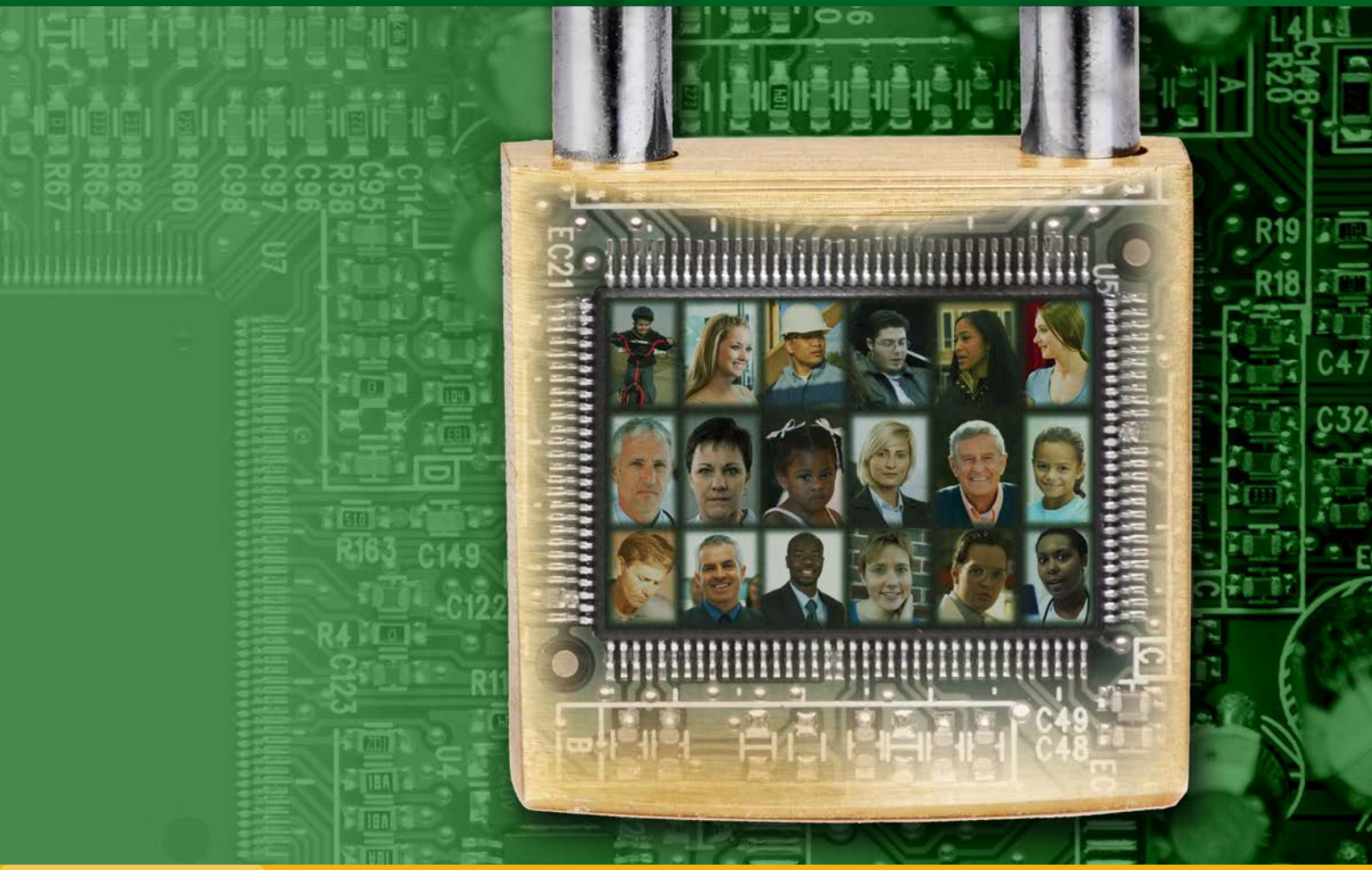
Office of the
Privacy Commissioner
of Canada

Securing the right to privacy



Annual Report to Parliament 2012-2013

Report on the *Privacy Act*

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

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

Cat. No. IP50-2013E-PDF
1913-7540

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

Follow us on Twitter: @PrivacyPrivee

Privacy Commissioner of Canada

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

Commissaire à la protection de la vie privée du Canada

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

October 2013

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

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Privacy Act* for the period of April 1, 2012, to March 31, 2013. This tabling is pursuant to section 38 of the *Privacy Act*.

Yours sincerely,

Original signed by

Jennifer Stoddart
Privacy Commissioner of Canada

Privacy Commissioner of Canada

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

Commissaire à la protection de la vie privée du Canada

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

October 2013

The Honourable Andrew Scheer, M.P.
The Speaker
The House of Commons
Ottawa, Ontario K1A 0A6

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Privacy Act* for the period of April 1, 2012, to March 31, 2013. This tabling is pursuant to section 38 of the *Privacy Act*.

Yours sincerely,

Original signed by

Jennifer Stoddart
Privacy Commissioner of Canada

Table of Contents

1.0 Commissioner's Message 1
1.1 THE YEAR IN REVIEW - Key Accomplishments during 2012-2013 5
1.2 Privacy by the numbers in 2012-2013 8

2.0 Moving to vulnerable information technology: A time of mounting privacy risks 11
2.1 Continued vulnerability: Managing the risks that remain with information technology 12
2.2 Royal Canadian Mounted Police disclosure of wiretap information 13
2.3 Correctional Service of Canada 13
2.4 Data breach reports 14
2.5 Loss of USB key at Human Resources and Skills Development Canada and Department of Justice Canada 16
2.6 Hard drive loss involves over half a million student loan borrowers 16
2.7 Immediate follow-ups 17
2.8 Financial Transactions and Reports Analysis Centre of Canada records, encrypted laptop, and USB key stolen from vehicle 17
2.9 Correctional Service of Canada unencrypted USB key lost and recovered in schoolyard 18

3.0 Handle with care: a call for respect amidst new incidents of unauthorized access and collection. 19
3.1 An Audit of the Canada Revenue Agency 20
3.2 Aboriginal Affairs and Northern Development Canada wrongly collects information from First Nations activist's personal Facebook page 26
3.3 Criminal background check on tenant 28
3.4 Estranged wife accessed husband's medical records 29
3.5 Canada Revenue Agency employee accesses tax file without authorization 29
3.6 National Defence employee accesses someone's personal health records for her own personal reasons 30

4.0 Justice delayed is justice denied: Persistent delays by federal institutions in responding to individual access requests and complaint investigations by our Office 31
4.1 Royal Canadian Mounted Police 32
4.2 Delays in responding to access requests 33

5.0 Private and safe: Securing the right to privacy amidst the quest for stronger public safety 35
5.1 An audit of Financial Transactions and Reports Analysis Centre of Canada 36
5.2 Privacy and the pursuit of perimeter security 42
5.3 Canada-United States Entry/Exit System 43
5.4 Customs Controlled Areas 44
5.5 Immigration Information Sharing Treaty 44
5.6 Temporary Resident Biometrics Project 45

Table of Contents

5.7 Global Visa Application Centres 46
5.8 Another round on lawful access 46
5.9 Emergency wiretapping—C-55 48
5.10 Federal use of unmanned aerial vehicles 49
5.11 Information about airline passengers—C-45 50

6.0 The OPC in Action 53
6.1 Privacy Impact Assessment Reviews 53
6.1.1 Canada Border Services Agency - Personnel Security Screening Standard 54
6.1.2 Audio Surveillance at Ports of Entry 55
6.1.3 Treasury Board of Canada Secretariat - Standard on Privacy and Web Analytics 55
6.1.4 Shared Services Canada - GCKey Authentication 56
6.1.5 Citizenship and Immigration Canada - Global Case Management System 57
6.1.6 Following up—Canadian Air Transport Security Authority and Full Body Scanners 57
6.1.7 Encouraging Compliance - Signage for video surveillance on Parliament Hill 57
6.2 Action through investigations 58
6.2.1 Denial was the starting point for Correctional Service of Canada 58
6.2.2 Correctional Service of Canada initially denies access to full report in favour of giving the "gist" 59
6.2.3 Royal Canadian Mounted Police revealed absolute discharge 60
6.2.4 Concern rasied over online disclosure - The Qalipu Mi'kmaq First Nation Band 60
6.2.5 Intake 61
6.2.6 Complaints 61
6.2.7 Early Resolution 62
6.2.8 Modernizing the Investigative Process 63
6.2.9 Investigations and dispositions - By the numbers 64
6.3 Audits 66
6.3.1 Disposal audit 67
6.3.2 Wireless audit 68
6.4 Inquiries 70
6.5 Supporting Parliament 70
6.5.1 Financial Accountability and Transparency of First Nations 71
6.5.2 *Income Tax Act* Requirements for Labour Organisations 72
6.6 Outreach 73
6.6.1 Privacy Impact Assessment Workshop 73
6.6.2 Access to Information and Privacy outreach 73
6.6.3 Speeches and presentations 74

6.7 Research 74
6.7.1 Facial recognition 75
6.7.2 Predictive analytics 75
6.7.3 Unmanned aerial vehicles 75
6.8 Guidance 76
6.8.1 A Privacy Emergency Kit 76
6.8.2 Privacy Breach Management Toolkit for health information 76
6.9 Action before the courts 77
6.9.1 *X. v. Privacy Commissioner of Canada* 77
6.9.2 *X. v. Privacy Commissioner of Canada* 77
6.9.3 *Privacy Commissioner of Canada v. Royal Canadian Mounted Police* 77
6.9.4 *X. v. The Privacy Commissioner of Canada* 78
6.9.5 *X. v. Her Majesty in Right of Canada, et al* 78
6.10 Public Interest Disclosures Under Section 8(2)(*m*) of *Privacy Act* 78
6.10.1 Royal Canadian Mounted Police 79
6.10.2 Passport Canada 79
6.10.3 Canada Border Services Agency 79
6.10.4 Correctional Service of Canada 79
6.10.5 Human Resources and Skills Development Canada 79

7.0 THE YEAR AHEAD 81
7.1 Mandatory data breach notification 81
7.2 Updating the *Privacy Act* 82
7.3 Surveillance, online and offline 82
7.4 Blurring OPC and departmental responsibilities 83
7.5 Lack of notification 83
7.6 Macro-projects, micro-review 83
7.7 Sharing everything 84
7.8 Consolidation of services and outsourcing 84
7.9 Security screening in the federal government 85
7.10 Other areas 85

Appendix 1 86

Appendix 2 90

1.0 Commissioner's Message

Securing the right to privacy: outlining the government's duty of care

In introducing my final Annual Report as Privacy Commissioner, one focused on securing the right to privacy, I want to underscore the critical importance of government's responsibility to collect only the information necessary to govern, as justified in a free and democratic society and to handle the personal information of Canadians with utmost respect.

This is not just a custodial role. It is about a relationship between citizen and state where fundamental freedoms may only be curtailed in a manner that is demonstrably justified and where the citizen's trust is honoured.

Canadians surrender their personal information to government out of necessity, often under legal compulsion. And in fact, the efficient delivery of important government services requires as much. In return, people justly expect that the government will exercise effective stewardship over such information.

Growing public concern

It is clear, however, that many Canadians have their doubts about whether this is the case. In fact, in a national telephone survey conducted for our Office in 2012-13, only 21% of Canadians said that they felt that governments take their responsibility to protect personal information seriously. While the result for the same question about businesses in the private sector yielded even greater scepticism (only 13% felt businesses take their responsibilities seriously), it is a disheartening result.

More generally, the survey also found that two-thirds of Canadians are concerned about the protection of their privacy. One-quarter indicated that they were "extremely" concerned. They are questioning their own ability to protect their personal information—56% are not confident that they understand how new technologies affect their privacy—and we have seen this lack of confidence increase steadily since the year 2000.

Canadians' growing unease about privacy protection is not surprising. New technologies are emerging and spreading rapidly, many of them fuelled by innovative and extensive uses of personal information that can be difficult, if not impossible, for individuals to fully comprehend. They are also being inundated by requests for more and more personal information; while at the same time they are hearing, frequently, about significant data breaches and leaks of personal information.

Examples that breed distrust

This Annual Report, unfortunately, offers numerous examples from the public sector of the types of issues that are heightening Canadians' general privacy concerns, while eroding their trust in the federal departments and agencies that collect their personal information.

For example, an audit of the Canada Revenue Agency (CRA), which routinely handles Canadians' sensitive financial data, found many instances of employees making unauthorized accesses to taxpayer files. Many of these breaches went undetected for a period of several years.

There is also evidence of increased delays in response times to requests for personal information under the *Privacy Act*, and response times to our Office on investigations and other matters.

For the third year in a row, the number of data breaches reported to our Office has reached an all-time high. Among the breaches noted in this report is the loss of a hard drive containing personal details of more than 500,000 student loan recipients.

This upward trend in data breaches could point to a higher level of data loss by institutions, or it could simply show greater diligence by departments in meeting their reporting obligations. Even in the latter and best case scenario, Canadians would be justified in demanding that greater diligence be paid to information handling practices in order to avoid breaches in the first place.

Other examples of note in this report include the unwarranted collection of personal information by two federal departments from a First Nations activist's personal Facebook page; the misuse of a Canadian Forces member's confidential health records by an estranged spouse; and the use of a law enforcement database by a landlord working as a Royal Canadian Mounted Police employee by day to check on a prospective tenant.

A decade of change

While our Office has reported similar transgressions during my decade as Commissioner, the ever-expanding use of technology is having a significant impact on the issues we are seeing. As the federal government strives to modernize its services and its workplace processes and tools, the collection, storage and sharing of personal information digitally will inevitably increase.

Innovation is essential, and it can offer many benefits, but it can also introduce vulnerabilities. The government must ensure that privacy policies

and procedures evolve accordingly. We should never forget the human values and individual decisions that technology aims to support. Privacy protection is rooted in a concern for the autonomy, dignity and integrity of the very citizens governments exist to serve; it's not data security for its own sake.

Along with significant advancements in technology, this past decade has seen a global quest to strengthen national security and public safety. During my time as Commissioner, our Office has sought to make clear that neither security nor privacy is an absolute and one should not be ignored or traded away in pursuit of the other.

In 2011, the Canadian and U.S. governments agreed on moving forward with a series of initiatives designed to facilitate trade and increase security, many of which involve greater information sharing between the countries about people's movements. Given the privacy implications involved, our Office has committed to keeping a keen eye on new programs as they develop and we share some key insights in this report.

Accountability is vital

While this report brings to light threats to personal information protection coupled with the privacy risks of certain initiatives by government institutions in the name of public safety, there are numerous other examples that demonstrate the government has not exercised the standard of care over personal information in its control which Canadians have every right to expect.

Departments and agencies have unparalleled access to people's most personal information, and this makes accountability all the more vital. Unless federal institutions are seen to be vigorously enforcing privacy protection, Canadians will doubt whether their personal information is secure. Similarly, if institutions continue to drag out the process of providing citizens with access to their personal information or the task of working with our Office in response to complaints, fundamental questions begin to arise regarding the adequacy of Canada's privacy regime.

The government's continued lack of action on introducing amendments to modernize the *Privacy Act* is also troubling. While the Act has been, and continues to be, effective at setting the ground rules for how federal government departments and agencies handle personal information, the world has changed dramatically since it was introduced over 30 years ago. Along with advances in technology, Canadians' concerns and expectations have moved forward, bringing healthy pressure to bear upon government and citizens. In order to maintain legitimacy, credibility and trust, the government's stewardship of personal information needs to respond in kind, and I firmly believe that updating the *Privacy Act* would not only modernize the law but also send a strong signal to public servants and citizens that the federal government takes its responsibility to protect personal information seriously.

Concluding with confidence

With my term as Commissioner coming to a close, I regret that I will not bear witness to the modernization of the *Privacy Act* during my mandate. I take great pride however in knowing that the work our Office has done has led to demonstrable improvements across the federal government when it comes to securing the right to privacy. While this report highlights many shortcomings in the information handling practices of federal institutions, I would note that I have also seen many sound privacy programs introduced and encouraging improvements in privacy practices during my term. I have also encountered innumerable public servants dedicated to the task of ensuring Canadians' privacy rights are respected.

As I move on to new challenges, I would like to specifically acknowledge the exceptionally dedicated and professional staff members of this Office who have supported me throughout my mandate. I feel very privileged and honoured to have worked with such a committed group of individuals, and I have every confidence that they will continue to advance the effort to defend Canadians' rights to privacy and the sanctity of their personal information as this Office transitions to new leadership.

Jennifer Stoddart
Privacy Commissioner of Canada

1.1 THE YEAR IN REVIEW

Key accomplishments during 2012-13

This section offers a quick overview of what our Office did during the past fiscal year to safeguard and strengthen the privacy rights of Canadians in their dealings with the federal government.

Privacy compliance audits

We conducted audits of the Canada Revenue Agency (CRA) and of the Financial Transactions and Reports Analysis Centre (FINTRAC).

The CRA audit, described in detail in Chapter 3, was prompted by repeated instances of egregious privacy breaches at the Agency, some involving multiple disclosures of taxpayer files which had continued undetected for years.

We found that, although the Agency has robust privacy policies and practices, serious weaknesses nonetheless exist in the implementation and monitoring of those measures.

In all, we made 14 recommendations to CRA related to: privacy breach management; employee access and monitoring; information technology security; and privacy management and accountability. The Agency accepted all of our recommendations and has responded with a concrete action plan and timetable to implement improvements. We will follow up on CRA's commitments in two years to ensure that all changes promised are fully implemented.

In Chapter 5, we describe our audit of FINTRAC which must be carried out every two years under a provision in the legislation governing that institution.

We found that FINTRAC had made limited progress in dealing with five of the 10 recommendations from our previous audit in 2009. We again recommended that these continuing issues be addressed.

FINTRAC continues to receive and retain personal information that is not directly related to its operating programs or activities, and which it does not need or use. Until this is addressed, there will be a discrepancy between FINTRAC's practice and its obligations under the *Privacy Act*.

Information requests and complaints

Forming part of the front line of the Office of the Privacy Commissioner of Canada is the Information Centre which responds to requests from individuals and organisations about privacy rights and responsibilities. In 2012-13 we received close to 10,000 requests, with over a quarter relating to the federal public sector.

This is almost double the number of information requests about federal privacy concerns received during the previous fiscal year, underlining the importance of this service to Canadians. Contributing to this record level was a groundswell

of concern expressed about some major data breaches that occurred this past year.

We also saw an increase in multiple complaints from the same complainant—251 complaints in the past fiscal year came from 18 individuals who each lodged eight or more complaints. Also reaching unprecedented heights were complaints about delays in which institutions responded to individual access requests outside the legislated time limits.

On the plus side, an increasing proportion of complaints are being successfully dealt with through negotiation and conciliation. This early resolution approach accounted for a third of our closed files in the past fiscal year, up from a quarter in the previous year.

Data breaches

Yet another record was set in 2012-13 in the number of data breaches which federal institutions reported to our Office, with 109 incidents representing an increase of more than a third from the previous year. As always, because departments and agencies are not required to notify our Office of breaches, it is impossible to discern whether the rise was attributable to more actual breaches or increased diligence in reporting.

Privacy Impact Assessments (PIAs)

Federal government institutions are required to assess the privacy impact of activities and initiatives that involve personal information. By completing a PIA, an organisation can identify potential privacy risks tied to a planned activity and explain how they will be mitigated.

We received 68 new PIAs in 2012-13, with many related to programs being implemented under the Canada-U.S. Beyond the Border Action Plan (see Chapter 5).

We assessed 21 of these as having the potential of being particularly privacy intrusive and made detailed and comprehensive recommendations for improvements. Some of these are highlighted in Chapter 6.

Policy and parliamentary affairs

During 2012-13, our Office appeared nine times before parliamentary committees and provided two written submissions. We conducted in-depth analyses of eight bills and three committee studies on privacy relevant topics, such as the rising use of social media. Our Office also continued to monitor several other legislative initiatives with potential privacy implications.

The government's omnibus budget bill (Bill C-45) raised several potential privacy issues as it extended border security measures affecting travellers to and from Canada. Another significant piece of legislation considered by Parliament was Bill C-55, which clarified the circumstances and legal controls put in place for the use of warrantless interceptions of electronic communication by police in emergencies.

We also made representations about privacy ramifications in two bills about financial transparency—Bill C-27 for First Nations and Bill C-377 for unions.

Reaching out to federal institutions

A vital part of our public sector work is outreach to federal institutions that fall under the authority of the *Privacy Act*. Examples of our outreach during the fiscal year included hosting the fourth annual Privacy Impact Assessment (PIA) workshop for public servants, which focused on information technology privacy and security and on PIAs involving multiple institutions. We also used this event to launch our new PIA video, designed to help federal departments and agencies meet the demands of the Treasury Board Secretariat Directive on PIAs, while reinforcing the expectations of our Office.

