature, the majority of time limits complaints are well-founded. The requirements for federal departments and agencies are clear: They have 30 days to respond to requests for access to personal information. Some time limits complaints are not well-founded because the organization has appropriately applied an extension notice, which allows for an additional 30 days to respond.

Time Limits Complaints Closed by Institution and Finding

As indicated in the following table, Correctional Services Canada has, by far, the highest number of Time Limits complaints. This is a reflection of the large volume of personal information it holds on inmates and the large number of requests it receives from that population. That institution recently received a significant increase in resources to address the volume. Likewise, National Defence, Canada Border Services Agency, the RCMP and the Canada Revenue Agency all have significant holdings of personal information and therefore face significant challenges in responding in a timely fashion to the high volume of requests they receive, with the resources they have available.

	Discontinued	Early Resolution	Not well-founded	Settled in course of investigation	Well-founded	Total
Correctional Service Canada	5	14	3	6	146	174
National Defence	2	0	0	0	26	28
Canada Border Services Agency	1	0	1	0	25	27
Royal Canadian Mounted Police	4	1	1	0	15	21
Canada Revenue Agency	0	0	3	1	14	18
Justice Canada	0	0	0	0	13	13
Service Canada	3	0	1	0	6	10
Canadian Security Intelligence Service	0	0	8	0	0	8
Foreign Affairs and International Trade Canada	0	0	0	0	8	8
Canada Post Corporation	0	2	0	0	3	5
Citizenship and Immigration Canada	0	0	0	0	5	5
Human Resources and Social Development Canada	1	0	2	0	2	5
Canada Firearms Centre	0	0	3	0	0	3
Privy Council Office	1	0	0	0	2	3
Public Works and Government Services Canada	0	0	0	0	3	3
Agriculture and Agri-Food Canada	0	0	2	0	0	2
Health Canada	0	0	0	0	2	2
Indian and Northern Affairs Canada	0	0	0	0	2	2
Library and Archives Canada	1	1	0	0	0	2
Correctional Investigator Canada, Office of the	0	1	0	0	0	1
Environment Canada	0	0	0	0	1	1
Export Development Corporation	0	0	0	0	1	1
Fisheries and Oceans	0	0	0	0	1	1
Inspector General of the Canadian Security Intelligence Service, Office of the	0	0	1	0	0	1
Public Safety Canada	0	0	0	1	0	1
Treasury Board of Canada Secretariat	0	0	1	0	0	1
Total	18	19	26	8	275	346

The increase in the number of well-founded time limit complaints can be directly attributed to the increase in requests institutions receive and the limited resources available to them. This trend affects the majority of government institutions.

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	26	1	39	2	21	21	4	114
Canada Revenue Agency	9	1	41	0	11	6	1	69
Immigration and Refugee Board	0	0	58	0	0	0	0	58
Royal Canadian Mounted Police	11	2	24	1	9	3	2	52
Citizenship and Immigration Canada	7	1	16	0	11	0	0	35
National Defence	10	1	9	0	3	2	1	26
Canada Post Corporation	8	1	4	1	10	0	0	24
Human Resources and Social Development Canada	11	1	5	0	2	1	2	22
Service Canada	3	1	7	1	7	2	1	22
Canada Border Services Agency	2	0	5	1	4	2	1	15
Foreign Affairs and International Trade Canada	1	1	6	0	2	4	0	14
Justice Canada, Department of	2	0	4	0	2	1	1	10
Fisheries and Oceans	0	0	0	0	7	0	0	7
National Parole Board	1	0	1	0	2	0	2	6
Canadian Security Intelligence Service	0	0	5	0	0	0	0	5
Health Canada	0	1	2	0	2	0	0	5
Indian and Northern Affairs Canada	1	0	1	0	3	0	0	5
Environment Canada	0	0	4	0	0	0	0	4
Library and Archives Canada	2	0	0	0	2	0	0	4
Statistics Canada	1	1	1	0	1	0	0	4
Transport Canada	2	0	2	0	0	0	0	4
Canadian Human Rights Commission	1	0	1	0	0	0	1	3
Freshwater Fish Marketing Corporation	0	0	0	0	3	0	0	3
Public Service Commission Canada	0	0	2	0	1	0	0	3
Canada School for Public Service	0	0	2	0	0	0	0	2
Privy Council Office	0	0	1	0	0	1	0	2
Public Safety Canada	0	0	0	0	2	0	0	2

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
Public Works and Government Services Canada	0	0	0	0	1	1	0	2
Treasury Board of Canada Secretariat	0	0	2	0	0	0	0	2
Agriculture and Agri-Food Canada	0	0	1	0	0	0	0	1
Canadian Air Transport Security Authority	0	0	1	0	0	0	0	1
Canadian Food Inspection Agency	0	0	1	0	0	0	0	1
Canadian Space Agency	0	0	1	0	0	0	0	1
Canadian Transportation Agency	1	0	0	0	0	0	0	1
Export Development Corporation	0	0	0	0	0	0	1	1
Industry Canada	0	1	0	0	0	0	0	1
Inspector General of the Canadian Security Intelligence Service, Office of the	0	0	1	0	0	0	0	1
Office of the Chief Electoral Officer	0	0	1	0	0	0	0	1
Veterans Affairs Canada	0	0	1	0	0	0	0	1
Total	99	13	249	6	106	44	17	534

Complaint Investigations Treatment Times - *Privacy Act*

Treatment times are the average number of months to complete a complaint investigation, from the date the complaint is received to when a finding is made.

By Finding

Disposition	Average Treatment Time in Months
Early Resolution	6.25
Well-founded	6.32
Resolved	16.17
Discontinued	16.57
Settled in the Course of Investigation	17.87
Not Well-founded	21.67
Well-founded Resolved	27.24
Overall Average	14.45

The significant difference between treatment times for well-founded complaints and not well-founded complaints arises from Time Limits complaints. They represent 34 per cent of our caseload, the majority of which are well-founded, and the majority of which are closed relatively quickly compared to other types of complaints.

By Complaint Type

Complaint Type	Average Treatment Time in Months
Time Limits	4.58
Extension Notice	6.07
Correction/Time Limit	7.10
Correction/Notation	13.14 *
Collection	16.09
Use and Disclosure	18.68
Access	22.14
Overall Average	14.40

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

