Annual Report to Parliament 2014-2015

PROTECTING PERSONAL INFORMATION AND PUBLIC TRUST

Report on the *Privacy Act*

Office of the
Privacy Commissioner
of Canada

2014-2015 *Privacy Act* Annual Report to Parliament
Protecting personal information and public trust

Office of the Privacy Commissioner of Canada
30 Victoria Street – 1st Floor
Gatineau, QC
K1A 1H3

(819) 994-5444, 1-800-282-1376

Cat. No. IP50E-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

30 Victoria Street
Gatineau, Quebec
K1A 1H3
Tel.: (613) 947-1698
1-800-282-1376
www.priv.gc.ca

Commissaire à la protection de la vie privée du Canada

30, rue Victoria
Gatineau (Québec)
K1A 1H3
Tél. : (613) 947-1698
1-800-282-1376
www.priv.gc.ca

December 2015

The Honourable George Furey, Senator
The Speaker
The Senate of Canada
Ottawa, Ontario K1A 0A4

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Privacy Act* for the period from April 1, 2014 to March 31, 2015.

Sincerely,

Original signed by

Daniel Therrien
Privacy Commissioner of Canada

Privacy Commissioner of Canada

30 Victoria Street
Gatineau, Quebec
K1A 1H3
Tel.: (613) 947-1698
1-800-282-1376
www.priv.gc.ca

Commissaire à la protection de la vie privée du Canada

30, rue Victoria
Gatineau (Québec)
K1A 1H3
Tél. : (613) 947-1698
1-800-282-1376
www.priv.gc.ca

December 2015

The Honourable Geoff Regan, P.C., M.P.
The Speaker
The House of Commons
Ottawa, Ontario K1A 0A6

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Privacy Act* for the period from April 1, 2014 to March 31, 2015.

Sincerely,

Original signed by

Daniel Therrien
Privacy Commissioner of Canada

Table of Contents

TO NOTE: In November 2015, some federal institutions were renamed. In this report, all institutions are referred to by the names they operated under during fiscal year 2014-2015.

Commissioner's Message

When I was appointed in early June of 2014—a few weeks into the 2014-2015 fiscal year covered by this report—I said that my overarching goal as Privacy Commissioner would be increasing the control Canadians have over their personal information.

As technology continues to evolve, it enables the collection and analysis of our personal information in ways and at a scale we could barely have imagined even a few years ago. These advances in data analytics may be used by federal institutions to improve their performance and delivery of services to Canadians and protect public safety.

At the same time, however, institutions need to develop and implement sufficient procedures to ensure this data is appropriately collected, used and protected and the *Privacy Act* respected. This need along with important questions about oversight and transparency have been highlighted evermore strongly given new laws proclaimed in the last year, giving federal institutions an unprecedented ability to disclose Canadians' personal information without individual knowledge and consent. In chapter three, this report looks back at three surveillance-related bills on which we commented before Parliament and some of our plans going forward to protect privacy upon their implementation.

This report, which also focuses on data breaches reported to our Office, and results of investigations and an audit we conducted, highlights the importance of developing and implementing rigorous procedures and safeguards to protect Canadians' information.

Guarding against breaches and preventing privacy violations can be a challenge that we do not want to minimize. However, given that Canadians are required to provide very sensitive information to federal departments and agencies, the government's duty of care is paramount.

Many institutions have made some strides to better protect personal information. This said, the over 250 data breaches reported to our Office during the reporting period, some of the investigations we summarize in this report and the results of our audit into the management of portable storage devices suggest there is still much room for improvement.

FOCUS ON DATA BREACHES

Data breaches diminish both the control individuals have over their personal information, as well as their confidence in institutions with which they entrust it. With our feature in chapter four, this report takes a close look at some of the more significant breaches, how they happened, and the responsible institutions' efforts to respond to these incidents and help prevent similar incidents from happening in the future.

The past year was the first in which the Treasury Board President's revised directive on data breach reporting required institutions to report "material" breaches of personal information to both our Office and Treasury Board of Canada Secretariat (TBS).

Mandatory reporting is an important step forward. As noted in previous annual reports, when reporting was voluntary, it was impossible to know whether the significant increases we were seeing in recent years indicated that there were more data breaches occurring, or whether institutions had simply been more diligent in reporting.