At another event, our Office discussed our initiatives to modernize OPC investigation processes with the officials responsible for Access to Information and Privacy (ATIP) units in 12 federal institutions which have traditionally been the subject of a higher than average number of privacy complaints.

In marking Data Privacy Day (January 28, 2013), our Office produced and distributed posters featuring our popular privacy-themed editorial cartoons to ATIP coordinators and other privacy and security professionals in the federal government.

Advancing knowledge

The rapidly evolving privacy environment, driven in part by the brisk pace of technological change, makes it essential for OPC specialists to be on the cutting edge of relevant research.

This past fiscal year, for example, we prepared research reports on facial recognition technology, predictive analytics, what an Internet Protocol address can reveal about a user and the privacy implications of unmanned aerial vehicles.

In addition our Office worked with some of our provincial counterparts to develop a Privacy Emergency Kit to help enable communications during emergencies while also respecting the need to protect personal information.

1.2 PRIVACY BY THE NUMBERS IN 2012-2013

Information requests

Related to the *Privacy Act*	**2,599**
Related to the *Personal Information Protection and Electronic Documents Act* (PIPEDA)	4,349
Not related exclusively to either Act	2,940
Total	**9,888**

Privacy Act* complaints

***Privacy Act* complaints 2012-2013**	
Category	**Total**
Accepted	
Access	378
Time limits	437
Privacy	1,458[1]
Total	**2,273**
Closed through formal resolution	
Access	107
Time limits	114
Privacy	78
Total	**299**
Closed through investigation	
Access	256
Time limits	234
Privacy	118
Total	**609**
Total closed	**908**

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

[1] This number includes 1,159 Human Resources and Skills Development Canada (now named Employment and Social Development Canada) breach-related complaints accepted in fiscal year 2012 2013.

Privacy Impact Assessment reviews

Received	**68**
Reviewed as high risk	21
Reviewed as lower risk	19
Total reviewed	**40**

Audits

Public sector audits tabled in Parliament	1

Policy and parliamentary affairs

Draft bills and legislation affecting the federal public sector reviewed for privacy implications	8
Public-sector policies or initiatives reviewed for privacy implications	51
Parliamentary committee appearances on public-sector matters	9
Submissions to Parliament	2
Other interactions with Parliamentarians or staff (for example, correspondence with MPs or Senators)	52

Communications activities *

Speeches and presentations	88
News releases and communications tools	27
Exhibits and other offsite promotional activities	29
Publications distributed	29,446
Visits to principal OPC website	2.1 million
Visits to OPC blogs and other websites	1.1 million

* Combined statistics for public and private sector initiatives

Requests to the OPC under the *Access to Information Act*

Requests received	**50**
Requests closed	56

Requests to the OPC under the *Privacy Act*

Requests received	**17**
Requests closed	15

2.0 Moving to vulnerable information technology:
A time of mounting privacy risks

Canadians are becoming increasingly sensitive about how their government collects and uses their personal information. In a telephone survey carried out for our Office in October through November 2012 among 1,513 adult residents of Canada, two-thirds said they were concerned about the protection of their privacy. One-quarter indicated that they were "extremely" concerned.

As well, the survey found a growing sense among Canadians that their ability to protect their personal information is diminishing. Seven in 10 think their personal information has less protection in their daily lives than a decade ago, marking a 10 per cent increase since the same question was asked in 2011. Meanwhile, only 21% indicated that they thought the federal government takes its responsibility to protect citizens' personal information very seriously.

The level of public concern over privacy almost certainly ratcheted higher in January. That's when Human Resources and Skills Development Canada (HRSDC)[2] stated that it had lost a hard drive that contained the personal information of more than half a million clients of the Canada Student Loans Program. Once notified of this breach, our Office launched an investigation, and at the time of writing this Annual Report, the investigation was still underway.

Massive data breaches like the lost hard drive are an example of the privacy vulnerabilities of modern information technology. The rise in such vulnerabilities is one of the four trends that our Office sees driving the mounting sensitivity of Canadians to federal government handling of their personal information. Some specific cases are explored in this chapter.

[2] Human Resources and Skills Development Canada (HRSDC) has since been renamed Employment and Social Development Canada; however, for the purposes of this report, we refer to the department by its name at the time of the breach incidents and throughout the reporting period.

A second trend contributing to the mounting public unease is inappropriate access by government officials to personal information, which is spotlighted in Chapter 3.

Next comes evidence of increasing delays with which some government agencies and departments are meeting requests for personal information under the *Privacy Act*. In some cases, we are also seeing increased delays in response times to our Office on investigations and other matters, a disturbing trend which is documented in Chapter 4.

The fourth trend may ultimately prove the most intractable. It is the continuing erosion of the privacy of Canadians because of the ever-increasing demands for personal information made in the name of national security, both domestically and internationally. Chapter 5 deals extensively with this.

Despite these four disturbing trends, the federal privacy picture is not entirely gloomy. As we also note in the following chapters, some federal institutions have made progress in handling requests under the *Privacy Act* in a timelier way despite dealing with an increasing volume without a commensurate increase in resources.

As well, in the privacy-sensitive realm of web analytics our Office has benefitted from commendable co-operation and collaboration from key players such as Shared Services Canada and the Treasury Board of Canada Secretariat.

2.1 CONTINUED VULNERABILITY: MANAGING THE RISKS THAT REMAIN WITH INFORMATION TECHNOLOGY

The social benefits that come with technology have left citizens in a paradoxical position. We have greater access to information about government than ever before, but each new electronic device or service seems to create new privacy risks. On one hand, the vast amount of personal information held by federal departments and agencies ensures that, by and large, Canadians receive efficient service for everything from Canada Pension Plan (CPP) payments to income tax refunds. The efficiencies come about because the databases are comprehensive and widely accessible within government organisations, and public services are instantly available online.

On the other hand, the uptake in data collection also magnifies the potential chaos that can be wrought by either human error or deliberate misuse.

Investigations by our Office over the past fiscal year found that information technology vulnerability was often combined with other factors in cases where the personal information of Canadians was not treated with due respect by federal institutions.

Topping things off, the past year marked the third year in a row that we have seen an all-time high in data breaches reported to our Office by federal institutions. These include two incidents reported

by HRSDC, in which a USB key holding sensitive personal information, including social insurance numbers and medical conditions of more than 5,000 people, and a hard drive with personal information of over 500,000 student loan recipients and 250 departmental employees were lost.

2.2 ROYAL CANADIAN MOUNTED POLICE DISCLOSURE OF WIRETAP INFORMATION

Another case of information technology vulnerability contributing to an erosion of privacy appears in Chapter 4. The 32-month investigation, which also serves as an example of delays in responding to our Office, centred on the unjustified disclosure by the Royal Canadian Mounted Police (RCMP) to another government agency of personal information obtained through a judicially authorized wiretap.

The information concerned an Agency employee whose conversation was recorded when he was in telephone contact with a second individual who was the designated target of a wiretap operated by a municipal police force. The municipal force disclosed the wiretap information to the RCMP where the Agency employee was enrolled in a cadet training program.

The RCMP ejected the cadet from the program and turned the wiretap information over to his employer in contravention of the *Criminal Code* and, therefore, also in contravention of the *Privacy Act*. The Agency then dismissed the individual.

2.3 CORRECTIONAL SERVICE OF CANADA

A third example of such vulnerabilities centres on the Correctional Service of Canada's (CSC) handling of the Offender Management System (OMS).

OMS is a computerized case file management system used by CSC and other criminal justice partners to manage information on federal offenders throughout their sentences. The system gathers, stores, and retrieves information required for tracking offenders and making decisions concerning their cases.

Personal information about offenders in the OMS includes, amongst other data, criminal histories and psychological evaluations.

A former inmate of a maximum-security penitentiary complained to our Office that his OMS file had been inappropriately accessed and some of his personal information given to the media without his consent.

Our investigation found that 98 individuals had accessed the complainant's OMS file during almost five months following his release from the institution, a time period specified in his complaint. Two of those individuals, both employees of the penitentiary, accessed the complainant's OMS file for reasons that could not be justified as being an operational need-to-know.

One employee acknowledged looking at the file out of curiosity. The other said he needed more information about the complainant for his own personal safety and that of his family.

In addition to these instances of inappropriate access, our investigation also revealed several shortcomings in the overall management of the OMS.

For example, CSC has no current policies or procedures that address the responsibilities of supervisors and managers to report inappropriate accesses to the OMS. Furthermore, the organisation does not have security measures in place to regularly monitor access and detect potential abuses of the system.

While a need to upgrade and update the OMS is recognized within CSC, no timeline has been set for the initial review.

We found the complaint about inappropriate access to be **well founded**. However we found no evidence that the two employees actually disclosed the personal information that appeared in the media.

2.4 DATA BREACH REPORTS

This past year we received a significant increase in the number of data breaches reported to our Office. Either there has been a jump in actual data breaches at federal departments and agencies for the third consecutive year, or institutions are becoming more diligent in reporting such incidents.

Since the reporting of data breaches is voluntary under current legislation, it is not possible to say definitively how much each factor is driving the numbers, which are up to 109 in the current fiscal year from 80 in the previous.

Federal public sector data breaches reported to the OPC

2008-09	26
2009-10	38
2010-11	64
2011-12	80
2012-2013	109

The scope, complexity and potential impact of many of these reported breaches also escalated, requiring greater time, resources and effort from our Office in carrying out the appropriate follow-ups.

A data breach occurs when there is loss or disclosure of personal information. Whether or not affected individuals are informed about a breach depends on its level of significance. Notably however, in this

year's two major incidents reported by HRSDC, hundreds of thousands of affected individuals were notified. Many filed complaints with our Office.

Under the Treasury Board of Canada Secretariat's guidelines, departments and agencies are encouraged—but not required—to report all significant data breaches to our Office in a timely fashion. Six federal institutions accounted for almost two-thirds of total reported data breaches (See Table).

Public Sector Data Breaches Reported to the OPC for 2012-2013

Department/Agency	Number of breaches reported
Canada Revenue Agency	22
Correctional Service of Canada	17
Human Resources and Skills Development Canada	11
Foreign Affairs and International Trade[3]	10
Veterans Affairs Canada	5
Citizenship and Immigration Canada	5
Canada Post	4
Statistics Canada	4
National Defence	3
Other departments/agencies	28
Total	**109**

As in previous years, accidental disclosure was the largest category of data breaches this year, with 57 breaches caused predominately by human error.

Unauthorized access to personal information or the unauthorized sharing of documents accounted for 13 breaches. Another 31 breaches could be assigned to the loss of documents, including six involving the loss of passports at Canadian embassies.

Theft was the cause of eight breaches. Laptops proved a popular target, with those breaches ranging from the personal tax information of 46 individuals to information about a dozen people whose Canada Pension Plan and Old Age Security status was being reviewed.

[3] The Department of Foreign Affairs and International Trade (DFAIT) has since been renamed the Department of Foreign Affairs, Trade and Development; however, for the purposes of this report, we refer to the department by its name throughout the reporting period.

Two data breaches drew significant media attention and led to the Privacy Commissioner initiating complaints against the Department of Justice Canada and HRSDC.

2.5 LOSS OF USB KEY AT HUMAN RESOURCES AND SKILLS DEVELOPMENT CANADA AND DEPARTMENT OF JUSTICE CANADA

Human Resources and Skills Development Canada (HRSDC) informed our Office on December 6, 2012, about the loss of a USB key which contained sensitive personal information of over 5,000 individuals who had appealed disability rulings under the Canada Pension Plan. The lost information included individuals' Social Insurance Number (SIN), name, birth date, medical condition, education level, occupation and any other agencies also making payments, such as worker's compensation.

We were also subsequently informed that the loss of the USB key involved a Department of Justice Canada lawyer working at HRSDC. On January 28, 2013, the Commissioner initiated a complaint against Justice relating to the loss of the personal information stored on the USB key.

Because the Commissioner initiated the investigation, the 163 individuals who had complained against HRSDC did not need to file new complaints against Justice to initiate a full investigation into the latter's role in the lost USB key incident. The results of the Commissioner's investigations of both departments will be made public following their completion.

2.6 HARD DRIVE LOSS INVOLVES OVER HALF A MILLION STUDENT LOAN BORROWERS

HRSDC informed our Office about the loss of an external hard drive containing the personal information of 583,000 Canada Student Loan borrowers and 250 departmental employees. The lost information included clients' SIN, name, birth date, home address, telephone number and loan balance.

The Commissioner initiated a complaint against the department on January 11. Consequently, those affected did not need to file individual complaints to initiate a full investigation. Nevertheless at the time of writing of this report, our Office has received 864 complaints arising from this breach. Following completion, the results of the Commissioner's investigation will be made public.

HRSDC has written to the approximately 310,000 loan borrowers for whom it had up-to-date and accurate contact details to notify them of the breach.

Privacy Commissioner launches investigation of Human Resources and Skills Development Canada breach of student loan recipient information.
http://www.priv.gc.ca/media/nr-c/2013/an_130111_e.asp

2.7 IMMEDIATE FOLLOW-UPS

For both breaches, HRSDC has contracted with Equifax Canada and TransUnion to provide those affected, upon consent, with free credit and identity protection services for up to six years following the incident.

Because USB keys and external hard drives are widely used in the government, our Office has decided to conduct an audit of other agencies and departments to examine their use of portable storage devices.

2.8 FINANCIAL TRANSACTIONS AND REPORTS ANALYSIS CENTRE OF CANADA RECORDS, ENCRYPTED LAPTOP, AND USB KEY STOLEN FROM VEHICLE

On October 18, 2012, in Calgary, hard copy records, an encrypted laptop and a USB key containing information in relation to Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) examinations were stolen from a vehicle rented by an Agency employee. The records were believed to include information used to identify casino patrons along with information on their financial transactions.

FINTRAC's internal investigation determined that a security procedure related to the use of USB keys was not followed in this case. With respect to the laptop, the fully protected hard drive is paired with the computer, meaning that it can only be decrypted from that laptop, and requires the use of a combination of security features in order to access information.

FINTRAC has notified those affected by this breach and is reviewing policies and procedures regarding the transportation and security of information. The FINTRAC breach investigation is ongoing.

2.9 CORRECTIONAL SERVICE OF CANADA UNENCRYPTED USB KEY LOST AND RECOVERED IN SCHOOLYARD

While dropping his child off one day, a Security Intelligence Officer employed at Matsqui Institution in Abbotsford, BC, dropped a Correctional Service of Canada (CSC) USB key in the school yard. The USB key was recovered by an employee of the school. The USB key said "CSC" on it, so the school employee returned it to a CSC employee.

Both the school employee and the CSC employee who handed the USB key into Matsqui Institution claim that they did not look at the contents of the unencrypted USB key. The device contained the personal information of 152 offenders, including data dealing with drug- and gang-related activity.

Representatives of CSC Information Technology Security committed to sending an awareness message on proper usage of USB keys to all staff in the region. We followed-up to ensure this was done and were satisfied with the action taken.

3.0 Handle with care:
A call for respect amidst new incidents of unauthorized access and collection

Canadians expect the government to safeguard from loss or unauthorized access the vast amounts of personal information that it holds.

Yet over the past fiscal year our Office has investigated some extremely serious leakages of personal information under the government's care as well as inappropriate access to personal information by public servants—some very senior—who were in positions of trust. Some of the most troublesome of these cases are recounted in this chapter.

For example, we recount the audit of an organisation accustomed to auditing others, the Canada Revenue Agency (CRA). Our audit came after years of hearing about unauthorized access of taxpayer records by CRA employees. In a sense, tax revenue is the lifeblood of the federal government, the flow of which is facilitated by personal information. In short, that personal information should be cared for with the same level of respect Canadians expect the federal government to demonstrate when handling their money.

This chapter also examines the unauthorized collection by the Departments of Aboriginal Affairs and Northern Development Canada and Justice Canada of personal information from a First Nations activist's Facebook page. Our investigation found that the personal information the departments collected had no connection to their operating programs or activities, and as a result, they crossed a line putting them in contravention of the *Privacy Act*.

3.1 AN AUDIT OF THE CANADA REVENUE AGENCY

Background

Over recent years our Office was made aware of several particularly egregious privacy breaches at the Canada Revenue Agency (CRA). Some of these breaches involved misdirected mail, lost portable devices and a misuse of email.

The most serious breaches involved employees making unauthorized accesses to multiple taxpayer files. Some of these breaches went undetected for a period of several years before being detected. In many of these cases, employees deliberately misused taxpayer information for personal reasons or financial gain. Our Office learned about a small number of these breaches from complainants, through media stories or from CRA.

The CRA is alerted to most privacy breaches by the public, other employees, third parties or from internal investigations and less so by its ongoing monitoring of employees' access to taxpayer information. Those employees found to have deliberately accessed or disclosed taxpayer information are subject to sanctions ranging from a suspension without pay to dismissal.

A breach involving an inappropriate access to—or disclosure of—sensitive taxpayer information can have serious impacts on the individual or individuals affected. In the worst case scenario, such a breach can result in identity theft, financial fraud and personal embarrassment for the affected taxpayers. Privacy breaches also have the potential to tarnish the Agency's reputation as a trusted custodian of Canadians' sensitive personal information.

In light of the issues that had come to our Office's attention, we initiated an audit of CRA in 2012 under section 37 of the *Privacy Act*. Our purpose was to assess the Agency's compliance with the fair information principles embodied in the *Privacy Act*. The audit focused on administrative and technical controls and safeguards over employee access to—and disclosure of—taxpayer information on CRA's taxpayer systems. We also reviewed the Agency's privacy accountability and risk assessment framework, including: privacy leadership; delegation of responsibilities; employee training and awareness; Privacy Impact Assessments (PIAs); and privacy breach management. Finally, we reviewed various information technology safeguards related to protecting taxpayer systems.

The "need-to-know" principle refers to limiting employees' access privileges to only the files and personal information directly related to their job description, work assignment and area of responsibility. This principle should be at the heart of any policy, practice or procedure governing employee access privileges and the exercise of those privileges.

For example, a data-entry clerk does not require the same level of system access as a tax auditor. By the same token, a tax auditor working on commercial

tax files should not regularly need access to personal income tax files.

Defining employee access privileges according to the need-to-know principle is an essential control to ensure the protection of Canadians' personal information and comply with the requirements of the *Privacy Act*. Considering the nature of CRA's vast operations, its dependence on sensitive taxpayers' personal information to carry out its mandate, and the high public expectations Canadians have for the protection of their information, we expected to find that the Agency would have strong access and monitoring controls in place to limit the number and extent of privacy breaches.

What we examined

During our 2012 audit, we interviewed employees at CRA's headquarters and Tax Centres in its four largest regions—Ontario, Pacific, Prairies and Quebec—which serve more than 80 per cent of Canadian taxpayers.

We also examined key documents, such as: the Agency's personal information, discipline and security policies and procedures; training materials; PIAs; breach investigations, threat and risk assessments, internal audits and corporate risk plans. Finally, we examined IT security controls used to assign and update access privileges, monitor employee access to sensitive taxpayer information, or otherwise used for the protection of taxpayers' information.

Why the issue is important

Since an earlier audit report of 2009, CRA has made progress in strengthening its privacy and security policies and procedures, and communicating its expectations to employees about the safeguarding of personal information. CRA's personal information record holdings are not only voluminous, but also highly sensitive. Individual taxpayer files typically contain financial, health, employment, family and identifying information. Citizens do not normally share these kinds of personal information outside of a close circle of family and friends.

The Agency has a clear mandate under the *Income Tax Act* to collect and use Canadians' information for tax administration purposes. However, it must be remembered that tax data—filed year after year—does not in fact belong to the Agency, but rather to the individual taxpayers who provided the data.

The Agency and its 40,000 employees, therefore, have an important legal and ethical duty to ensure that Canadians' personal information, entrusted to the CRA, is not inappropriately accessed, used or disclosed. This duty must be respected on a day-to-day basis and for as long as this personal information is under the Agency's legal control.

Year in, year out, the CRA collects a veritable mountain of taxpayers' information from over 27 million Canadians. This information forms the bedrock upon which our country's tax system is built. For the Canadian tax system to work as efficiently and effectively as it does today, the CRA relies on

these many millions of individual taxpayers to submit accurate, complete and timely information and to pay their taxes when due. By law, Canadians are required to file their income tax returns no later than the end of April each year. In practice, CRA relies on Canadians providing that information voluntarily—without intervention by the Agency. Ninety-one percent of Canadians filed their income taxes on time in 2012. Ninety-four per cent of individual taxpayers who owed taxes paid the amount due on time. This extraordinary level of compliance by Canadians should not be taken lightly.

To maintain citizens' invaluable and exceptional level of confidence and goodwill, it is essential that the Agency continuously strives to improve its privacy and security safeguards and reduce its risk of privacy breaches.