Having nearly a full fiscal year of institutions operating under the new requirements, we are starting to gain better insight into federal breaches, which should provide a clearer baseline for comparison in the future. Understanding why and how breaches occur, how to guard against them, and how to mitigate the risk to Canadians when they do happen was a major focus for the Office over the past year and will remain so going forward.

While we did see some cases where network vulnerabilities and technological glitches led to the disclosure of Canadians' personal information, our review of data breaches reported during 2014-2015 found that—as in previous years—accidental disclosure, a risk which can often be mitigated by more rigorous procedures, was the leading cause. In fact, accidental disclosure was by far the largest category of data breaches, representing 73 percent of the total number reported.

Knowing that nearly three quarters of breaches could have been prevented with greater care is a concern. It shows that institutions are still suffering breaches stemming from misdirected

mail or overly large envelope windows despite years and years of similar episodes. Relatively simple steps can and must be taken to curtail these types of breaches. It is my hope that this year's annual report will serve as a reminder of the need for greater vigilance.

IMPACT OF BREACHES

The consequences of a data breach, however unintentional, can be significant.

In one example, detailed in chapter four, the Canada Revenue Agency (CRA) accidentally delivered the personal information belonging to more than 1,000 individuals and businesses to a CBC journalist. The CBC subsequently released a story in which it identified several of the individuals affected by the breach.

Another case detailed an incident where Health Canada sent letters to more than 41,000 people across Canada in envelopes that showed the letters were from the Marihuana Medical Access Program. The fact that an individual is enrolled, or has an interest, in a program that allows access to marihuana for medical purposes is clearly very sensitive information which should not be disclosed without explicit consent.

In a further case, the names of individuals requesting records under the *Access to Information Act* related to a former Aboriginal Affairs and Northern Development Minister's expenses were revealed to departmental personnel who had no need to know such information.

Each of these three cases—along with others featured in this report—called upon institutions to further improve and follow procedures to strengthen their protection of personal information and get results needed to maintain Canadians' trust.

PORTABLE STORAGE DEVICES AUDIT

Our audit completed in 2014-2015 also called upon many institutions to adopt or improve procedures to safeguard personal information held on portable storage devices. These range from small hard drives to even smaller devices—such as USB keys or memory sticks. Their small size and portability, coupled with their capacity to store large amounts of data, make them a valuable tool. Unfortunately, these same characteristics mean they can also be easily lost or stolen.

Following a number of breaches involving portable storage devices affecting thousands of Canadians, our Office initiated a horizontal audit of the management of these devices within federal institutions during 2014.

Our audit, described in chapter five, found that while progress has been made in reducing the risk, there are opportunities for improvement. I encourage all institutions to examine our findings to seek ways to improve their management of portable devices so they

can continue benefiting from such useful tools while reducing the likelihood of a breach within their organizations. Such action could help the federal government better safeguard data and help reduce the number of breaches reported per year.

COMPLAINTS

The number of complaints related to the handling of Canadians' personal information by federal institutions to our Office during the fiscal year increased slightly compared to the previous year, discounting a significant number submitted by a small group of individuals. Including these, our Office accepted a total of 3,977. Minus those in abeyance, the figure stood at 1,040, for a slight yearly increase.

As demands increase, we continue striving for ways to bring about results for parties as effectively as possible. In an effort to better manage demands on our limited resources, our Office has adopted a number of strategies including, where appropriate, resolving complaints through conciliation and negotiation. I am pleased to say that the number of complaints we are able to resolve through our early resolution process, which sees the needs of complainants satisfied without requiring a standard, resource-intensive investigation continues to rise. In the past year, a total of 422 complaints were settled this way.

UNDERSTANDING CANADIANS' PRIVACY PRIORITIES

In 2014-2015 we undertook a wide-ranging effort to identify the key privacy issues that are most significantly affecting Canadians in order to increase the overall control they have over their personal information. Our aim was to identify strategic privacy priorities that will guide some of our Office's work over the next five years.

To do so, we engaged stakeholders across Canada—meeting with civil society and consumer advocacy groups, our provincial counterparts, industry and legal service providers, academia, and government—to hear their views on what would be the defining privacy issues of greatest relevance to Canadians between now and 2020. We consulted individual Canadians through focus groups.