What we found

CRA has a culture of security and confidentiality through its integrity framework, policies, training and awareness and other initiatives. Marked weaknesses exist however in the implementation and monitoring of some of its key privacy and security policies and practices. These weaknesses impair CRA's ability to ensure that taxpayer information is as secure as it can be from inappropriate internal access, use or disclosure. Most notably:

- in spite of our recommendation stretching back to our 2009 audit, a Chief Privacy Officer (CPO) was only appointed on April 3, 2013, three days upon the completion of this audit examination. Moreover, the role of the CPO has not been fully defined to ensure Agency-wide coordination of privacy accountabilities, responsibilities and activities;
- PIAs are not always completed to assess risks prior to the implementation of program changes affecting taxpayers' personal information;
- Threat and Risk Assessments are not completed for many information technology systems that process taxpayer information, and this may result in undetected weaknesses;
- The Agency's controls to prevent, detect and quickly investigate inappropriate employee access and use of taxpayer information are limited by the lack of an automated tool to identify and flag potentially inappropriate accesses and by certain gaps in the collection of audit trail information for CRA computer systems;
- inappropriate accesses to thousands of taxpayers' files have gone undetected over an extended period of time; and
- because the Agency's ATIP Directorate is not regularly informed about many privacy breaches involving inappropriate access to and disclosure of taxpayer information, our Office is not informed and precluded from providing advice about how to avoid similar breaches in the future.

Our recommendations

Privacy accountability and management

The Agency should:

- define fully the role of the CPO and monitor the implementation of the position's mandate in terms of employee privacy awareness, privacy risk reduction and overall Agency compliance with the *Privacy Act*;
- complete, review and approve PIAs prior to the implementation of any new program or initiative that may raise privacy risks to taxpayer information; and
- ensure that its ATIP Directorate is notified of all breaches as they are discovered.

Employee access and monitoring

The Agency should:

- continue to enhance its Identity and Access Management System controls to ensure that employee access is limited to only that information required to carry out their job functions, based on the need-to-know principle;
- review existing generic user IDs[4] to determine whether they are required, authorized and controlled and delete all generic user IDs that are not in use;
- ensure that all generic user IDs are subject to established review and approval processes;
- continue to strengthen its audit logging systems and processes, and incorporate risk assessment tools to flag potentially inappropriate employee activities on its systems;
- ensure adequate measures are in place to mitigate the risks associated with developer access to taxpayer information in test environments; and
- rigorously control, track and monitor transfers of taxpayer information from operational[5] to test environments.

[4] A generic user ID is one shared by several individuals working on the same project or activity.

[5] A non-operational "test environment" is used by information technology staff to develop and test systems before they are used to process tax returns in the regular business or "operational environment".

Information technology security

The Agency should ensure that:

- its policies, practices and procedures are followed to manage local applications and adequate safeguards are used to protect the taxpayer information they contain;
- its Local Application Repository[6] is reviewed regularly for completeness, accuracy and currency; and
- follow up at each stage of the review and quality assurance processes and ensure that all local applications are approved by delegated officials before implementation.

Canada Revenue Agency management response to our recommendations

The Agency accepted all of our recommendations and has responded with a concrete action plan and timetable to improve its privacy and security protections in a number of important ways. Agency plans are also underway to improve access rights management and to more closely monitor employee access to taxpayer information. We will follow up on the CRA's commitments in two years to ensure that all changes promised have been fully implemented.

[6] A local application is software used to perform a specific information technology business function required in a local or regional location.

About the Canada Revenue Agency

The Canada Revenue Agency (CRA) is subject to the *Privacy Act* and to the privacy and security requirements of the Treasury Board of Canada Secretariat and the Government of Canada for the management and protection of Canadian taxpayers' personal information. Section 241 of the *Income Tax Act* also imposes confidentiality requirements on all Agency employees and on others who have legal access to taxpayer information. Serious breaches of confidentiality involving taxpayer information may result in an employee's dismissal.

The Agency is one of the federal government's largest institutions. It has an extremely broad and complex mandate to administer tax laws, collect taxes and distribute many social and economic financial benefits to taxpayers for the federal government and on behalf of most provinces and territories.

CRA interacts with more Canadians than any other government organisation and its operations have a significant impact on millions of individuals and businesses. It also holds one of the most extensive data banks in Canada.

In 2012, the Agency received almost 27 million individual tax returns, issued more than 34 million tax payments, sent 111 million credits and benefits payments to almost 12 million Canadians and responded to 17.7 million general calls. In that year CRA also had approximately 40,000 employees in five regions, 40 tax service offices and tax centres across Canada. Roughly two out of every three of these employees has some electronic access to taxpayer information through the Agency's various taxpayer systems.

The Agency's Commissioner and Chief Executive Officer is responsible for the day-to-day administration of, and compliance with, various pieces of legislation including the *Income Tax Act* and the *Privacy Act*. However, the Minister of National Revenue is ultimately responsible for compliance with both laws.

3.2 ABORIGINAL AFFAIRS AND NORTHERN DEVELOPMENT CANADA WRONGLY COLLECTS INFORMATION FROM FIRST NATIONS ACTIVIST'S PERSONAL FACEBOOK PAGE

It turns out that the misconception that people surrender their right to privacy by posting on Facebook is unfortunately still breeding to some degree within government circles.

Officials of Aboriginal Affairs and Northern Development Canada (AANDC) and the Department of Justice Canada put forward that very argument in defending their years-long collection of personal information posted by prominent First Nations activist Cindy Blackstock on her personal Facebook page.

But a formal investigation by our Office rejected that argument. We concluded that "the public availability of personal information on the Internet" does not "render personal information non-personal."

We recommended that both departments stop accessing personal information on Ms. Blackstock's page and other social media sites, unless they could demonstrate a direct connection to legitimate government business. We also recommended the destruction of any personal information collected previously without such a direct connection.

Finally, we recommended that both AANDC and the Department of Justice Canada develop and implement internal policies and guidelines governing the collection of personal information from social media sites by their employees and limiting it only to situations in which a direct connection exists to their operating programs or activities.

Both departments accepted these recommendations in full.

Background

Ms. Blackstock had complained to our Office that the two federal departments had contravened the *Privacy Act* by engaging in a systematic and deliberate collection of her personal information for purposes not directly related to a government operating program or activity.

The complaint specified three different activities:

- surreptitious monitoring of her public speeches and distributing detailed reports of her remarks widely within both departments;
- repeated accessing of her Indian status records in the government database, although there was no question about her Indian status; and
- repeated accessing and monitoring of her social media feeds, in particular her personal Facebook page, and distributing reports of her online postings widely within both departments.

Ms. Blackstock also contended that these privacy invasions were linked to a human rights lawsuit

against the federal government by her employer. That litigation alleged that the inequitable funding of child welfare services on reserves amounted to discrimination.

Findings

After a detailed and lengthy investigation, our Office made **no finding** on the first activity, since in this case the information from her public speeches wasn't "personal information" under the *Privacy Act*. We found the complaint about the second activity to be **not well founded** because of an absence of evidence.

However, we found the complaint based on social media monitoring to be **well founded**.

In February 2010 both departments began monitoring social media sites and feeds linked to the complainant which included Twitter, YouTube, BlogSpot, Google Alerts and three separate Facebook pages which the complainant administered.

Our investigation found that two of the Facebook pages were not personal in character but instead devoted primarily to the affairs of the First Nations organisation which employed the complainant and to a campaign to support the human rights complaint.

The third page, however, was categorized by Facebook as a "personal page" and featured information about the complainant's friends, personal views, skills and residency, which clearly constitute personal information under the *Privacy Act*.

Our investigation established that it was clear to officials in both departments that they were accessing and compiling information about the complainant personally and not just about her employer or the human rights campaign. Under the Act, restrictions on the collection of personal information apply, whether the personal information is available publicly or not.

The principle restriction is that the information so collected must be directly related to a government operating program or activity. Our investigation concluded that the personal information collected was not obviously relevant to policy development by AANDC, as the department contended, or to the human rights lawsuit with which the Department of Justice was particularly concerned.

Furthermore, the lack of transparency surrounding the collection of personal information from the complainant's Facebook page by the two federal departments would seem to violate the spirit, if not the letter, of the *Privacy Act*.

3.3 CRIMINAL BACKGROUND CHECK ON TENANT

A woman applied to rent a basement apartment in a building owned by two Royal Canadian Mounted Police (RCMP) employees. The landlords asked for personal identification so they could "look into" the people allowed into their rental suite.

In response, the woman provided her driver's licence and also that of her roommate.

Later the woman complained to our Office that the landlords had performed a background check for criminal records on her using their privileged access to the nation-wide Canadian Police Information Centre (CPIC) database.

An internal investigation by the RCMP confirmed that one of the landlords, an RCMP officer, had run a CPIC check on the prospective renter because she was from "out of town." The officer said he had done this to minimize the risks to officer safety and organisational security.

Information in the CPIC database is personal information as defined in the *Privacy Act* and therefore to be used only to satisfy a legitimate law enforcement purpose, in line with the policies and procedures governing the use of the database.

Our investigation found that the RCMP officer clearly accessed the database for personal reasons, and not for authorized operational purposes. On April 4, 2012, we informed the RCMP that the complaint was **well founded**.

In its April 30, 2012, response, the RCMP listed the remedial actions taken:

- the officer would be made aware of the gravity of the situation and the inappropriateness of his actions;
- the RCMP apologized in writing to the complainant for the violation of her privacy rights; and,
- on April 20, the RCMP issued a communiqué reminding all employees of the policies and procedures governing the use of RCMP databases, including CPIC. Communiqués were also planned to inform employees of the measures to be taken in the event of transgressions.

Our Office is satisfied with these remedial actions.

3.4 ESTRANGED WIFE ACCESSED HUSBAND'S MEDICAL RECORDS

A sergeant stationed at a Canadian Forces Base complained that his military health records had been accessed without authorization by his estranged wife, who was employed as a civilian at the Base.

The sergeant provided a copy of a report from the system audit log of the Canadian Forces Health Information Services (CFHIS) which recorded when his medical records had been accessed by his estranged wife.

National Defence (DND) confirmed that the estranged wife had accessed the sergeant's CFHIS account and deleted a physiotherapy appointment scheduled for him at the base health services centre. DND also advised our Office that the estranged wife had been observed accessing a paper physiotherapy file about the sergeant which was in a protected folder.

Because the estranged wife had been fully informed of the criteria for acceptable use of CFHIS electronic records, DND determined that she had willfully breached the department's rules and regulations. National Defence applied system restrictions automatically barring her access to the sergeant's CFHIS medical files.

The access and use of the sergeant's medical information is clearly inconsistent with the purpose for which the information was originally intended and does not meet one of the permissible uses defined in the *Privacy Act*. Therefore we upheld the complaint as **well founded**.

DND informed our Office that it has implemented new CFHIS controls to deal with improper access. The department also advised us that it is evaluating the systems and practices that apply to collection, retention, use and disclosure, as well as the overall security of CFHIS files.

3.5 CANADA REVENUE AGENCY EMPLOYEE ACCESSES TAX FILE WITHOUT AUTHORIZATION

A complainant alleged that the Canada Revenue Agency (CRA) contravened the use and disclosure provisions of the *Privacy Act* when a CRA employee accessed his tax file in 2005 and 2006.

The complainant became suspicious that his tax files were being accessed when he learned that several people within his community had gained intimate knowledge of his financial information including his exact salary. After making a personal information request to CRA, he received an audit trail report of his T1 tax account showing all accesses to it over more than six years.

Upon reviewing the audit trail he recognized the name of a CRA employee who had made two

accesses. Specifically, the employee accessed the following personal information related to the complainant: Social Insurance Number, income and deductions, employment and income slips, filing history, children's information, address, date of birth, and marital status.

Our investigation revealed that the employee accessed the account without authorization and beyond the authority and requirements of his position. Accordingly, the complaint was deemed **well founded**. CRA has confirmed that the employee no longer has access to taxpayers' information.

3.6 NATIONAL DEFENCE EMPLOYEE ACCESSES SOMEONE'S PERSONAL HEALTH RECORDS FOR HER OWN PERSONAL REASONS

A complainant alleged that his personal health information was accessed inappropriately by a Canadian Forces (CF) employee with whom he had a prior personal relationship.

Our investigation revealed that the employee accessed the complainant's health information held in the Canadian Forces Health Information System (CFHIS) numerous times after receiving an anonymous message, advising that the complainant was "sick" and as a result, her own health was at risk.

The employee admitted to accessing and using the complainant's personal information for her personal reasons, which were clearly inconsistent with the purpose for its collection and the complaint was **well founded**.

As a result of our investigation, National Defence (DND) acknowledged the importance of a comprehensive and up-to-date privacy awareness and training process for its employees. DND advised that it has implemented new controls in the CFHIS to deal with improper access, it has updated the Canadian Forces Health Service policy on appropriate use and disclosure of personal health information, and it has provided training to CF heath care staff on patient privacy.

4.0 Justice delayed is justice denied:
Persistent delays by federal institutions in responding to individual access requests and complaint investigations by our Office

Last year, we raised the alarm over too many federal institutions being consistently delinquent in dealing with requests from Canadians to access their personal information. And this year, the trend of increasing delays has continued and broadened.

Time-delay complaints have been consistently high in recent years but we received an unprecedented number in 2012-2013. Furthermore, the requests have become more complex and many are about obtaining access to emails, making the processing more arduous for federal institutions.

We have also noted a trend toward a loss of expertise in the review process at some institutions, which causes additional delays. As well, since institutions are experiencing increased requests for personal information, there are further delays in responding to our Office.

For privacy rights to be truly meaningful, organisations must work to meet their obligations and do so in a timely manner. Unfortunately, federal institutions continue to struggle—and increasingly fail—to respond to privacy requests from individuals within legislated timelines.

Equally important, they struggle to respond in a timely fashion to our Office once a complaint has been received. This often translates into lengthier and more resource-intensive investigations.

All told, if it's true that time is money then Canadians are effectively being shortchanged on both fronts. The following are some examples.

4.1 ROYAL CANADIAN MOUNTED POLICE

A complainant filed multiple denial-of-access complaints against the Royal Canadian Mounted Police (RCMP). Due to an oversight, the RCMP failed to process some of those requests, which then snowballed into more delays. Investigation delays further worsened because the administrative liaison contact provided by the RCMP was unfamiliar with the requests, and so had to refer matters requiring clarification to an analyst with knowledge of the files.

Such uncoordinated collaboration by the RCMP was responsible for prolonged delays throughout the entire investigation, contributing to difficulties in locating records. For example, as part of a missing record investigation, our Office requested a copy of an alleged missing record (a binder of information) to determine its relevance to the requests. The RCMP took 15 months to provide the binder, partly because of differing views concerning what constituted responsive records relative to the request, but also because its search for the document took a protracted amount of time.

In another case involving the RCMP, an individual complained that the force violated his privacy rights by disclosing his personal information to his then employer without legal authority. On the basis of that information, the complainant was ejected from an RCMP cadet training program and, subsequently, also dismissed by his employer.

The personal information in question was derived from a judicially authorized wiretap by a municipal police force investigating another individual for criminal offences. Further details on the substance of this case can be found in Chapter 2. However, the case also offers an object lesson in serious delays by a federal department.

Throughout this lengthy process, the RCMP advanced at least six separate legal arguments to justify the disclosure of the wiretap information. When our Office posed questions or sought further

***Access delayed is access denied: Guidance for Access to Information and Privacy Officers on Deemed Denials under the* Privacy Act**

A substantial majority of the complaints received by our Office come from individuals alleging that a federal institution unjustly denied them timely access to their personal information.

The *Privacy Act* gives individuals a general right to have access to their personal information held by federal institutions upon written request. Federal institutions are generally obliged to meet those requests, although there are exceptions.

Our Office has produced guidance for individuals about this process and our efforts to help speed things up.

http://www.priv.gc.ca/resource/fs-fi/02_05_d_50_e.asp

representations regarding each successive argument, the RCMP would often respond, not by providing the specifics requested, but by asserting a different and unrelated legal argument.

In all, the length of this 32-month investigation is in large part attributable to undue delays caused by the RCMP.

4.2 DELAYS IN RESPONDING TO ACCESS REQUESTS

The upward trend for time-delay complaints is expected to continue as institutions struggle to meet demands in responding to privacy requests within legislative timelines.

The following are some alarming cases that we've seen.

Transport Canada: Three separate cases took 21, 23 and 27 months for the department to process. In one case, the delay was caused by a lack of personnel with appropriate security clearance to review the material.

Royal Canadian Mounted Police: There has been a significant increase in the number of time-delay complaints received against the Royal Canadian Mounted Police (RCMP)—96 this year compared to 25 last year. In 2012-2013, we experienced consistent delays in receiving needed information from the RCMP, significantly impacting our ability to conduct timely investigations.

When a request was finally answered (typically within eight to 12 months—unless the request did not involve many documents), our Office was often not updated unless we followed up. Overall, there appeared to be either a poor understanding or an outright disregard of the investigative process and this Office's mandate. We note, however, as of this report's writing, key positions within the RCMP's Access to Information and Privacy Office have recently been filled. It is hoped that this will bring more positive results in the next reporting year. We will be closely monitoring the situation.

Department of Justice Canada: Time delays by this department have been so egregious that we actively pursued three deemed denial complaints in the past fiscal year in an attempt to accelerate action. Throughout the complaint processes, while the department did provide some work plans with respect to when it would finish processing the requests, these were ultimately not respected. With regard to two of these complaints, our Office filed two respective applications before the Federal Court, but when the department finally sent final releases to both complainants, we discontinued our applications since the issue of timeliness then became moot. With respect to the third complaint, the complainant did not consent to this Office bringing an application on her behalf.

Correctional Service of Canada: This Agency continues to rank first for the most time-delay complaints. However, it should be noted that the way in which Correctional Service of Canada (CSC)

processes requests tends to result in a high tally of complaints. For example, if a single request requires access to a number of Personal Information Banks, CSC processes and reports it as multiple requests, which in turn increases the potential number of time delays that can be incurred.

Despite the record number of time-limit complaints against CSC, the Agency makes an effort to work with us collaboratively, and provides action plans, commitment dates and quick turnaround to our Office.

A success story—National Defence: Although experiencing a significant increase in the number of requests in the last few years, National Defence (DND) has been able to find efficient ways to minimize delays in responding. There has been a significant drop in time-delay complaints received by our Office (from 77 in 2011-2012 to 52 in 2012-2013), and collaboration and communication with our Office has been very good.

5.0 Private and safe:
Securing the right to privacy amidst the quest for stronger public safety

Questions surrounding public safety have understandably occupied many policy minds and discussions throughout the first years of the 21st century. While security is an undeniable government responsibility and human need, so is privacy. One cannot unduly eclipse the other, and therein rests the challenge of advancing measures to enhance public safety while respecting and protecting Canadians' privacy. The following chapter examines this interface on many fronts.

First, we feature our Office's audit of the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), which collects 65,000 reports about Canadians' financial dealings every day from banks, life insurance agents, real estate agents and casinos. Our audit found that FINTRAC was receiving and retaining personal information beyond what is authorized by its governing legislation. Moreover, FINTRAC has yet to stop the practice.

This chapter also examines the most recent incarnation of the lawful access debate along with our efforts to have a dialogue with federal institutions about their potential use of unmanned aerial vehicles.

It also offers a detailed look into key initiatives linked to the Beyond the Border Action Plan. With the stated intention of increasing security and easing trade flow, Canada and the U.S. are implementing a number of measures along their common border. Many of these relate to the movement of people and have potentially serious privacy implications. One example noted in this chapter allows the possible strip-searching of anyone entering certain areas near or associated with borders, even though no signs will be posted specifying the locations of such zones.

5.1 AN AUDIT OF FINANCIAL TRANSACTIONS AND REPORTS ANALYSIS CENTRE OF CANADA

Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) is an independent federal agency authorized to receive and analyze information on financial transactions, and to disseminate intelligence about suspected money laundering and terrorist financing activities.

Created in 2001, the Agency operates at arm's length from law enforcement but can disclose information to law enforcement and security organisations, as well as to the Canada Border Services Agency and the Canada Revenue Agency.

More than 300,000 entities are legally required to report to FINTRAC cash transactions or electronic funds transfers of $10,000 or more by their clients. Any transactions—or attempted transactions—that trigger "reasonable grounds to suspect" money laundering or terrorist financing activities must also be reported, regardless of the amount of money.

The reports are submitted without the consent of the clients and mostly without their knowledge. This financial surveillance now involves more than 65,000 reports received daily (primarily from financial institutions) detailing the private financial dealings of ordinary Canadians.

Considering the clear potential risks to privacy, Canadians must be assured that their personal information is being appropriately managed within well-established controls. Privacy involves not only protecting data but also ensuring that the amount of personal information collected and retained is kept to the minimum necessary.

Under amendments passed in 2006, the legislation covering FINTRAC—the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*—requires our Office to review FINTRAC every two years and report the results to Parliament. Our first audit was completed in 2009.

Highlights of our 2009 audit

In 2009 we found that FINTRAC had received and retained more information than allowed by its legislative authority. Existing mechanisms, including the screening and continued monitoring of reports, needed to be improved to ensure that FINTRAC's information holdings are both relevant and not excessive.

Although FINTRAC had put into place elements of a privacy management framework, some gaps needed to be addressed. We had also found that FINTRAC was unable to provide assurance that the guidance provided by its regulatory partners to reporting entities is consistent with requirements established under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*.

Focus of the current audit

This year, we conducted an audit that focused on assessing the progress made by FINTRAC to address our 2009 recommendations. We also examined FINTRAC's management of personal information acquired, used and disclosed in its capacity as a financial intelligence unit and also while carrying out its compliance mandate.

What we found

Although FINTRAC had initially responded positively to 10 of 11 previous audit recommendations, and agreed to implement corrective action to address identified gaps, weaknesses and deficiencies, our current audit found that limited progress has been made to address half of the recommendations.

The 2009 audit highlighted a number of areas where FINTRAC could strengthen privacy protections for Canadians. For example, we recommended that the Agency work with its intelligence partners to ensure, as much as possible, that any affiliation of individuals with terrorist groups was confirmed before retaining this data and making it available for analytical purposes. We also recommended that FINTRAC establish written criteria to help those responsible for submitting reports to determine when the thresholds for disclosures to the Canada Border Services Agency and Communications Security Establishment Canada have been met. Satisfactory progress had been made to address these recommendations.

Similarly, FINTRAC has made satisfactory progress to address gaps that existed in its privacy management framework. In responding to our 2009 audit recommendation, FINTRAC has:

- appointed a Chief Privacy Officer responsible for providing strategic leadership and overseeing privacy-related activities;
- established a formal process to identify and mitigate privacy risks associated with new or substantially redesigned programs and services;
- implemented a privacy breach identification and reporting protocol; and
- expanded security awareness initiatives.

While FINTRAC has enhanced its process for managing threat and risk assessments and continues to have a sound security infrastructure, we did find practical instances of non-compliance with established security policies.

Excessive reporting

Some of the most serious deficiencies identified in our previous audit related to the receipt and retention of personal information. In 2009 we found that reporting entities were sending FINTRAC information that exceeded what was required under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, including:

- financial transactions below the $10,000 reporting threshold;

- Suspicious Transaction Reports that did not demonstrate "reasonable grounds to suspect" money laundering or terrorist financing activities; and
- Voluntary Information Records where no suspicion of money laundering or terrorist financing was evident.

We recommended in 2009 that FINTRAC take steps to limit the receipt of personal information to only that required by law. Agreeing to the recommendation, FINTRAC stated that it had already taken steps to reduce the potential of receiving information that should not have been sent. Despite this effort, over-reporting continues to be a problem.

In a sample of reports examined during our current audit, we found a number of large cash transaction reports, international electronic funds transfer reports and reports on cross-border movement of currency that fell below the $10,000 reporting threshold. We also found instances of reports made on the basis of unsubstantiated suspicion; they did not clearly demonstrate reasonable grounds to suspect money laundering or terrorist financing activities. For example:

- a young professional cashed three bank drafts worth almost US$100,000 purchased from a major Canadian bank. The issuing bank confirmed the validity of the drafts. The manager of the money services business where the drafts were cashed obtained satisfactory answers to various questions on the transaction but nevertheless filed a Suspicious Transaction Report with the explanation that "the amount of money simply did not match his age."
- an individual, who purchased a home from his childhood friend, released the deposit directly to the seller instead of to the seller's lawyer. The notary who reported the transaction stated: "this is a long-time client of mine and I have no reason to suspect money laundering or terrorist activity but as I was not sure whether the following (as described above) needed to be reported or not, I thought it best to do so."
- an individual wanted to change €5,000 into Canadian dollars. To dissuade the individual from completing the exchange, the reporting entity informed the individual that the full amount would be frozen for 21 days. The client decided not to proceed with the transaction.

These examples would suggest that some reporting entities continue to be unclear on their reporting obligations, or default to reporting if in doubt, rendering privacy a secondary consideration.

Fundamental to privacy is the principle that personal information should be kept only if there is a legitimate and authorized need. In 2009 we recommended that FINTRAC permanently delete from its holdings all information that should not have been received. FINTRAC welcomed the recommendation, and recognized the importance of ensuring that its database contains only information that the Agency is authorized to hold. FINTRAC stated that it would continue to explore and develop new ways to achieve this goal.

Unfortunately FINTRAC has made little progress in meeting this commitment. The Agency continues to retain information that exceeds the parameters and thresholds of reportable transactions specified in the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. This presents an unquestionable risk to privacy by making accessible information which should never have been received in the first place.

Our recommendations

Many of our current audit recommendations are similar to those made in 2009.

To reconcile its obligations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* with those under the *Privacy Act*, we recommend that FINTRAC analyze and assess incoming reports to ensure that it retains only information which it has the legislative authority to receive and which is directly related to an ongoing program or activity. As a complementary measure, we recommend that FINTRAC assess the effectiveness of its outreach programs and strengthen them where necessary to mitigate the risk of entities over-reporting.

We have also repeated our 2009 recommendation that FINTRAC identify and dispose of personal information that it currently retains and should not have received, and that is not directly related to its operating programs and activities.

The extent to which FINTRAC's database contains information that it should not be retaining is unknown.

Further issues—Compliance mandate

In addition to its analysis and disclosure functions, FINTRAC has a mandate to ensure reporting entities comply with their obligations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. It fulfills this mandate through various means, including compliance examinations that involve the review and collection of personal information about the clients of reporting entities.

Limiting the collection of personal information, or data minimization, is a key element of privacy protection. Data minimization—restricting the collecting of information to that which is strictly necessary to fulfill an identified purpose—mitigates privacy risks. Simply stated, data not collected is data not at risk.

In our previous audit we found instances where there was no demonstrated need for FINTRAC to retain certain types of records to execute its compliance mandate. We noted that some of FINTRAC's examination files captured personal information in significant detail where the information did not appear to be required to substantiate examination findings.

We recommended that FINTRAC observe the principle of data minimization. FINTRAC agreed with the recommendation, and stated that it would reinforce the importance of respecting the principle when training its compliance officers and updating its policies and procedures.

In June 2009, FINTRAC established a policy under which all records obtained during a compliance examination were scanned and retained electronically, and the hard copies destroyed. Owing to an increased number of examinations, the compliance staff was instructed in 2011 to limit the scanning and retention to only records necessary for substantiating compliance deficiencies.

However, our latest audit found that FINTRAC has not updated its policies and procedures to formally reflect this 2011 guidance. As well, it has not established criteria or guidelines to assist compliance officers in determining the type of records or information relevant to supporting such compliance deficiencies.

We observed inconsistencies in the application of the scanning policy, as well as in the collection and reproduction of personal identifiers (e.g. social insurance and health card numbers). We also found instances where compliance files retained personal information that was not required to substantiate examination findings.

FINTRAC's response

We presented nine recommendations in our current audit. In responding, FINTRAC has accepted all of them and indicated that adequate measures are already in place to address five of the recommendations. However, we believe additional work is required. The Agency has agreed to take action to address the four remaining recommendations.

FINTRAC stated that it accepts our current recommendations about limiting receipt and retention of personal information that exceed the parameters and thresholds of reportable transactions under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. Despite its acceptance of similar recommendations in 2009 and its commitment then to address them, the Agency now maintains that it has a legal obligation to receive and retain for 10 years any report or information provided by reporting entities, regardless of whether it meets the parameters and thresholds set out by the legislation.

Conclusion

Although FINTRAC has stated that it has an obligation under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* to receive and retain any report or information provided, regardless of whether it should have been reported, Section 4 of the *Privacy Act* requires government institutions to limit the collection of information to only that which relates directly to an operating program or activity.

In other words, institutions should not collect and retain information unless it is required to fulfill their mandates. Moreover, Treasury Board Secretariat policy states that government institutions must have a demonstrable need for each piece of personal information collected in order to carry out the program or activity.

The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* obligates FINTRAC to analyze and assess reports it receives. FINTRAC has

stated that its obligation in this regard is to analyze and assess reports for the purpose of determining whether the information should be disclosed to law enforcement or security partners as part of a financial intelligence disclosure.

FINTRAC also maintains that it is legally obligated to retain all information it receives for a minimum of 10 years, regardless of its relevance.

However, the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* must be reconciled with the requirements of the *Privacy Act*. To accomplish that, FINTRAC is also obligated to analyze and assess reports for the purpose of ensuring that it does not accept and retain information outside the parameters and thresholds set out in the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. Until FINTRAC implements a process for doing so, it will continue to receive and retain information that it does not need or use in an operating program or activity; and by extension, it will not fully comply with its obligations under the *Privacy Act*.

Entities reporting personal information to FINTRAC

- Financial entities of all types (banks, credit unions, *caisses populaires*);
- Life insurance companies, brokers or agents;
- Securities dealers, portfolio managers, provincially authorized investment counsellors;
- Foreign exchange dealers;
- Money services businesses;
- Dealers in precious metals and stones;
- Crown agents accepting deposit liabilities and/or selling money orders;
- Accountants/accounting firms, real estate brokers/sales representatives involved in activities, such as receiving or paying funds on behalf of a client;
- Casinos (except some temporary charity casinos); and
- Real estate developers.

5.2 PRIVACY AND THE PURSUIT OF PERIMETER SECURITY

Since February 2011 the Canadian and U.S. governments have been working towards integrating their common border to increase security and facilitate trade. *Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness*, published in December 2011, provided implementation details but did not address any of the privacy recommendations submitted that June by our Office.

As well, at that point neither government had specifically addressed privacy concerns arising from the far-reaching action plan.

Responding to these developments, privacy commissioners and ombudspersons from across Canada issued a joint resolution on April 2, 2012, as Prime Minister Stephen Harper and President Barack Obama were meeting in Washington with Mexican President Felipe Calderon.

The resolution urged the Canadian federal government to take all necessary steps to ensure that the standards and values behind our privacy laws are not diminished by programs developed to implement the Canada-U.S. perimeter security action plan, more commonly known as the Beyond the Border Action Plan.

The joint resolution spelled out 13 recommendations, including:

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

Several of the concerns expressed in the resolution were addressed by a *Joint Statement of Privacy Principles,* which the Canadian and U.S. governments made public on June 28, 2012. The official announcement noted however that "this Statement of Privacy Principles is not intended to constitute a treaty or other binding agreement under international law."

According to Treasury Board's directive, a Privacy Impact Assessment (PIA) must be performed for federal government programs that involve personal information, and this assessment must then be submitted to our Office for review. Consequently, all federal programs resulting from the action plan's implementation will be subject to such a review and will receive recommendations as necessary from our Office. Details about PIAs received during the last fiscal year related to the Canada-U.S. border can be found in the following section of this chapter.

Resolution of Canada's Privacy Commissioners and Privacy Enforcement Officials on the Canada-U.S. Perimeter Security and Economic Competitiveness Action Plan: http://www.priv.gc.ca/media/nr-c/2012/res_120402_e.asp

5.3 CANADA-UNITED STATES ENTRY/EXIT SYSTEM

Under the Beyond the Border Action Plan, Canada and the U.S. will systematically exchange information collected about travellers crossing their common border; the record of someone entering one country will serve as the record of that same person leaving the other.

Canada has not previously routinely tracked the exits of individuals going to the United States and there are concerns that the information may be used for extensive secondary purposes. To test technical capacity, the Canada Border Services Agency (CBSA) conducted a Phase I field trial from October 2012 until January 2013, sharing data with the U.S. on third-country nationals and foreign nationals at two land crossings in Ontario and two in B.C.

Phase II, which began on June 30, 2013, expands the project to all land crossings. Future phases will include the exchange of information on all travellers crossing land borders, including citizens of Canada and the U.S., as well as all air travel passenger exits. When fully implemented by June 2014, the Entry/Exit Program will provide the governments of both countries with the history of how long Canadians, U.S. citizens, Permanent Residents, Temporary Residents, and visitors have been in and out of their respective countries.

Various secondary uses for this information by federal institutions other than CBSA are being considered.

We recommended that signs be clearly posted at border crossings indicating why this information is being collected and how it will be used, that secondary uses be strictly limited, and that disclosures of exit/entry information be clearly justified. We are concerned about the lengthy retention period for this information—75 years—and have asked CBSA to review whether this retention period is justifiable. We are concerned that, as the initiative evolves in future phases, additional data elements such as fingerprints or photos may be included. The implementation of a biometric exit system to collect fingerprints from visitors leaving the country has long been proposed by the United States and is under discussion in Europe.

Further, we are also concerned about the aggressive timelines for rolling out this and other Beyond the Border activities. We received the PIA for Phase I of the Entry/Exit program only a few days before the field trial began. In response to this and other issues, the Commissioner wrote to the President of the CBSA to register concern and request that PIAs be provided earlier to ensure that any recommendations could be formulated, considered and implemented well in advance of an initiative taking effect.

5.4 CUSTOMS CONTROLLED AREAS

Customs Controlled Areas (CCAs) are large areas near or associated with borders, where workers and departing domestic travellers may come into contact with international travellers and/or goods that have not been cleared by customs.

New regulations allow CBSA officers to stop, question, detain, search and even strip-search individuals while they are within these areas. These extraordinary powers can be used even when individuals have no intention of crossing a border.

We expressed concern that the areas that may be designated as customs-controlled are extensive and travellers have no way of knowing when they are inside or outside of them. We asked that clear signage be posted indicating the area boundaries and recommended that the rationale for designating a CCA be clearly justified and demonstrated.

CBSA has indicated that while general signs will be posted at points of entry advising travellers that there *may* be CCAs, the specific locations of these areas where border officers may use these extraordinary powers will not be indicated.

5.5 IMMIGRATION INFORMATION SHARING TREATY

For many years Citizenship and Immigration Canada (CIC) and the U.S. Department of State have shared information on a case-by-case basis, where suspicion warranted the collection of further data for decision-making about visa applicants or refugee claimants.

The Beyond the Border Action Plan expands this exchange considerably. Each country will now systematically and automatically query the immigration data systems of the other for negative or derogatory information on all third-country visa applicants.

Information collected through these queries will be used in deciding on admissibility. We are concerned that this initiative may greatly increase the volume of derogatory information collected by CIC, and that some of the information collected will not be

necessary or applicable to Canadian immigration laws.

We recommended that CIC clearly define and limit the type of information that will be defined as "derogatory" to ensure that only accurate and relevant information is used to make an immigration decision.

We received and reviewed a PIA on the biographic information-sharing aspect of this program in 2013, and expect to receive another PIA on the sharing of fingerprints and photos in 2014.

5.6 TEMPORARY RESIDENT BIOMETRICS PROJECT

The Temporary Resident Biometrics Project (TRBP) is an interdepartmental project managed jointly by CIC, the CBSA, and the Royal Canadian Mounted Police (RCMP). It is designed to systematically capture, match, and verify biometric information from foreign nationals who apply to visit, study or work in Canada. Beginning in late 2013, foreign nationals from certain countries seeking visas to enter Canada will be required to give their fingerprints and have their photograph taken as part of their application.

We have consulted with the three agencies regarding the project's developments, and two new PIAs were submitted to our Office in 2012-2013. A significant development that arose since our review of the interim PIA was that the RCMP will now be permitted to retain information, including fingerprints collected during the visa application process, and use this data for domestic law enforcement purposes. Fingerprints collected from individuals applying to visit, work, or study in Canada will be stored by the RCMP for a minimum of 15 years; any fingerprints collected by the police in the course of criminal investigations, including latent prints collected from crime scenes, may now be queried against this database. We are concerned about the lengthy retention and uses of fingerprints of individuals who have not been charged with, or convicted of, any criminal offence.

And as is the case with many programs under the umbrella of the Beyond the Border Action Plan, we have concerns about the wide-scale, routine sharing of information with other countries, recognizing that once information goes beyond Canada's borders, it may be impractical or impossible to prevent unauthorized uses, disclosures, or transfers of that information, or to ensure that it is properly protected.

5.7 GLOBAL VISA APPLICATION CENTRES

Visa Application Centres operated overseas by private-sector service providers under contract with CIC are another component of the TRBP. These centres offer services for students, workers, and visitors to Canada who need temporary resident visas and will collect application information including fingerprints and photos, as required under the TRBP. The completed applications will be transferred electronically to CIC, and the fingerprints will be stored by the RCMP in a database as part of its Real Time Identification System.

We made a number of recommendations related to safeguards for sensitive biometric information and the importance of ensuring accuracy. We also noted privacy concerns related to risks posed by potentially conflicting legislation in the local jurisdiction where a Centre is located.

We recommended that CIC conduct a survey of local jurisdictions prior to awarding contracts to assess privacy risks and protections. We expect to receive a PIA for the final phase of the Visa Application Centre project in fall 2013.

5.8 ANOTHER ROUND ON LAWFUL ACCESS

Since the mid-1990s, our Office has periodically engaged with the federal government over various proposals to recast Canada's legal framework regulating the use of electronic surveillance.

In February 2012, the government introduced Bill C-30, the latest version of so-called "lawful access" legislation. Like several previous bills since 2005, C-30 proposed to expand the legal tools of the state to conduct surveillance and access private information.

The legislation (also known as the *Protecting Children from Internet Predators Act*) would have granted authorities new powers to:

- monitor and track the digital activities of Canadians in real-time;
- require service providers to preserve metadata, content and communication of their subscribers and turn it over if presented with a production order;
- compel production of subscriber information without a warrant or judicial oversight; and
- provide mandatory interception capacity in all devices and services, allowing covert remote access to the electronic files and communications of individuals.

Our Office has repeatedly stated that it understands the challenges faced by national security authorities and law enforcement in fighting online crime, especially with the current revolution in communication technologies.

However, any legislation expanding electronic surveillance by the state should also demonstrably help protect the public, respect the fundamental privacy principles established in Canadian law and be subject to proper oversight.

Shortly after the introduction of C-30, our Office identified serious privacy concerns similar to past versions of lawful access bills. In particular, we were concerned about access, without a warrant, to subscriber information. For instance, allowing authorities to compel names, home addresses, email account details and IP addresses for any reason related to policing, with no court oversight, seemed a considerable expansion of authority. Just as an example, an IP address can act like a digital fingerprint and provide a starting point to compile a picture of an individual's online activities, including registration with online services, a catalogue of personal interests based on websites visited, organisational affiliations and even physical location.

Since this broad power was not limited to reasonable grounds to suspect criminal activity or to a criminal investigation, it could affect any law-abiding citizen.

WHAT AN INTERNET PROTOCOL ADDRESS CAN REVEAL ABOUT YOU

"It's no different than looking someone up in a phone book." That's the argument by proponents of "lawful access" legislation such as C-30 which would let law enforcement and national security authorities gather subscriber information about Internet users without getting authorization in advance from a judge.

In a similar vein the warrantless collection of so-called "metadata" which is part of all Internet communications has been compared to simply reading the outside of an envelope.

Our Office conducted extensive technical testing to examine the privacy implications of information about Internet subscribers that could have been collected under C-30 and which goes beyond the name, address and telephone number found in a phone book.

This additional subscriber information covered email addresses, mobile phone numbers and the individual internet protocol (IP) addresses which are assigned by service providers to all subscriber electronic devices using their network. Every version of lawful-access legislation proposed in Canada in recent years (such as the previous C-52) would have obliged Internet Service Providers to turn over such information when the authorities asked for it.

In general, our findings lead to the conclusion that, unlike simple phone book information, email addresses, mobile phone numbers and IP addresses can be used to develop very detailed portraits of individuals that provide insight into someone's activities, opinions, interests, leanings and lives.

The full study is available on our website: http://www.priv.gc.ca/information/research-recherche/2013/ip_201305_e.pdf

Many Canadians reacted strongly against the proposed legislation, saying it would have a significant negative impact on their fundamental right to privacy.

On February 11, 2013—almost exactly a year after C-30 was introduced—Justice Minister Rob Nicholson announced that the legislation would not be proceeding further in Parliament. He also said that any future proposal "to modernize the *Criminal Code* will not contain the measures contained in C-30, including the warrantless mandatory disclosure of basic subscriber information or the requirement for telecommunications service providers to build intercept capability within their systems."

In a statement, Commissioner Stoddart hailed the government's announcement as "a welcome development for privacy in Canada."

"I applaud the many Canadians who spoke out about their concerns with the Bill and their deep attachment to their privacy rights," the Commissioner added.