This process was immensely helpful and I am grateful for the contribution of stakeholders and individuals who took the time to participate and share their views with us.

A report summarizing what we heard from individuals and stakeholders, as well as the identified four priorities and how we intend to address them is available on our web site, entitled "The OPC Privacy Priorities 2015-2020: Mapping a course for greater protection."

While much of the work done by the Office cannot be predicted or controlled, we *do* have some latitude in deciding which audits we launch, which compliance review work we undertake and what kind of proactive guidance and public education we conduct.

MOVING FORWARD WITH NEW STRATEGIC PRIVACY PRIORITIES

It is this discretionary work that these four strategic priorities will help to direct and focus over the coming five years.

The Economics of Personal Information

Today's information-based economy and society has spurred the commoditization of personal information and new business models being developed around the use of Big Data, the Internet of things and mobile technologies.

Canada's privacy laws are rooted in the ability of individuals having control over their personal information—and this ability hinges on the quality of consent. In an age where analytics and algorithms identify new possible uses for data not yet even conceived or imagined, many participants in our exercise questioned whether it was realistic any longer to seek one-time consent in exchange for personal information.

Our goal here is enhancing privacy protection and trust, so individuals may confidently participate in an innovative digital economy.

The Body as Information

The information generated by our bodies is uniquely personal, and can be highly sensitive. As more and more information about our bodies is collected, digitized, catalogued and analysed in biometric and DNA databases, the impacts on privacy can be profound. The exploitation of this information for commercial profit-making motives or to assist government surveillance efforts, may adversely affect not only our right to privacy in respect of our personal information, but our bodily integrity and our very dignity as human beings.

Today, the federal government is expanding its use of genetic material. In 2014, the *DNA Identification Act* was amended, adding five new categories of DNA profiles for collection, including those: from victims of crime; of missing persons and their relatives; and from individuals who provide samples voluntarily.

At the same time, federal institutions are expanding their use of biometrics as identifiers. Bill C-59, for example, which became law in June 2015, expands fingerprint collection from certain travellers to Canada. The collection and retention of fingerprints, palm prints, iris scans and facial photographs, particularly if these elements are matched to other data points already in the government's possession, can raise profound privacy issues. Our Office will be engaged on initiatives in which federal institutions seeks to make use of data both about and of Canadians to ensure the privacy

implications raised by such activities are recognized and respected.

Reputation and Privacy

The Internet and the digital society it has spawned have had a profound impact on personal reputation management. Once personal information moves online in one context, it can be extremely challenging to remove or keep it from being used in different contexts. Though people grow and change over time, the personal information posted online about them may cast a constant shadow.

The federal government has demonstrated a growing appetite for the use of publicly available personal information in the context of security screening, including information found on social media sites. This gives rise to the risk of profiling that may see people defined by their digital past.

Our goal will be to create an environment where people can use the Internet to explore their interests without fear of their digital trace leading to unfair treatment.

Government Surveillance

As documented in chapter three, the past year in Parliament has seen some dramatic shifts in the landscape around national security. With the passage of Bill C-51, the *Anti-Terrorism Act, 2015*—which includes the *Security of Canada Information Sharing Act*—Canadians can expect that more and more of their personal information will be shared with a wider range of government institutions for the broad purpose of addressing "activities that undermine the security of Canada."

Briefly, this Act enables all Government of Canada institutions to share any information they have collected about Canadians with any or all of 17 federal departments and agencies with a mandate, or part of a mandate, related to national security as long as the information is "relevant" to the recipient institution's mandate in that regard.

As I have detailed to Parliament—I believe the law's goal of enabling information sharing to identify threats is accomplished at much too great a cost to privacy. The door has been opened to the personal information of ordinary, law-abiding citizens being collected and shared disproportionately. This sets up the prospect of profiling and the use of Big Data analytics on all Canadians.

Among other concerns, the threshold for sharing information—that it be "relevant" to national security—sets the bar far too low. I had recommended amending the Bill to replace "relevant" with "necessary or proportional." In addition, there is a glaring lack of clear personal information retention and destruction obligations for organizations.

As well, the additional sharing of personal information enabled by the legislation is not accompanied by a corresponding increase in oversight. Indeed, of the 17 departments and agencies authorized to receive information for national security purposes under the legislation, only three have dedicated independent review or oversight bodies.