5.9 EMERGENCY WIRETAPPING—C-55

In April 2012 the Supreme Court of Canada ruled unconstitutional a section of the *Criminal Code* that permitted access to private communications in an emergency without prior judicial authorization. The case of *R. v. Tse* arose from an alleged kidnapping in British Columbia where police initiated a wiretap without court approval claiming urgent circumstances.

The Court found certain aspects of the legislation to be unconstitutional and gave the government until April 13, 2013, to bring the law in line with the Charter by:

- specifying that only police officers—and not all peace officers—can make emergency wiretaps and then only in cases of certain serious crimes;
- ensuring that individuals whose private communications have been intercepted on an emergency basis are notified within 90 days; and
- mandating public reporting of all interceptions made on an emergency basis.

In response, the federal government brought in Bill C-55 on a "fast track" process, which included a hearing March 25, 2013, by the Senate Standing Committee for Legal and Constitutional Affairs. Appearing before the committee Assistant Commissioner Chantal Bernier described C-55 as "a positive development for privacy."

The Assistant Commissioner further noted that the monitoring of the private communications of Canadians "is one of the most invasive powers that investigators hold." In 2010 the OPC had identified key considerations for such interceptions as empirical justification of their necessity as well as accountability and transparency.

The approach of C-55 "clearly fits within the analytical framework developed by our Office in that it limits the privacy intrusion to what is solely needed for security," added the Assistant Commissioner.

C-55 became law just two days after the Senate hearing, receiving Royal Assent on March 27, 2013.

5.10 FEDERAL USE OF UNMANNED AERIAL VEHICLES

Media reports and increased licensing activity prompted our Office in the fall of 2012 to ask selected federal government institutions about current and planned use of unmanned aerial vehicles (UAVs). In Canada, UAVs are considered aircraft covered by the *Aeronautics Act* and therefore can be used only within limits prescribed by Transport Canada through the *Canadian Aviation Regulations*.

We contacted a number of institutions that we anticipated may be using UAVs, including the Royal Canadian Mounted Police (RCMP) and National Defence (DND), but received responses from only a few. Among those who had responded as of this report's writing, the RCMP outlined its use of the technology to survey car accident scenes and conduct search and rescue activities. The RCMP maintained that it was not using UAVs to conduct surveillance or collect personal information. DND meanwhile noted that while it uses UAVs, it only does so in field operations outside Canada. The National Research Council Canada planned only very limited trial usage related to improving navigation.

Considering the capacity of UAVs for surreptitious operation, the potential for the technology to be used for general surveillance purposes, and their increasing prevalence—including for civilian purposes—our Office will be closely following their expanded use. We have conducted in-depth research on the privacy implications of UAVs, which we will continue to flesh out as we learn more about the deployment of this technology.

We will also continue to engage federal government institutions to ensure that any planned operation of UAVs is done in accordance with privacy requirements. We strongly encourage any institution considering the use of such technology to first undertake a Privacy Impact Assessment to ensure proper attention to potential privacy risks and their mitigation.

In October and November of 2012 our Office sponsored a survey of 1,531 Canadians on privacy matters, including their perceptions about the use of UAVs. While four out of five indicated that they were very comfortable with the use of UAVs by law enforcement for search-and-rescue missions, acceptance dropped to two out of five for their use in monitoring public events or protests.

The full report can be read here: http://www.priv.gc.ca/information/por-rop/2013/por_2013_01_e.asp

5.11 INFORMATION ABOUT AIRLINE PASSENGERS—C-45

Our Office made representations to two separate Parliamentary committees about a small but significant change to a program that already has serious privacy ramifications for air travellers.

The program involves the collection, use and disclosure of potentially sensitive personal information about passengers arriving in Canada by air. It has two linked components—Advanced Passenger Information (API) and the Passenger Name Record (PNR).

API is the biographical information found in a passport or travel document and is therefore largely unchanging. PNR, however, changes from trip to trip because it is the information typically found in a computerized reservation system, such as itinerary, method of ticket payment, bags checked and seat information.

PNR information is potentially much more revealing because it can provide more sensitive information about travelling companions, who purchased the ticket, and can include special meal requests and other information from which religion, ethnicity or health status could be inferred. PNR can be used to create profiles of travellers and to draw inferences.

The seemingly minor amendment included as a section of the massive omnibus budget bill (Bill C-45) requires air carriers to provide API/PNR information to the Canada Border Services Agency (CBSA) not only about persons "on board a conveyance" but also about persons "expected to be on a conveyance."

In a written submission to the House of Commons Standing Committee on Public Safety and National Security, Commissioner Stoddart wrote that air carriers would now have to provide information to CBSA even earlier than currently, and "include information about individuals who cancel their travel at the last minute."

"Our understanding is that these proposed changes are being driven by the Canada-U.S. *Perimeter Security and Economic Competitiveness Action Plan*, and possibly by the ongoing negotiations between Canada and the European Commission on a new PNR Agreement. Generally, the new approach to screening decisions is to use advance passenger information to approve or deny boarding overseas," Stoddart added.

Our Office has repeatedly expressed concern regarding the lack of transparency about how the passenger information collected through API/PNR program is used. As well, many details of the program are negotiated secretly with other countries.

Our Office has regularly noted issues relating to the fact that the personal information gathered through API/PNR by CBSA is widely shared with other federal agencies (such as the RCMP and the Canadian Security Intelligence Service), provincial counterparts and partners in other jurisdictions.

Assistant Privacy Commissioner Bernier expressed many of the same concerns in testimony before the Senate Standing Committee on Transport and Communications.

The Assistant Commissioner also said that API/PNR should be looked at in relation to other travel programs, such as the Passenger Protect Program (PPP or "no fly") and a new Electronic Travel Authorization (eTA) program also being introduced as part of Bill C-45. The eTA program requires people from visa-exempt countries, including most European nations, to submit an application form to Citizenship and Immigration Canada before traveling to Canada.

"The relationship of the API/PNR program to the proposed eTA program and the PPP is not clear to us and, if it is not clear to us, we doubt that most Canadians will understand how they relate to one another," said the Assistant Commissioner.

Bill C-45 was approved in Parliament without amendment and became law on December 14, 2012.

6.0 The OPC in Action

As the *Privacy Act* enters its fourth decade—approaching middle age by human standards—the mission of our Office remains to protect and preserve the privacy rights of individuals in their dealings with the 250 federal agencies and institutions governed by the Act.

That mission, however, has become far more complex and challenging as government institutions continue enlarging their inventories of personal information about Canadians along with their technological capacity to process that data.

This chapter provides an overview of how our Office has risen to that challenge in the past fiscal year. It provides a detailed overview of action we have taken in investigations, before Parliament, in the courts and following up on past audits to see how our recommendations were implemented by institutions when it comes to disposing of information and using wireless devices.

On top of this, the chapter provides some explanation behind a dramatic upswing in complaints received over the past year along with providing a taste of the concerns raised by citizens to our Information Centre. It also tells some key success stories where institutions took advantage of the opportunity to satisfy complainant needs through the process of early resolution as opposed to more formalized and, at times, lengthy investigations.

6.1 PRIVACY IMPACT ASSESSMENT REVIEWS

Since 2002, federal departments and agencies have been directed by Treasury Board of Canada Secretariat (TBS) to conduct a Privacy Impact Assessment (PIA) early in the development of initiatives that pose potential threats to privacy, and to submit them to our Office for review. The goal is to identify privacy risks and devise strategies to eliminate or mitigate them.

Our Office asks that as part of this process, government institutions subject their programs and activities to a four-part test: Is the initiative absolutely necessary?; Is it likely to be effective in achieving its objectives?; Is the anticipated infringement on privacy by the initiative proportionate to any potential benefit to be derived?; And, are less intrusive alternatives available?

When the four-part test has been met, we ask government institutions to demonstrate that the data collection is minimized and appropriate, that the information collected will be securely protected, that uses and disclosures are appropriate and controlled, and that the information will be disposed of in accordance with the *Privacy Act*.

While we have always provided advice to institutions at multiple stages during the PIA process, in 2012-13 we decided to expand our informal consultation activities. These more informal consultations allow us to provide guidance earlier in the process, and to be informed of initiatives in advance of receiving a PIA. Our review process is more targeted, to ensure that our resources are devoted to initiatives which pose the greatest risk to privacy and that our advice is provided in a more timely fashion to ensure relevance and enable institutions to implement recommendations as early as possible.

We do not approve assessments or endorse projects or proposals during our review, nor can we oblige institutions to implement our recommendations, or even to heed our advice. That said, we find that departments and agencies are generally willing to work with us to resolve privacy concerns.

Canadians also benefit from the transparency brought by the PIA process when departments and agencies publish summaries of completed assessments on their websites.

In 2012-13, we received 68 new PIAs and held 22 consultations in addition to our ongoing work on files from previously submitted initiatives. We sent out 20 letters of detailed and comprehensive recommendations for initiatives we judged particularly intrusive, along with 29 more letters with less detailed recommendations for initiatives which, in our view, posed lower risks.

Highlights of some noteworthy assessments follow.

6.1.1 Canada Border Services Agency - Personnel Security Screening Standard

Our Office received a PIA for the Canada Border Services Agency's (CBSA) revamped screening program, the High Integrity Personnel Security Screening Standard, shortly before its implementation in June 2012. Because of the timing of the PIA submission, we were unable to review it before the screening program became operational.

Within days the program was making headlines, largely because of an integrity questionnaire that asked Agency employees—and potential employees—about drug abuse, alcohol consumption, gambling, hiring of prostitutes, taking part in sex tourism, or downloading images of bestiality.

We identified major risks to privacy during our review of the screening standard, particularly tied to broad and highly invasive questions. Our Office provided the Agency with recommendations related to the intrusiveness of the questionnaire, and also

identified concerns regarding consent, notification and safeguards.

As well, we were concerned about the overly broad application of the entire program to employees whose duties did not require access to sensitive information and assets, as well as insufficient evidence to support the necessity and effectiveness of the screening standard.

Responding to our recommendations, CBSA stopped using the questionnaire in October 2012. The Agency has since revised it to eliminate or modify questions unlikely to elicit information to support an individual's loyalty and reliability. Our Office, however continues to have serious concerns about the lack of evidence to substantiate the need for the screening standard on top of the service provided for the federal government by the Canadian Security Intelligence Service (CSIS) or to support the effectiveness of such questionnaires in achieving the stated goals.

6.1.2 Audio Surveillance at Ports of Entry

Our Office has been consulting with the CBSA on how the Agency uses audio-enabled video surveillance at ports of entry since we received a PIA about the initiative in 2011.

Our review of the PIA raised serious concerns about the proposed extensive use of audio as well as video to record travellers at ports of entry; at that time the Agency indicated to us that the project had been cancelled.

We again engaged the Agency on this issue following media reports in June 2012 of advanced preparations for audio-video surveillance at some Canadian airports. After several consultation meetings and correspondence indicating our concerns, we have been assured by the Agency that audio recording activities have been suspended at ports of entry, pending the submission of a new PIA. Excepted are Agency interview rooms, where travellers suspected of customs infractions are questioned. At the time of this report's writing, a new PIA had yet to be received.

6.1.3 Treasury Board of Canada Secretariat - Standard on Privacy and Web Analytics

Web analytics is the collection and analysis of data about web traffic and user visits for the purpose of understanding and optimizing web usage. Web analytics tools generally record the interaction of visitors with web pages by collecting internet protocol (IP) addresses.

Our Office has been examining the use of web analytics by government institutions since 2010. In June 2011, we expressed concern over the lack of formal guidance to institutions from the Treasury Board of Canada Secretariat (TBS) on how to use web analytics in a privacy-sensitive manner. In response to our concerns, TBS drafted the new Standard on Privacy and Web Analytics and conducted a PIA into associated privacy risks.

After extensive dialogue between our Office and TBS, the final PIA and Standard established recommended timelines for the retention and

disposal of personal information collected through web analytics. Profiling the web usage of individuals through web analytics data is specifically prohibited. The Standard also includes a detailed list of requirements for privacy notices about web analytics.

Although we were pleased to see the majority of our recommendations addressed, we continue to recommend that TBS provide concrete guidance to institutions in conducting their own PIAs related to using web analytics.

6.1.4 Shared Services Canada - GCKey Authentication

As reported in our 2011-12 Annual Report, we continue to follow the evolution of the federal government's Cyber Authentication Renewal Strategy. Until the end of 2012, Shared Services Canada (SSC) oversaw an Access Key service which authenticated businesses and individuals in their online dealings with the Government of Canada.

We reviewed GCKey, the Government of Canada branded authentication service which replaced Access Key. It allows businesses and individuals to sign on to online-enabled federal government programs and services using a combination of a username and password they create themselves.

Our Office was concerned by the absence of a retention and disposal schedule for personal information in GCKey. As well, the password creation process lacked a test to verify that passwords chosen did not contain ordinary dictionary words. We recommended that SSC establish a retention and disposal schedule for data containing personal information, such as log files produced by GCKey and security questions and answers linked to GCKey credentials.

We also recommended adding a dictionary test during the password creation process to increase both the security of individual passwords and the overall security of the GCKey authentication service. In short, this test ensures that an individual cannot choose as a password a word that can be found in a dictionary and, as a result, be vulnerable to being guessed or cracked by "dictionary attack" software.

While SSC examined the overall architecture of GCKey, it did not look at how government departments would implement this service. We expect federal government departments to conduct their own risk assessments, including undertaking a PIA and submitting it to our Office, before they adopt the GCKey service.

We have already reviewed a PIA from Human Resources and Skills Development Canada (now called Employment and Social Development Canada) on its adoption of the GCKey service and expect to receive more PIAs from other institutions examining their transition from Access Key to GCKey.

6.1.5 Citizenship and Immigration Canada - Global Case Management System

Citizenship and Immigration Canada initiated the Global Case Management System (GCMS) in 2000, to replace older systems and provide an integrated immigration case management system. The new global system is expected to continue absorbing other lines of business within the Department and will eventually replace the important Field Operations Support System, currently used by many institutions carrying out control and enforcement work in the immigration sphere.

Our Office reviewed the first release of the GCMS in 2004 and reviewed the second release this year. We identified several privacy risks about the safeguarding of sensitive data and made recommendations in this regard. We also noted that the PIA lacked a comprehensive outline of the flow of personal information in and out of the new global system.

In light of the GCMS's key role in delivering many immigration programs and initiatives, we undertook a two-month project to map all electronic transfers of data to and from this system. This allowed us to better understand how much data in this system is accessed and shared with other institutions, both at the provincial and federal level. We identified more than 30 systems and interfaces directly linked to the GCMS that either receive data from this system, transmit information to it, or do both.

In addition we organized a site visit to see first-hand how data are accessed and used by GCMS users and to view a demonstration of the system's interactions with other connected systems and interfaces. This visit added greatly to our knowledge of the GCMS and assisted with our evaluation of the system's potential privacy risks. We will continue to follow this file closely as the GCMS evolves.

6.1.6 Following up—Canadian Air Transport Security Authority and Full Body Scanners

After years of consultation with our Office on full-body scanners, the Canadian Air Transport Security Authority (CATSA) informed us this year that it would be implementing the use of Automated Threat Recognition technology at airports across Canada. This software allows direct transfer of any anomalies discovered during scanning to a stick figure image—which is all the screening officer sees. This approach eliminates the viewing of the traveller's actual image and follows a key recommendation of our Office that CATSA explore privacy-enhancing technologies for body scanners.

6.1.7 Encouraging Compliance - Signage for video surveillance on Parliament Hill

The Royal Canadian Mounted Police (RCMP) is expanding its video surveillance coverage on Parliament Hill by installing 134 more video cameras in addition to the 50 currently in place. Some new cameras offer panoramic views and zoom capability. As noted in our 2011-12 Annual Report, we were concerned that visitors to Parliament Hill were not informed by signs of video surveillance, and

that this may infringe on privacy rights, particular during peaceful protests.

We recommended that signs be posted prominently at entrances to Parliament Hill, informing visitors that they are being recorded, and referring them to a contact for more information. The RCMP, which is working in partnership with Public Works and Government Services Canada, the House of Commons, the Senate, the National Capital Commission, Parks Canada and others on this project, invited us to share this message with the Parliament Hill Signage Workshop and provided its project partners with our publication, *Guidance on the Use of Video Surveillance in Public Places by Police and Law Enforcement Authorities*.

We remain actively engaged with this workshop group as they work on the final arrangement of signs on and around Parliament Hill.

Guidance on the Use of Video Surveillance in Public Places by Police and Law Enforcement Authorities.
www.priv.gc.ca/surveillanceguidance

6.2 ACTION THROUGH INVESTIGATIONS

In addition to examples related to information technology and inappropriate access already featured in this report, the year included many other investigations of interest. Some key examples follow.

6.2.1 Denial was the starting point for Correctional Service of Canada

Between September and December 2010, an inmate at a maximum-security penitentiary requested 18 video recordings of incidents in which he was involved, which he alleged showed Correctional Service of Canada (CSC) officers committing assaults, hate crimes, and sexual harassment.

CSC refused to make available the videos, claiming that the videos included third party personal information that could not reasonably be severed, and that disclosure of the information would be injurious to the security of a penal institution.

The complainant alleged that the information was being withheld by CSC "in a blatant attempt to conceal corruption, harassment, and criminal misconduct by many of its officers."

Our investigation revealed that CSC had not even retrieved or reviewed the requested video recordings before responding to the complainant. Ten videos had already been destroyed under CSC's standard retention rules when the inmate made his request, but CSC did not so inform him.

Six other videos still existed at the time of the complainant's request, but CSC made no effort to retrieve them and they too were destroyed.

We found the complaints concerning these 16 video recordings to be **well founded**.

The remaining two videos involved use of force. Under CSC rules, such recordings must be retained for a minimum of 30 days, in contrast to the standard 4.5-day minimum retention period for any other recordings.

CSC cited the same two provisions of the *Privacy Act* for withholding these two recordings as for the other 16. However, the organisation did not actually review the two recordings before making the exemption claim.

Unlike with the other 16 recordings which had been destroyed, the investigator was able to review these two recordings. We found the videos did not show inmates other than the complainant, as CSC had stated in its refusal to release the recordings. Our Office however, determined that CSC had correctly applied the other grounds for refusal by demonstrating that disclosing the information could reasonably be expected to be injurious to the security of a penal institution.

We found that the complaints about these two video recordings were **resolved**.

CSC's responses to all the cases are troubling in that they appear to indicate an approach where denial of access is the starting point for handling requests for personal information under the Act rather than the openness and accountability that the Act was intended to promote. In 16 cases, CSC applied exemptions to disclosing records that did not even exist when CSC responded. We recommended that CSC implement appropriate measures to ensure that *Privacy Act* requests for records reach the appropriate officials in time to stop the records being destroyed where there is a short retention period for records.

6.2.2 Correctional Service of Canada initially denies access to full report in favour of giving the "gist"

In a complaint to our Office made in January 2011, a complainant alleged that Correctional Service of Canada (CSC) had denied him access to a copy of a report regarding his treatment and supervision. Some two months after making the access request in 2010, the complainant received a three page report containing two findings. In conversation with the report's writer, however, the complainant became aware that the report was in fact 10 pages long, holding 14 findings. Our investigation revealed that indeed, the official report was 10 pages.

CSC officials explained that the report was based on informal interviews and so it was decided that the more detailed report should be withheld in place of a condensed document providing the "gist."

The abbreviated version, in our view, was a misrepresentation of the information. The manner in which the requested information was processed by CSC's Access to Information and Privacy Office in response to the complainant's request was contrary to CSC's responsibility to identify all relevant information that existed at the time his request was received and to process that information in accordance with the provisions of the Act.

After lengthy negotiations, a copy of the full report was provided to the complainant with some personal information of other parties withheld. CSC also agreed, at our request, to undertake a review into how the access request was handled along with communicating to staff about their obligations under the *Privacy Act*, including a presentation to executives underscoring the important role the organisation plays in ensuring privacy rights.

6.2.3 Royal Canadian Mounted Police revealed absolute discharge

To be allowed to work at an airport, a man applied in July 2010 for the necessary Transportation Security Clearance. In September 2011, Transport Canada (TC) informed the man of its refusal to grant him the security clearance based on information received from the Royal Canadian Mounted Police (RCMP).

The man complained to our Office that the RCMP had disclosed his personal information to TC.

However, in applying for the security clearance the complainant had authorized TC to seek all relevant information including information in law enforcement records and had also authorized anyone having information relevant to the clearance to release such information to TC.

In carrying out a law enforcement record check for TC, the RCMP obtained from police in B.C. a summary of an incident in 2009 involving the complainant. The RCMP added information that the incident had been transferred to a provincial court which granted the complainant an absolute discharge a few months later.

In 2011, the RCMP provided TC with its report, including the information about the incident and the absolute discharge.

Under the *Criminal Records Act* the RCMP is not allowed to disclose the record of an absolute discharge when more than a year has passed unless the Minister responsible for the RCMP has given prior approval.

Because no such approval was obtained in this case and 19 months had elapsed since the absolute discharge, the disclosure contravened the *Criminal Records Act*. Nor was it one of the limited disclosures of personal information authorized in the *Privacy Act*. Accordingly, we found the complaint to be **well founded**.

We recommended that the RCMP send a letter of apology to the complainant.

6.2.4 Concern raised over online disclosure - The Qalipu Mi'kmaq First Nation Band

The Qalipu Mi'kmaq First Nation Band was created by agreement between the Government of Canada and the Federation of Newfoundland Indians and formally established in 2011. The Band gives formal status to the Mi'kmaq people who are scattered around Newfoundland and cannot therefore be described with reference to land they collectively occupy.

The agreement establishing the Qalipu set up an enrollment process which called for the full name and date of birth of all founding band members to be published in the Canada Gazette, which is available online.

A woman who had been recognized as a founding member complained to our Office that Aboriginal Affairs and Northern Development Canada (AANDC) was putting her at risk of identity theft by widely publishing such complete personal information.

Our investigation determined that the disclosure of the complainant's name and date of birth was consistent with the *Privacy Act* provision that personal information can be disclosed without the individual's consent when the disclosure is for the purpose for which the information was originally collected.

As well, the disclosure was for the identification and recognition of Band members, the very reason why it was initially collected on enrollment forms.

We found the complaint to be **not well founded**. Given identity theft is a real risk in today's electronic environment however, we asked that AANDC explore other options in the future. Possibilities include furnishing only a partial date of birth or enabling linking through another identifier to an offline registry that contains the date of birth.

6.2.5 Intake

A specialized Intake Unit is dedicated to analyzing, registering and triaging all written complaints about privacy matters raised to our Office. This unit plays a vital role in helping our Office understand complainants' concerns and expectations.

All complaints filed under the *Privacy Act* are forwarded to this unit. After an initial review of the complaint, the Intake team will follow up with the complainant if necessary for clarification and to obtain any additional information needed for an investigation.

The Intake team has had considerable success with resolving some privacy problems immediately, thus eliminating the need for individuals to submit lengthy, more formalized investigations.

6.2.6 Complaints

For the second consecutive year there was an increase in the number of complaints under the *Privacy Act* accepted by our Office. For 2012-13 the total was 2,273, the highest number ever and a 133 per cent increase from the previous fiscal year.

That record total however, was swollen by 1,159 complaints arising from two data breaches involving Human Resources and Skills Development Canada[7] and Department of Justice Canada. Since the Commissioner initiated her own complaints in these cases, individuals did not need to register complaints to trigger a formal investigation, yet a number of complaints were filed nonetheless.

Subtract the 1,159 complaints filed in relation to these two breaches and 1,114 complaints remain. Of these, 251 or 20 per cent consisted of eight complaints or more from each of 18 individuals. Over the previous three years, almost three-quarters of all complainants filed more than one complaint.

Most of these multiple complaints related to a breakdown in employer-employee relationships within federal institutions. As part of the modernization project detailed later in this chapter, strategies are being developed to streamline multiple complaints brought by the same complainant.

Underlying employer-employee problems and employee workplace grievances with union involvement also increased the number of complaints generally.

We have also noticed a rise in complaints from members of the federal public service related to the sharing of their personal information with third-party service providers.

Separately there has also been an increase in the number of complaints and data breaches involving inappropriate access by employees or vulnerabilities in information technology.

Complaints can be lodged for different reasons under the *Privacy Act* and these fall into three distinct categories—access, privacy and time limits. These categories are described in Appendix 1. Detailed statistics about complaints are in Appendix 3.

6.2.7 Early resolution

Early resolution is the best possible outcome for all concerned when it is successful. For individuals who lodge a complaint under the *Privacy Act*, it means getting the answers they seek quickly. For government institutions, it means avoiding an often lengthy and resource-consuming process.

In essence, early resolution usually relies on negotiation and conciliation rather than more formal investigation.

All complaints are examined when received to see if they could be candidates for early resolution. Considerations include the apparent complexity of the case and whether it appears to involve issues already previously addressed.

[7] Human Resources and Skills Development Canada (HRSDC) has since been renamed Employment and Social Development Canada; however, for the purposes of this report, we refer to the department by its name at the time of the breach incidents and throughout the reporting period.

Complainants are often satisfied with an explanation of what information departments can legally withhold under statutory exemptions. Furthermore, if departments were found in similar circumstances to have complied with the *Privacy Act*, potential complainants often agree there is little point in going ahead with a formal investigation.

In recent years, early resolution success has been growing steadily. In 2012-13 we closed more than a third of all complaints received through early resolution, compared to one-quarter in the previous fiscal year.

6.2.8 Modernizing the investigative process

The existing process within our Office for investigating complaints under the *Privacy Act* has come under increased strain as the volume of complaints has ratcheted up. At the same time our Office has come to appreciate the value in moving from a model that was largely based on the positions of the parties to one that pays more attention to satisfying the interests of all parties.

These two factors fed into a project in 2012 to modernize the investigation process. The result was a series of measures which we believe will improve our service to Canadians by reducing the number of more formal investigations as well as reducing the time and resources required to investigate complex and potentially systemic complaints.

Four priorities guided the project:

- strengthening the initial intake step, which plays a gatekeeping role, and enhancing the early resolution approach which, where appropriate, can eliminate the need for a more formal investigation;
- introducing a mediation approach to complaint investigations which focuses on end results and takes into account the interests underlying the parties' positions;
- strengthening relationships with federal institutions in order to facilitate information exchange and expedite response times; and
- modifying the investigative process to make it more streamlined and efficient.

Key to much of the modernization was making our various procedures proportionate to the different challenges or, as the adage says, *"don't use a sledgehammer to crack a nut."*

For example, data breaches will now be analyzed when first reported to decide whether their impact will be low, medium or high. This will be determined based on the potential level of harm to the parties involved or to the public, the risk of recurrence, the controls in place and actions taken to prevent or correct the problem, and the level of communication. The investigation process will be tailored to the impact level.

There has been a jump recently in complaints to our Office about federal institutions not responding within the statutory time limits to requests from individuals for their personal information. This increase often results from the institutions having to deal with a higher volume of requests without more privacy staff.

In response to these developments, the modernization project developed a new strategy for dealing with these time-limit complaints, again based on the proportionate model. The first course of action will be to attempt early resolution. (See explanation earlier in this section.)

Other approaches range from promptly issuing a deemed denial and resolving a complaint to the satisfaction of the complainant where possible.

Other important process innovations from the modernization project include:

- replacing snail mail by encrypted email—where technically possible—for faster communications with 14 key institutions which account for a high volume of complaints;
- designating a "portfolio" of key institutions for teams of investigators to build expertise about those institutions, minimize the number of investigators each institution must deal with and aid in identifying and effectively dealing with systemic issues; and
- assigning a single investigator to handle multiple complaints from the same individual and dealing with these in a single report wherever possible.

Implementation of the modernization process is continuing and further potential improvements are being assessed.

6.2.9 Investigations and dispositions - By the numbers

Several important complaint investigations are described in detail in Chapters 2 and 3. This section looks at the big picture behind the numbers. Detailed statistics are available in Appendix 3.

In 2012-2013, complaints accepted by our Office more than doubled from the previous fiscal year—2,273 compared to 986. This unprecedented increase was driven by the 1,159 new complaints arising from the two breaches at Human Resources Development Canada.

A total of 908 complaints were closed during the year, with a third of those through the use of early resolution. In the previous year, our Office closed 913 cases, with nearly a quarter through early resolution.

Access issues were the trigger for more than 70% of our not well founded cases. Usually individuals were challenging an institution's refusal to provide access to their personal information. In most cases however, we found that appropriate exemptions had been applied or that the institution had conducted a reasonable search for information and we were

satisfied that no other responsive records existed. The number of well-founded cases we see in the public sector continues to be significantly higher than in the private sector. Roughly three quarters of the well founded cases under the *Privacy Act* in 2012-2013 involved complaints about institutions failing to respond to access requests within legislated time limits.

DISPOSITIONS*	No. of Cases	Percentage
Not well founded	166	18
Well founded	276	30.5
Early resolution	299	33
Discontinued	60	7
Settled	33	4
Well founded resolved	47	5
Resolved	22	2
No jurisdiction	5	0.5
Total	908	100

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

After a drop between the previous two reporting periods the average treatment time to complete exclusively formal investigations rose slightly in 2012-2013 to 8.3 months from 7.6 in 2011-2012.

Delays in responses from departments and agencies accounted for part of this increase as did an increase in complex complaints. The more complex category of complaints related to the use, disclosure, collection and retention of personal information rose from 22 per cent of formal investigation complaints in the previous year to 64 per cent this year.

Our refining of the early resolution approach however, has helped keep the average time to complete cases low overall. The combined treatment times for both formal investigations and early resolution categories amounted to 6.7 months in 2012-2013. While that was a 15 per cent increase over last year's 5.8 months, it was still faster than the previous three years: 19.5 months in 2008-09, 12.9 months in 2009-10 and 7.2 months in 2010-11.

In those earlier years, our Office calculated treatment times from the date complaints were received, even though some lacked essential information and required clarification before work could start. Starting in 2011, complaints have been considered "accepted" only after the contents are complete. We feel this definition allows for a more accurate picture of treatment times.

This means that the complaint numbers for fiscal year 2011-12 onwards were not compiled on exactly the same basis as those of previous years. For percentage

changes, however, this makes little significant difference.

More than 90 per cent of all complaints accepted during 2012-13 originated from the Top 10 Institutions, a slight increase over the mid-80s percentage of the previous three fiscal years.

The departments on the Top 10 list did change, however, compared to a year earlier:

- Human Resources and Skills Development Canada jumped to 1st place from 8th;
- Canada Revenue Agency dropped from 4th place to 7th;
- The Department of Justice Canada is new on this year's list, in the 3rd spot, as well as Canadian Food Inspection Agency in 9th and Transport Canada in 10th;and
- The Canadian Security Intelligence Service, Public Works and Government Services Canada, and Canada Post all dropped off the list this year.

Top 10 Institutions by Complaints Received in 2012-13

Institution	
Human Resources and Skills Development Canada	1030
Correctional Service of Canada	284
Department of Justice Canada	188
Royal Canadian Mounted Police	182
National Defence	90
Canada Border Services Agency	88
Canada Revenue Agency	76
Veterans Affairs Canada	56
Canadian Food Inspection Agency	33
Transport Canada	27
All other departments and agencies	219

6.3 AUDITS

The *Privacy Act* gives the Commissioner discretion to carry out audits of the personal information handling practices of federal departments and agencies. If an audit finds any shortcomings, the Commissioner can recommend remedial action to the institution.

The audit findings and recommendations may be published in an annual report or a special report to Parliament. Other than such public disclosure, the Act provides no further enforcement powers. Generally, approximately two years after publication, we follow up to determine whether the institution has addressed our recommendations and fulfilled its commitments.

This year we followed up on our 2010 audits of disposal practices and the use of wireless technologies within selected federal institutions.

We are pleased to note that, of the 34 recommendations related to these two audits that were accepted, all have been fully or substantially implemented.

6.3.1 Disposal audit follow-up

Background

Federal institutions collect vast amounts of personal information in support of public policy and to deliver programs and services. When records with no archival or historical value reach the end of their retention period or when data are stored on obsolete computers, the information is disposed of.

Under the *Privacy Act*, federal institutions are obliged to protect information destined for disposal with the same care that they give to data still in use. At stake is the public's trust in the government's ability to safeguard sensitive personal information.

The lack of adequate controls over disposal of unneeded government documents was at the core of one of the most egregious privacy breaches ever encountered by our Office. In 1998, our Office discovered that four truckloads of intact confidential federal government records containing personal information were about to be sent to the United States, South Korea and China. The private company hired to shred and recycle the records was instead exporting them intact because whole paper brought a higher price than shredded on the recycling market.

We recommended then that Library and Archives Canada (LAC) use off-site shredding services only if the companies could guarantee security, and only if the shredding was done under supervision.

At the time of the initial audit, LAC provided records storage and destruction services to more than 90 federal departments and agencies. We examined its off-site paper waste destruction program and the contractual arrangements with private shredding companies.

We also examined the disposal of surplus computers through donations to the Government of Canada's Computers for Schools program, which is operated by not-for-profit organisations under agreements with Industry Canada (IC).

The audit

Our audit, completed in October 2010, found that LAC had a comprehensive set of policies, procedures and processes for managing the disposal of federal government records. Security requirements embedded in off-site destruction contracts complied with Government policy, and they provided controls to ensure records are transported, stored and disposed of in a secure manner.

However, we also found that:

- the off-site destruction of records was not systemically monitored—through periodic inspections and audits—to ensure privacy and

security requirements were met in a consistent manner; and

- uniform shredding specifications, intended to make the reconstruction of information on shredded paper impracticable, were not in place.

The Computers for Schools program is managed by IC. The program collects and refurbishes surplus computers donated by government and private sector sources for distribution to schools, public libraries, aboriginal communities and not-for-profit learning organisations throughout Canada.

Treasury Board of Canada Secretariat policy requires federal departments and agencies to wipe surplus computers of all classified and protected records before donation to the Computers for Schools program. We tested computers from 31 federal institutions and found that 28 institutions (90%) had not fulfilled this obligation.

We also found that IC had not established a protocol for analyzing and addressing security weaknesses reported to it by Computers for Schools refurbishment centres.

The follow-up

LAC and IC report that the four 2010 audit recommendations have been fully implemented.

The Computers for Schools Program has developed a new surplus certification report. Any computer donation is accompanied by a signed statement that the material provided is complete and in good working condition, and that all computer and laptop hard drives listed on the report have been electronically wiped of any protected information.

Furthermore, a revised security questionnaire is received annually from each refurbishment centre and it is analyzed to identify and address potential security gaps or weaknesses.

LAC has confirmed that all contracts for off-site destruction services include shredding specifications that meet federal government security requirements. The contracts also include standard clauses to provide an adequate level of periodic monitoring.

In addition, service providers must issue certificates of destruction, recording the date that records are destroyed and the name of the authorized contractor personnel who conducted and/or witnessed the destruction.

6.3.2 Wireless audit follow-up

Background

Tens of thousands of federal public servants have been issued smart phones or other portable devices with which they can communicate by voice or data. Some departments and agencies maintain wireless networks, enabling public servants equipped with laptops and other mobile devices to connect to their office computers.

Such wireless technologies bring flexibility and convenience but also present privacy risks.

Five organisations were selected for audit examination: Canada Mortgage and Housing Corporation, Correctional Service of Canada, Health Canada, Human Resources and Skills Development Canada, and Aboriginal Affairs and Northern Development Canada (then known as Indian and Northern Affairs Canada).

The audit

Our audit, also completed in October 2010, found that the five selected institutions had policies, procedures and processes for managing personal information transmitted to and stored within their wireless environments. Our Office however, identified weaknesses that needed to be addressed, including:

- none of the institutions had fully assessed the threats and risks inherent in wireless technologies;
- only three of the five institutions had implemented strong password protection protocols for smart phones;
- none of the institutions had established a requirement to encrypt data stored in the memory of wireless devices;
- four of the five institutions did not have documented procedures to mitigate the risk of a data breach resulting from a lost or stolen device; and
- with one exception, the institutions did not, as a general practice, educate staff on how to use wireless devices in a manner that protects privacy.

We also found that all of the audit institutions allowed PIN-to-PIN or peer-to-peer messaging. Yet none were able to demonstrate that they had implemented measures to address the security issues associated with the use of this communication method, as recommended by Communications Security Establishment Canada (CSEC). Finally, we noted weaknesses surrounding the management of surplus wireless devices.

The follow-up

We followed up with the five institutions to assess whether they had acted on their commitments concerning our recommendations. Of the 30 audit recommendations that were collectively accepted, the institutions reported that 29 had been fully implemented; the remaining one recommendation has been substantially implemented. The remedial actions taken include:

- completing threat and risk assessments on wireless networks;
- incorporating privacy risks and mitigation techniques into various staff awareness initiatives;
- formalizing processes to address lost and stolen wireless devices;
- implementing password protection and data encryption policies;

- implementing policies and processes to restrict the use of pin-to-pin messaging; and
- introducing mechanisms to provide assurance that data stored on surplus wireless devices is purged before disposal.

The measures implemented by the five institutions to address our recommendations will mitigate the privacy risks posed by wireless technologies and devices.

6.4 INQUIRIES

Our Information Centre responds to requests for information about privacy rights and responsibilities from the public and organisations. In 2012-13, we received almost 10,000 such requests.

Over 25% of information requests were connected to the *Privacy Act,* ranging over a wide variety of issues. Some of the more common questions concerned how individuals can access their personal information held by government departments; how our Office's complaint process operates; and how legislation applies in the case of lost information or accidental disclosure.

Almost a third of the requests dealt with matters where our Office has no jurisdiction. In those cases we offer assistance by referring individuals to other organisations or by suggesting ways to resolve issues or track down information.

6.5 SUPPORTING PARLIAMENT

Parliamentary appearances

During 2012-13, our Commissioner, Assistant Commissioner and other officials from our Office made nine formal appearances before Members of Parliament and Senators. We also made two written submissions to parliamentary committees.

The matters covered included:

- privacy implications of border security measures affecting travellers in the omnibus Bill C-45 (details in Chapter 5);
- new legislation related to financial transparency of First Nations (Bill C-27) and unions (Bill C-377) (details below);
- amendments to the *Criminal Code* limiting warrantless interceptions by police in emergencies also in Bill C-55 (details in Chapter 5);
- the OPC's Main Estimates;
- special study on social media led by the Standing Committee on Access to Information, Privacy and Ethics (ETHI) on which we appeared twice; and

- *Privacy Act* and PIPEDA Annual Reports, also at ETHI.

6.5.1 Financial accountability and transparency of First Nations

Bill C-27, an *Act to Enhance the Financial Accountability and Transparency of First Nations*, requires that First Nations chiefs and councillors provide an audited schedule of remuneration every year to the Minister of Aboriginal Affairs and Northern Development.

The schedule covers any payments by the First Nation, or any entity it controls, to its chief and each of its councillors, acting in either their official or personal capacity. The bill also requires that First Nations publish the schedule on their websites, and make copies available upon request. Additionally, the Minister is required to publish the schedules on the department's website.

During her appearance before the House of Commons Standing Committee on Aboriginal Affairs, the Commissioner advised committee members that the *Privacy Act* allows disclosure of personal information without consent where so authorized by another Act of Parliament (in this case, Bill C-27 itself).

So the issue was not the legality of the legislation, but rather striking a balance between two equally important democratic principles—accountability and privacy. The Commissioner offered several considerations for the Committee to take into account particularly in weighing the proportionality of the legislation and considering less privacy-intrusive alternatives. Overall, the Commissioner presented the committee with a four-step analytical framework to find the right balance between achieving stated policy objectives and the protection of privacy.

The framework can be summarized by four key questions about a government initiative or program:

The first evaluates whether a measure proposed under an initiative or program is required to achieve the stated policy objectives;

The next question considers whether the proposed measure will be successful in achieving the stated policy goal. There may be instances where the proposed measure may not be particularly effective in achieving the objectives for which it was designed;

The third question—which focuses on proportionality—functions as a sort of balancing test to help determine whether the salutary effects of the proposed measure outweigh the potentially harmful effects on the privacy of individuals; and

Finally, the fourth question asks whether the proposed measure can be substituted by another measure that might have a less adverse effect on privacy.

The bill received Royal Assent March 27, 2013.

6.5.2 *Income Tax Act* requirements for labour organisations

Private member's Bill C-377 was introduced in the House of Commons December 5, 2011, by Conservative MP Russ Hiebert. The legislation would amend the *Income Tax Act* to require every labour organisation and labour trust to file with the Minister of National Revenue a public information return for the year, within six months after the end of each fiscal period.

The Minister would then be required to make publicly available the information in those returns, including on the departmental web site in a format that allows for word searches to be performed and for cross-referencing of data.

The Commissioner appeared before the Standing Committee on Finance on November 7, 2012, in a panel with seven other witnesses. She indicated that Bill C-377 raised serious privacy concerns and, in a way similar to Bill C-27, proposed the four-step analytical framework to evaluate whether the bill struck the right balance between transparency and accountability on the one hand and the privacy rights of individuals on the other.

In an appearance before the committee on October 25, 2012, Mr. Hiebert suggested amendments to his bill that would have mitigated the privacy intrusive provisions. Since the Committee did not report back to the Commons before the end of a 30-day extension however, Bill C-377 was deemed reported without amendment on November 27, 2012.

On December 7, 2012, in the Commons, Mr. Hiebert and the Opposition submitted again several amendments to address various issues stemming from C-377; only those introduced by the MP were passed. Some did address privacy issues, such as an amendment to eliminate the risk of disclosing personal information about individuals receiving health care, pension, or other types of benefits under a registered benefit plan. Another successful amendment removed home addresses from the reporting requirements.

The Commissioner appeared once again on C-377 following its reference to the Senate Standing Committee on Banking, Trade and Commerce in May 2013, where she expressed greater comfort with the amended version of the bill and offered some opportunities for further clarifying the legislative intent.

In late June, the Senate passed an amendment which obviated the main provisions of C-377. The future of the legislation was uncertain at the time of writing this report.

Other parliamentary activities

During 2012-13, our Office examined eight bills and three committee studies to analyze the potential privacy implications of the legislation and of the recommendations in the committee reports (i.e. cyberbullying, social media, etc.). We had more than 52 formal interactions with parliamentarians and clerks, including follow-ups to committee appearances, subject-matter inquiries from MPs

and Senators, face-to-face meetings and technical briefings.

6.6 OUTREACH

A vital part of our public sector work is outreach to as many as possible of the 250 federal institutions that fall under the authority of the *Privacy Act*.

Our goals are to promote the importance of notifying our Office of privacy breaches, to help federal institutions resolve outstanding privacy matters and to make clear our expectations for the completion of Privacy Impact Assessments (PIAs).

6.6.1 Privacy Impact Assessment Workshop

For the fourth consecutive year, we hosted a PIA workshop attended by more than 60 privacy and data protection officials from federal institutions.

Introducing a new format, this year's workshop featured two panel discussions which focused on information technology (IT) privacy and security and multi-institutional PIAs.

Experts from the Communications Security Establishment Canada and our Office were on hand to answer questions related to IT security and privacy. Officials from Citizenship and Immigration Canada, the Royal Canadian Mounted Police and the Canada Border Services Agency provided attendees with practical advice about how they coordinated and produced a multi-institutional PIA for the Temporary Residents Biometrics Project.

While our Office is gratified by the number of federal public servants who wish to attend our large workshops, in the future we plan to deliver smaller PIA sessions on more specialized topics. This will also allow us to tailor these sessions to both beginners and advanced privacy officers.

To assist with our development of these smaller PIA sessions, we conducted a survey in December 2012 to gauge the level of PIA experience within federal government institutions and to assess the PIA needs and interests of the privacy community. We received valuable feedback through 121 completed surveys.

6.6.2 Access to Information and Privacy outreach

We continue to be pleased with the popularity of a Community Breakfast which we organize along with the Office of the Information Commissioner of Canada for Access to Information and Privacy (ATIP) professionals in federal institutions. ATIP professionals from 46 institutions attended the breakfast in February.

We believe the event helped strengthen relations with the ATIP community for both our Office and for the Information Commissioner's Office. ATIP officials took advantage of the event to share experiences and exchange ideas and to meet both

the Privacy Commissioner and the Assistant Privacy Commissioner.

Our Office had more focused consultations with ATIP officials and others from the 12 federal institutions which are the subject of the most privacy complaints. Starting this spring we discussed with them our initiatives to modernize the OPC investigative process. We sought feedback and exchanged best practices.

The modernization project had also been outlined in December 2012 at a meeting with the ATIP community convened by the Treasury Board of Canada Secretariat.

6.6.3 Speeches and presentations

Commissioner Stoddart made presentations to the staff at the Library of Parliament and before a gathering of federal Deputy Ministers where she explained the key ways in which our Office works with federal institutions while outlining key privacy trends across the public sector. Among her key themes was the issue of inappropriate access to personal information which is explored in depth in Chapter 3.

Following reports of two breaches, Assistant Commissioner Chantal Bernier accepted the invitation to address managers and employees at Human Resources and Skills Development Canada in late January. The Assistant Commissioner called attention to the importance of data protection and advised on fundamental practices responsible organisations should observe.

In February, the Assistant Commissioner delivered a presentation to managers of Public Safety Canada, National Defence and Citizenship and Immigration Canada portfolios at the Department of Justice Canada, where she addressed the interface between privacy and security matters.

On a similar note, in March, Commissioner Stoddart accepted an invitation to address the senior management team at Canada Border Services Agency in April. The invitation came following a letter the Commissioner sent to CBSA's President raising issues related to the late submission to our Office of the PIA dealing with phase I of the Entry/Exit system (discussed in Chapter 5) along with concerns about the Agency's plans for audio monitoring at airports and its integrity questionnaire (each discussed earlier in Chapter 6).

6.7 RESEARCH

To meet the challenges of a complex and rapidly evolving privacy environment, our research specialists actively seek out new issues and analyze them to provide foundational knowledge on priority areas. Developing and sharing knowledge gained through this research is a crucial feature of the OPC's mission to promote and protect the privacy rights of individuals.

Partly because of the complex and rapidly evolving privacy environment, we are finding the work we do on a particular issue is often relevant to our mandates under both the private and public sector. Examining issues from such different points of view has helped build a strong basis for advising Parliament, developing policy positions, conducting investigations and promoting public awareness of privacy issues in general.

Technologies and techniques used in one sector can have various applications. For example, the reports we prepared on facial recognition and predictive analytics illustrate issues that straddle both public and private mandates.

6.7.1 Facial recognition

A convergence of factors, such as the proliferation of surveillance cameras, cheap mass data storage and camera-equipped smart phones, has meant that facial recognition has become a viable and increasingly accurate technology for governments, law enforcement and commercial interests.

Our Office prepared a research report on facial recognition technology which explores these developments. The report concludes that researchers and policy-makers are only beginning to catch up in considering the societal implications of this technology.

6.7.2 Predictive analytics

Predictive analytics is another area where the social implications have yet to be fully explored. Our research report examined the mining of customer data for clues about personal habits, preferences and shopping intentions, and explained that the techniques are equally applicable to the public sector.

Our examination of this issue is part of a continuing effort to understand the value of big data to organisations, in both the private and public sector, and to reflect on the privacy implications of such emerging technologies.

6.7.3 Unmanned aerial vehicles

Also this past year, we began exploring the privacy impacts of unmanned aerial vehicles (UAVs), commonly referred to as "drones." The intention was to learn about some of the current and prospective uses for UAVs domestically by public and private sector organisations, to understand the current regulation of UAV flight, and to identify any important privacy concerns that could arise from the proliferation of their use in Canada.

The current state of domestic UAV use in Canada is still fairly limited, constrained by existing aviation regulations. Our Office however, realizes that their expanded use could come with considerable privacy implications depending on the purposes of their use, the context and location of their use, and the types of technology mounted on them. Our Office will therefore continue to monitor this issue closely and,

going forward, if UAV use changes in Canada, we would anticipate being engaged in discussions on this subject, as well as having an opportunity to review privacy impact assessments.

6.8 GUIDANCE

Developing practical guidance on key privacy issues is another way that the OPC strives to fulfill its mission to promote and protect the privacy rights of individuals. In 2012-13, we produced two key new guidance resources for public sector organizations: guidance on how to protect privacy in emergencies and a Privacy Breach Management Toolkit for health information.

6.8.1 Privacy Emergency Kit

Our Office completed a Privacy Emergency Kit to help public and private sector organisations subject to federal privacy laws enhance the timeliness and content of communications during an emergency, while also giving people confidence that their personal information will be handled appropriately. We were pleased to develop this guidance in consultation with several provincial and territorial privacy oversight offices across Canada.

Taking steps to anticipate information flows in emergencies forms part of a sound risk management strategy for all organisations. Far from impeding information flows, privacy laws encourage organisations to make the best preparations to help enable emergency responses in a privacy-respectful way, such as drafting policies and information-sharing protocols and to work with Public Safety Canada officials who helped share the kit during Emergency Preparedness Week.

6.8.2 Privacy Breach Management Toolkit for health information

Over the last few years, Treasury Board of Canada Secretariat (TBS) officials have coordinated an informal working group with members from several federal departments with responsibilities for delivering health-related programs.

Privacy breaches have been an area of common concern for these departments and a subgroup of that working group was asked to develop the main elements of a Privacy Breach Management Toolkit.

The Toolkit is intended to give federal institutions a common understanding of what constitutes a privacy breach and how to respond. It is based on the Privacy Breach Guidelines of the TBS but it goes further by providing tools and workflow guidance from start to finish — from containing a breach to extracting lessons from the experience.

Our Office had been monitoring the work of the subgroup and we look forward to the completion of the project, which would contribute to a consistent and comprehensive approach to breach management across departments.

6.9 ACTION BEFORE THE COURTS

In accordance with Section 42 of the *Privacy Act*, the Privacy Commissioner may apply to appear before the Federal Court, in cases where a federal institution has denied an individual access to his or her personal information. As well, the Commissioner may occasionally be the subject of an application for judicial review.

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

Here are summaries of cases in which we were involved during 2012-2013.

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

6.9.1 *X. v. Privacy Commissioner of Canada*

Court File No. 2011 FC 1266; confirmed on appeal at 2012 FCA 229

An individual filed an access request with the Social Sciences and Humanities Research Council of Canada and later complained to our Office that access to his personal information was denied. After an investigation, we determined that the complaint was **not well founded**.

The complainant sought judicial review of the report of findings issued by our Office. The application was dismissed with costs by the Federal Court. The complainant appealed to the Federal Court of Appeal which also dismissed the application with costs.

6.9.2 *X. v. Privacy Commissioner of Canada*

Court File No. 2013 FC 44

The same complainant brought a second judicial review application after our investigation into another complaint resulted in a finding of **not well founded**. The application for judicial review was struck by the Federal Court as lacking any chance of success. Our Office collected its costs concerning this proceeding.

6.9.3 *Privacy Commissioner of Canada v. Royal Canadian Mounted Police*

Court File No. T-1712-12

A court application was filed under Section 42 of the *Privacy Act* by our Office following the investigation of an access complaint against the Royal Canadian Mounted Police (RCMP) which was deemed **well founded**. The RCMP subsequently agreed to release the personal information originally requested by the complainant and we discontinued the application.

6.9.4 *X. v. Privacy Commissioner of Canada*

Court File No. T-125-13

The applicant filed an application for judicial review concerning a report of findings issued by our Office regarding the investigation of a complaint against Human Resources and Skills Development Canada. The applicant seeks to require our Office to reinvestigate the complaint. The matter is currently before the Federal Court.

6.9.5 *X. v. Her Majesty in Right of Canada, et al.*

Court File No. CV-12-0716-00

The plaintiff in this matter filed an action against 30 different named defendants who represent a mix of federal, provincial, and municipal entities and their employees. Included among the defendants are the Privacy Commissioner and employees of the Office of the Privacy Commissioner of Canada.

Regarding the OPC employees, the plaintiff's claims concern our Office's investigation into a complaint the plaintiff filed against Human Resources and Skills Development Canada. The plaintiff seeks damages from all defendants. The matter is currently before the Ontario Superior Court of Justice.

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

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

- The public interest in disclosure clearly outweighs any resulting invasion of privacy; or
- The disclosure would clearly benefit the individual to whom the information relates.

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

Our Office reviews the intended disclosures and may express any concerns with the proposed disclosures or recommend that the individual whose personal information is being disclosed be notified of the disclosure if the institution has not already done so. If the department declines to notify the individual, the Privacy Commissioner is empowered to do so.

The decision to release personal information in the public interest however, is ultimately at the discretion of the head of the institution and the Commissioner has no authority to prevent it.

During 2012-2013 our Office reviewed how we handled notices from institutions intending to make

public interest disclosures to ensure we respond appropriately. Some government departments also consulted with us to review their policy and procedure documents on the processing of disclosures in the public interest.

In 2012-2013, we handled 85 disclosure notifications under section 8(2)(*m*), down from 107 in the previous fiscal year. The following highlights some disclosure notifications our Office received.

6.10.1 *Royal Canadian Mounted Police*

The Royal Canadian Mounted Police notified our Office of 19 public interest disclosures in 2012-13, the highest number of any institution. The majority of those dealt with individuals being released into the community after serving sentences for assault or sexual assault and who were considered at a high risk to reoffend.

6.10.2 *Passport Canada*

Passport Canada (PPTC) made 16 disclosures of contact information to provincial health authorities for individuals identified as sitting close to a person with infectious tuberculosis on a commercial flight. In previous annual reports, the PPTC disclosures were included with those from the Department of Foreign Affairs and International Trade.

6.10.3 *Canada Border Services Agency*

The Canada Border Services Agency (CBSA) notified our Office of 11 public interest disclosures which largely concerned the removal from Canada of individuals on the "Wanted by the CBSA" list.

6.10.4 *Correctional Service of Canada*

Correctional Service of Canada made 11 disclosures either to advise victims before the transfer of an inmate to another penitentiary or to provide family members with an investigation report into the death of an inmate.

6.10.5 *Human Resources and Skills Development Canada*

Human Resources and Skills Development Canada notified our Office of nine public interest disclosures during the fiscal year. Many of these disclosures were made to police in cases to locate a missing person, notify the next of kin or where an individual had threatened serious harm to either himself or others.

Other public interest disclosures originated with National Defence (5), the Immigration and Refugee Protection Board (3), Transport Canada (3), the Department of Foreign Affairs and International Trade (2); Public Safety Canada (2) and one each from the Canada Revenue Agency, Canadian Human Rights Tribunal, Export Development Canada and Aboriginal Affairs and Northern Development Canada.

7.0 The Year Ahead

What concrete developments can our Office anticipate in the next 12 months? What can we clearly predict as the next stage in Canada's ongoing debate about privacy and the personal sphere? Here are a handful of issues that we can see developing over the horizon.

7.1 MANDATORY DATA BREACH NOTIFICATION

Canadians deserve more insight into how their data are being used and disclosed by the federal government.

While private actors have been responding proactively to calls for more transparency in this context, much remains to be done in connection with governmental bodies in Canada.

Similarly, data breach notification requirements in both the public and private sectors seem to be foundational elements in improving approaches to cybersecurity across the system.

Our Office has been actively discussing mandatory breach notification requirements and thresholds with other federal organisations active in cybersecurity, like the Treasury Board of Canada Secretariat, Public Safety Canada, the Royal Canadian Mounted Police and Competition Bureau Canada. It is our hope that breach notification might become mandatory across federal organisations in the near future.

7.2 UPDATING THE *PRIVACY ACT*

The logic that government should be held to a standard equal to or even higher than the private sector should resonate with many Canadians. The latest Annual Report from the Clerk of the Privy Council makes a general call for federal organisations to match the dynamism of the private sector and be held to the same standards and expectations. This is a call that should also apply to the handling of Canadians' personal information.

The past several years have featured open, detailed debate around the standards of care which citizens expect of the federal government about the treatment, sharing and safeguarding of sensitive information.

Privacy breaches from within governmental organisations, open debate on the relative merits of various technical surveillance measures, questions about how Canadian courts view the limits and appropriate protections afforded to personal information and private communications have all contributed to this discussion.

At the heart of these matters lies federal public sector privacy legislation which has not been substantively updated in three decades marked by immense technological change and greater information sharing across borders.

It is appropriate, timely and healthy for Canadians to have this debate.

7.3 SURVEILLANCE, ONLINE AND OFFLINE

Impassioned debates over the government's national security agenda and the privacy rights we enjoy as citizens can be expected to continue. The media will question, academics will study and debate, government will defend and Parliamentarians examine—all to the betterment of our open, democratic society.

With unprecedented new types of threats and rapidly expanding surveillance capacity however, our traditional bulwarks of protection for privacy now warrant serious debate in their own right.

Canada needs to recalibrate the tension between privacy and security. The debate to achieve that can only happen through discussion at all levels of our society. It is an open discussion that our Office welcomes and hopes to help facilitate through our research, speeches, reports and international work.

7.4 BLURRING OPC AND DEPARTMENTAL RESPONSIBILITIES

We have noticed an increasing trend for federal departments and agencies to "consult" with our Office and then imply publicly that the action in itself has addressed or eliminated all privacy risks. While we do our best to add value in the interest of protecting the privacy rights of Canadians, our Office does not have any power to enforce its recommendations on Privacy Impact Assessments (PIAs).

Responsibility and accountability for privacy risks must ultimately lie with the government institution. When the Access to Information and Privacy offices in agencies and departments rely too heavily on our Office, they are not building their own capacity to develop PIAs and to address privacy issues.

We are increasing our outreach to provide guidance to officials in these offices so they can be increasingly relied upon within their institutions to provide much-needed and valuable privacy expertise.

7.5 LACK OF NOTIFICATION

In the coming year, we will be closely following a developing trend that threatens to shortchange Canadians' information needs. In several PIAs received this year, our Office noted organizations deciding against posting signs to provide public notification of video observation. Our Office is told that in border areas, there is a danger of so-called 'sign clutter' and that the physical layout of some spaces makes it difficult or unsightly to keep the signs prominently displayed.

Some institutions have opted for other forms of public notification, such as a public communications plan, instead of signs. We will be following this trend closely.

7.6 MACRO-PROJECTS, MICRO-REVIEW

The Beyond the Border Action Plan presents unique challenges for PIAs. Shifting to a perimeter model for border security means that many PIAs do not take into account the myriad connections existing between, at times, numerous, separate programs and activities.

As a result, several PIAs we received this year did not take a broad enough approach to provide a cogent analysis of how the Beyond the Border changes could affect privacy in the broader context. Given the fact that more PIAs related to this undertaking are expected over the coming year, we endeavoured to communicate this issue across government, including offering a session during our annual workshop on how departments can collaborate to produce an inter-departmental PIA in the hopes that this will encourage more holistic and integrative analysis.

7.7 SHARING EVERYTHING

Cross border cooperation between governments is leading to greater and greater information sharing across borders. During the year we received several PIAs on initiatives to facilitate the systematic sharing of information with the Canadian and American federal governments. In the past, such information-sharing has occurred on a carefully considered case-by-case basis.

Our Office noted a trend this past year however, for these processes to be systematized and significantly expanded. It is expected that this trend will continue through future phases of the Beyond the Border Action Plan and various perimeter security initiatives.

Although Canada and the United States are similar in many ways, the two countries have very different privacy regimes. While our Office has endeavoured to identify the major privacy risks through the review process, it is not possible to anticipate where there may be gaps between the two jurisdictions when dealing with projects of such a broad scale and complexity.

7.8 CONSOLIDATION OF SERVICES AND OUTSOURCING

The search for efficiencies across federal institutions is ongoing and we will continue to keep a close eye on initiatives to help ensure privacy is not left behind. The move to consolidate or share services has been done formally through the establishment of Shared Services Canada, which focuses on the management of the government's information technology infrastructure, and also less formally through activities such as consolidation of human resources and finance systems by small and medium institutions.

We have also seen the federal government seek to leverage existing capacities and infrastructures for new purposes:

- within the government, such as using pre-existing systems for new biometrics storage;
- with the private sector, for such things as records storage and human resources functions.

Considering the current fiscal climate and the push to streamline program delivery, we anticipate this trend will continue. Our Office will continue to provide privacy advice to institutions as they move in this direction.

7.9 SECURITY SCREENING IN THE FEDERAL GOVERNMENT

Changes to security screenings are expected in the coming year. Over the past year, our Office examined PIAs which raised concerns about how screenings were being carried out in departments and agencies, signalling the need for research in this area.

We discovered that practices vary greatly by institution, since the Personnel Security Screening Standard from the TBS leaves much to the discretion of departmental security officers.

Within the federal government there is an increased reliance on conducting credit checks and a greater appetite to receive non-conviction information from the Royal Canadian Mounted Police rather than just information on criminal records. In addition, more and more institutions are seeking approval for enhanced screening methods such as polygraph testing and potentially invasive screening questionnaires, such as that withdrawn by the Canada Border Services Agency after a public backlash (as explained in Chapter 6).

Against this backdrop, TBS is revising the Personnel Security Screening Standard. Our Office will be working closely with officials there as the new standard is being developed to ensure a productive dialogue on any privacy risks associated with potential changes.

We have been assured that a PIA on the new standard will be conducted by TBS and expect that institutions implementing new screening practices will conduct their own assessments.

While there is a clear need to ensure the federal public service is comprised of trustworthy, reliable individuals who are loyal to the national interest, we must ensure that any invasive screening measures being implemented are proven to be necessary and effective at ensuring these qualities.

7.10 OTHER AREAS

Earlier this report described the modernization project undertaken to streamline our investigation process (Chapter 6). The coming year will see the implementation of the recommendations. While improved efficiencies are already being achieved in some areas, the full impact of some measures may take more than a year to be felt.

We continue to expand our state-of-the-art testing laboratory to further strengthen our technology support capacity in support of new investigations.

Appendix 1

DEFINITIONS

Complaint Types

1. Access

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

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

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

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

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

2. Privacy

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

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

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

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

3. Time Limits

Time limits - The institution did not respond within the statutory limits.

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

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

Findings and other Dispositions under the *Privacy Act*

1. Investigative Findings

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

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

Resolved: The evidence gathered in the investigation supports the allegations in the complaint, but the institution agreed to take corrective measures to rectify the problem, to the satisfaction of this office.

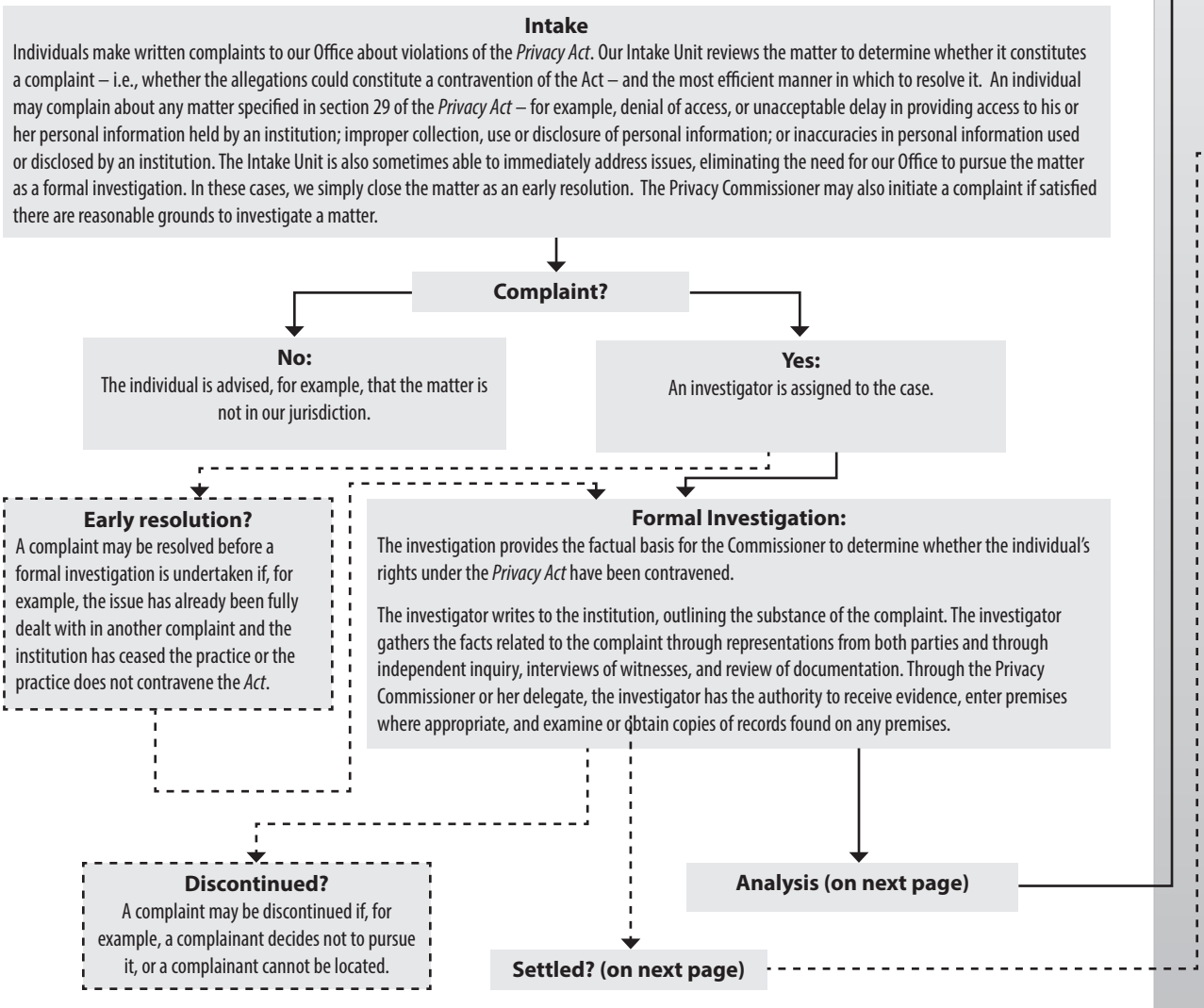
2. Other Dispositions

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

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

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

INVESTIGATION PROCESS UNDER THE *PRIVACY ACT*



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

Analysis:

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

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

Settled?

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

Findings:

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

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

The possible findings are:

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

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

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

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

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

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

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

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

Appendix 2

COMPLAINTS AND INVESTIGATIONS UNDER THE *PRIVACY ACT*, APRIL 1, 2012 TO – MARCH 31, 2013

PA Complaints Accepted by Complaint Type

	Early Resolution		Investigation		Total Count	Total Percentage
Complaint Type	**Count**	**Percentage**	**Count**	**Percentage**		
Access						
Access	92	4.05%	280	12.32%	372	**16.37%**
Correction – Notation	5	0.22%	0	0.00%	5	**0.22%**
Denial of Access	1	0.04%	0	0.00%	1	**0.04%**
Time Limits						
Time Limits	108	4.75%	305	13.42%	413	**18.17%**
Extension Notice	6	0.26%	12	0.53%	18	**0.79%**
Correction – Time Limits	3	0.13%	3	0.13%	6	**0.26%**
Privacy						
Use and Disclosure	82	3.61%	1334	58.69%	1416	**62.30%**
Collection	12	0.53%	16	0.70%	28	**1.23%**
Retention and Disposal	3	0.13%	7	0.31%	10	**0.44%**
Policy	2	0.09%	0	0.00%	2	**0.09%**
Commissioner Initiated Complaint	0	0.00%	2	0.09%	2	**0.09%**
Grand Total	**314**	**13.81%**	**1959**	**86.19%**	**2273**	**100.00%**

PA Top 10 Institutions by Complaints Accepted

Respondent	Access		Time Limits		Privacy		Commissioner Initiated Complaint	Grand Total
	Early Resolution	Investigation	Early Resolution	Investigation	Early Resolution	Investigation	Investigation	
Human Resources and Skills Development Canada	2	5	1	4	16	1001	1	**1030**
Correctional Service of Canada	24	66	47	91	16	40	0	**284**
Justice Canada	1	17	0	5	2	162	1	**188**
Royal Canadian Mounted Police	20	38	6	90	11	17	0	**182**
National Defence	8	13	19	33	1	16	0	**90**
Canada Border Services Agency	7	21	6	12	2	40	0	**88**
Canada Revenue Agency	7	32	7	14	4	12	0	**76**
Veterans Affairs Canada	1	2	7	28	4	14	0	**56**
Canadian Food Inspection Agency	2	5	10	14	0	2	0	**33**
Transport Canada	0	8	2	7	3	7	0	**27**
Grand Total	**72**	**207**	**105**	**298**	**59**	**1311**	**2**	**2054**

PA Top 10 Institutions in 2012-2013 by Complaints Accepted and Fiscal Year

Organization	2009-2010	2010-2011	2011-2012	2012-2013
Human Resources and Skills Development Canada	20	25	26	1030
Correctional Service of Canada	290	276	326	284
Justice Canada	11	9	9	188
Royal Canadian Mounted Police	60	75	117	182
National Defence	47	65	115	90
Canada Border Services Agency	26	29	55	88
Canada Revenue Agency	49	53	65	76
Veterans Affairs Canada	2	15	39	56
Canadian Food Inspection Agency	0	8	3	33
Transport Canada	8	14	6	27
Grand Total	**513**	**569**	**761**	**2054**

PA Complaints Accepted by Institution

Respondent	Early Resolution	Investigation	Grand Total
Aboriginal Affairs and Northern Development Canada	3	15	18
Agriculture And Agri-food Canada	8	1	9
Canada Border Services Agency	15	73	88
Canada Economic Development for Quebec Regions	0	2	2
Canada Post Corporation	14	7	21
Canada Revenue Agency	18	58	76
Canada School of Public Service	0	1	1
Canadian Broadcasting Corporation	1	0	1
Canadian Food Inspection Agency	12	21	33
Canadian Heritage	0	1	1
Canadian Human Rights Commission	1	1	2
Canadian Human Rights Tribunal	0	2	2
Canadian Museum of Civilization	0	1	1

PA Complaints Accepted by Institution (cont.)

Respondent	Early Resolution	Investigation	Grand Total
Canadian Radio-Television and Telecommunications Commission	1	0	1
Canadian Security Intelligence Service	3	16	19
Citizenship and Immigration Canada	11	6	17
Correctional Service of Canada	87	197	284
Elections Canada	1	1	2
Environment Canada	1	1	2
Fisheries and Oceans	1	6	7
Foreign Affairs and International Trade	2	5	7
Health Canada	1	5	6
Human Resources and Skills Development Canada	19	1011	1030
Immigration and Refugee Board	3	0	3
Indian Residential Schools Resolution Canada	1	0	1
Industry Canada	2	1	3
Justice Canada	3	185	188
Library and Archives Canada	1	0	1
Military Police Complaints Commission	0	3	3
National Defence	28	62	90
Natural Resources Canada	0	1	1
Natural Sciences and Engineering Research Council of Canada	0	1	1
Office of Infrastructure of Canada	0	1	1
Office of the Commissioner of Official Languages	0	1	1
Office of the Correctional Investigator Canada	1	1	2
Office of the Information Commissioner of Canada	1	1	2
Parks Canada Agency	1	0	1
Parole Board of Canada	0	1	1
Passport Canada	6	3	9
Privy Council Office	0	2	2
Public Health Agency of Canada	3	4	7
Public Prosecution Service of Canada	0	2	2

PA Complaints Accepted by Institution (cont.)

Respondent	Early Resolution	Investigation	Grand Total
Public Safety Canada	1	2	3
Public Sector Integrity Canada	0	1	1
Public Service Commission Canada	0	3	3
Public Service Staffing Tribunal	1	0	1
Public Works And Government Services Canada	3	17	20
Royal Canadian Mint	0	2	2
Royal Canadian Mounted Police	37	145	182
Royal Canadian Mounted Police External Review Committee	0	1	1
Service Canada	2	1	3
Shared Services Canada	2	0	2
Social Science and Humanities Research Council of Canada	0	1	1
Statistics Canada	1	17	18
Transport Canada	5	22	27
Transportation Safety Board of Canada	0	1	1
Treasury Board of Canada Secretariat	1	1	2
Veterans Affairs Canada	12	44	56
Veterans Review and Appeal Board Canada	0	1	1
Grand Total	**314**	**1959**	**2273**

PA Complaints Accepted by Province/Territory

	Early Resolution		Investigation		Total Count	Total Percentage
Province / Territory	Count	Percentage	Count	Percentage		
Alberta	27	1.19%	134	5.90%	161	7.08%
British Columbia	64	2.82%	197	8.67%	261	11.48%
Manitoba	18	0.79%	33	1.45%	51	2.24%
New Brunswick	9	0.40%	31	1.36%	40	1.76%
Newfoundland and Labrador	1	0.04%	15	0.66%	16	0.70%
Northwest Territories	0	0.00%	2	0.09%	2	0.09%
Not specified	1	0.04%	3	0.13%	4	0.18%
Nova Scotia	18	0.79%	56	2.46%	74	3.26%
Ontario	129	5.68%	1260	55.43%	1389	61.11%
Other (Not US)	1	0.04%	6	0.26%	7	0.31%
Prince Edward Island	1	0.04%	7	0.31%	8	0.35%
Quebec	33	1.45%	164	7.22%	197	8.67%
Saskatchewan	8	0.35%	23	1.01%	31	1.36%
United States	4	0.18%	1	0.04%	5	0.22%
(blank)	0	0.00%	27	1.19%	27	1.19%
Grand Total	**314**	**13.81%**	**1959**	**86.19%**	**2273**	**100.00%**

PA Dispositions by Complaint Type

Complaint Type	Well-founded	Well-founded resolved	Not well-founded	Resolved	Discontinued	ER-Resolved	No Jurisdiction	Settled	Grand Total
Access									
Access	24	46	117	18	21	101	4	23	354
Correction – Notation	0	0	0	0	0	6	0	0	6
Language	0	0	0	0	2	0	0	0	2
Fees	0	0	0	0	1	0	0	0	1
Time Limits									
Time Limits	197	0	12	2	13	108	0	2	334
Extension Notice	3	0	3	0	1	6	0	0	13
Correction – Time Limits	2	0	0	0	0	0	0	0	2
Privacy									
Use and Disclosure	49	1	25	1	18	64	1	7	166
Collection	1	0	6	0	4	10	0	1	22
Retention and Disposal	0	0	3	1	0	2	0	0	6
Policy	0	0	0	0	0	2	0	0	2
Grand Total	**276**	**47**	**166**	**22**	**60**	**299**	**5**	**33**	**908**

PA Dispositions of Time Limits by Institution

Respondent	Well-founded	Not well-founded	Resolved	Discontinued	ER-Resolved	Settled	Grand Total
Aboriginal Affairs and Northern Development Canada	0	0	0	0	1	0	1
Canada Border Services Agency	8	2	0	0	8	0	18
Canada Post Corporation	0	1	0	0	0	0	1
Canada Revenue Agency	16	1	0	0	4	0	21
Canadian Food Inspection Agency	12	0	0	0	10	0	22
Citizenship and Immigration Canada	2	0	0	1	3	0	6
Correctional Service of Canada	65	3	1	1	34	0	104
Fisheries and Oceans	2	1	0	0	0	0	3
Foreign Affairs and International Trade	1	0	0	0	2	0	3
Health Canada	0	0	0	0	1	0	1
Human Resources and Skills Development Canada	4	0	0	1	1	0	6
National Defence	39	1	1	10	27	0	78
Natural Resources Canada	1	0	0	0	0	0	1
Parks Canada Agency	0	0	0	0	1	0	1
Public Health Agency of Canada	0	0	0	0	2	0	2
Public Prosecution Service of Canada	1	1	0	0	0	0	2
Public Works And Government Services Canada	5	0	0	0	1	0	6
Royal Canadian Mint	0	1	0	0	0	0	1
Royal Canadian Mounted Police	32	2	0	1	7	2	44
Statistics Canada	0	2	0	0	0	0	2
Transport Canada	4	0	0	0	3	0	7
Treasury Board of Canada Secretariat	0	0	0	0	1	0	1
Veterans Affairs Canada	10	0	0	0	7	0	17
Service Canada	0	0	0	0	1	0	1
Grand Total	**202**	**15**	**2**	**14**	**114**	**2**	**349**

PA Dispositions of Access and Privacy Complaints by Institution

Respondent	Well-founded	Well-founded resolved	Not well-founded	Resolved	Discontinued	ER-Resolved	No Jurisdiction	Settled	Grand Total
Aboriginal Affairs and Northern Development Canada	1	0	1	0	0	2	0	0	4
Agriculture And Agri-food Canada	0	0	1	0	0	8	0	0	9
Canada Border Services Agency	3	2	11	3	4	14	0	2	39
Canada Post Corporation	1	2	2	0	2	17	0	2	26
Canada Revenue Agency	4	5	20	2	1	11	0	3	46
Canadian Broadcasting Corporation	0	0	1	0	0	1	0	0	2
Canadian Food Inspection Agency	1	0	1	0	0	2	0	0	4
Canadian Forces Grievance Board	0	1	0	0	0	0	0	0	1
Canadian Human Rights Commission	0	2	0	0	0	1	0	0	3
Canadian Human Rights Tribunal	0	0	1	0	0	0	0	1	2
Canadian Radio-Television and Telecommunications Commission	0	0	0	0	0	1	0	0	1
Canadian Security Intelligence Service	0	0	18	0	1	3	0	0	22
Canadian Space Agency	0	0	3	0	0	0	0	0	3
Citizenship and Immigration Canada	1	6	5	0	0	5	0	1	18
Correctional Service of Canada	49	10	38	7	11	44	1	4	164
Elections Canada	0	0	0	0	0	1	0	0	1
Environment Canada	0	1	0	0	0	1	0	0	2
Fisheries and Oceans	0	0	2	1	0	1	0	0	4
Foreign Affairs and International Trade	0	0	1	0	0	0	0	0	1
Health Canada	0	0	1	0	0	0	0	1	2
Human Resources and Skills Development Canada	1	3	2	0	1	8	0	3	18
Immigration and Refugee Board	0	0	1	0	1	0	0	0	2
Indian Residential Schools Resolution Canada	0	0	0	0	0	1	0	0	1
Industry Canada	0	1	1	0	0	2	0	1	5
Justice Canada	0	1	0	0	1	3	0	1	6
Library and Archives Canada	0	0	0	0	0	0	0	1	1
Military Police Complaints Commission	0	0	0	0	1	0	0	0	1
National Defence	4	3	8	2	1	11	0	5	34

PA Dispositions of Access and Privacy Complaints by Institution (cont.)

Respondent	Well-founded	Well-founded resolved	Not well-founded	Resolved	Discontinued	ER-Resolved	No Jurisdiction	Settled	Grand Total
National Gallery of Canada	0	0	0	0	1	0	0	0	1
National Research Council Canada	0	1	1	0	0	0	0	0	2
Natural Resources Canada	0	1	1	0	1	0	0	0	3
Office of the Correctional Investigator Canada	0	0	0	0	0	1	0	0	1
Office of the Information Commissioner of Canada	0	0	0	0	0	1	0	0	1
Parks Canada Agency	1	0	0	0	0	0	0	0	1
Parole Board of Canada	0	0	0	0	1	0	3	0	4
Passport Canada	0	0	1	0	0	3	0	0	4
Public Health Agency of Canada	0	1	0	0	5	1	0	0	7
Public Prosecution Service of Canada	0	0	1	0	0	0	0	0	1
Public Safety Canada	0	0	1	0	0	1	0	0	2
Public Service Staffing Tribunal	0	0	0	0	0	1	0	0	1
Public Works And Government Services Canada	0	1	6	1	0	2	0	0	10
Royal Canadian Mounted Police	6	4	19	4	10	28	0	6	77
Shared Services Canada	0	0	0	0	0	1	0	0	1
Statistics Canada	1	1	0	0	0	1	0	0	3
Transport Canada	0	0	0	0	1	3	0	0	4
Treasury Board of Canada Secretariat	0	0	0	0	0	1	0	0	1
Veterans Affairs Canada	1	0	3	0	2	4	1	0	11
Veterans Review and Appeal Board Canada	0	0	0	0	1	0	0	0	1
VIA Rail Canada	0	1	0	0	0	0	0	0	1
Grand Total	**74**	**47**	**151**	**20**	**46**	**185**	**5**	**31**	**559**

PA Treatment Times - Early Resolution Cases by Complaint Type

Complaint Type	Count	Average Treatment Time (Months)
Access		
Access	101	2.12
Correction – Notation	6	1.26
Time Limits		
Time Limits	108	2.42
Extension Notice	6	0.20
Privacy		
Use and Disclosure	64	2.48
Collection	10	2.12
Policy	2	2.38
Retention and Disposal	2	2.23
Grand Total	**299**	**2.25**

PA Treatment Times - Formal Investigations by Complaint Type

Complaint Type	Count	Average Treatment Time (Months)
Access		
Access	264	11.82
Language	2	21.61
Fees	1	19.11
Time Limits		
Time Limits	228	4.46
Extension Notice	7	4.99
Correction – Time Limits	2	6.41
Privacy		
Use and Disclosure	111	10.69
Collection	14	8.88
Retention and Disposal	4	15.43
Grand Total	**633**	**8.88**

PA Treatment Times - All Closed Files by Disposition

Disposition	Count	Average Treatment Time (Months)
Formal Complaints		
Well-founded	276	7.10
Not well-founded	166	10.80
Discontinued	60	9.07
Well-founded resolved	47	14.51
Settled	33	8.68
Resolved	22	10.62
ER-Unsuccessful	17	3.23
ER-Unsuitable	7	4.11
No Jurisdiction	5	7.97
ER-Resolved	**299**	**2.25**
Grand Total	**932**	**6.75**

PA Incidents by Institution

Respondent	Incident
Canada Revenue Agency	22
Correctional Service of Canada	17
Human Resources and Skills Development Canada	11
Foreign Affairs and International Trade	10
Citizenship and Immigration Canada	5
Veterans Affairs Canada	5
Canada Post Corporation	4
Statistics Canada	4
National Defence	3
Royal Canadian Mounted Police	2
Passport Canada	2
Shared Services Canada	2
Fisheries and Oceans	2
Export Development Canada	2
Health Canada	2
Aboriginal Affairs and Northern Development Canada	2
Canadian Air Transport Security Authority	2
Elections Canada	1
Canadian Food Inspection Agency	1
The Pierre Elliott Trudeau Foundation	1
Library and Archives Canada	1
Canadian Radio-Television and Telecommunications Commission	1
Canadian Human Rights Commission	1
Environment Canada	1
Financial Transactions and Reports Analysis Centre of Canada	1
Transport Canada	1
Public Prosecution Service of Canada	1
Justice Canada	1
Public Works And Government Services Canada	1
Grand Total	**109**