In the short and medium terms, we will examine and report on how national security legislation such as Bill C-51 is implemented. We intend to use our review and investigative powers to examine the collection, use and sharing practices of departments and agencies involved in surveillance activities to ensure that they comply with the *Privacy Act*. We will report our findings to parliamentarians and the public, and issue recommendations for potential improvements to policies or legislation, as warranted.

LOOKING AHEAD

While much of this report is necessarily about reviewing our activities in the past fiscal year, we must also focus on the future.

We have adopted strategic approaches to ensure that we address our privacy priorities with concrete steps. To that end, we will be promoting innovative and technological ways of protecting privacy; promoting strengthened accountability and privacy governance; collaborating with our privacy oversight partners where we can; looking at new ways to reach and educate individuals about privacy protection; and taking a specific focus on helping groups that are particularly at risk from privacy threats (including youth and seniors).

In pursuing these priorities toward the central goal of giving Canadians more control over their personal information along with all the tasks carried out by this Office, I am privileged to do so working with and enjoying the support and counsel of a team of talented and knowledgeable individuals unified in their commitment to assuring the protection of Canadians' right to privacy.

Privacy by the numbers

Information requests related to *Privacy Act* matters	**1,461**
Privacy Act complaints accepted and active	**1,040**
Privacy Act complaints accepted and in abeyance[1]	**2,937**
Privacy Act complaints closed through early resolution	**422**
Privacy Act complaints closed through standard investigation	**1,485**
Privacy Impact Assessments (PIAs) reviewed as "high risk"	**51**
PIAs reviewed as "lower risk"	**22**
Public sector audits concluded	**1**
Public interest disclosures by federal organizations	**266**
Legislation affecting federal public sector reviewed for privacy implications	**14**
Public sector policies or initiatives reviewed for privacy implications	**38**
Parliamentary committee appearances on public sector matters	**12**

1 These complaints in abeyance were submitted by a small number of individual complainants.

Formal briefs submitted on public sector matters	**11**
Other interactions with parliamentarians or staff (for example, correspondence with MPs' or Senators' offices) on public sector matters	**19**
Speeches and presentations delivered *	**99**
Visits to main web site *	**2,448,066**
Blog visits *	**1,103,262**
YouTube site visits *	**39,812**
Tweets sent *	**743**
Twitter followers as March 31, 2015 *	**9,426**
Publications distributed *	**8,229**
News releases and announcements issued *	**33**

* *Denotes activities not exclusive to public sector matters, but reflecting the Office's full work between April 1, 2014 and March 31, 2015*

Before Parliament:
A focus on surveillance issues

As noted in the Commissioner's Message, this past year saw considerable developments in the area of government surveillance. The potential impact of these changes on Canadians' privacy is a matter of profound importance to this Office.

As part of our priority setting exercise, the ever-broader authority and capacity of government agencies to collect and share Canadians' personal information was raised time-and-again during our engagement with stakeholders and in focus groups with individual Canadians. The concerns they expressed, together with our own concerns, assured that government surveillance would be one of our four strategic priorities.[2]

Certainly, no one would argue the need to protect public safety, whether the threat is terrorism or the risk that our children will be subjected to online bullying and harassment. Canadians want to be and feel secure, but not at any and all costs to their privacy. In short, they want both. It is worth noting that, in focus groups we conducted in 2014, participants told us they were generally comfortable with government surveillance for protecting national security and crime prevention. But, when asked about surveillance being applied to their communications, many did not like the idea of being profiled without their knowledge and were concerned about how surveillance might infringe on basic rights and freedoms.

Several legislative initiatives drew the attention of the Office over the course of the past year. The Office, in turn, made its concerns known to parliamentarians through submissions and appearances before committees of the House of Commons and the Senate.

2 https://www.priv.gc.ca/information/pub/pp_2015_e.asp

EYE ON GOVERNMENT SURVEILLANCE

The reporting period featured three specific bills interwoven by the fact that they increased the government's ability to collect, use and disclose personal information about Canadians without consent.

****

Bill C-51

In January 2015, Bill C-51 (the *Anti-Terrorism Act, 2015*) was tabled in Parliament. The Bill included the *Security of Canada Information Sharing Act* (SCISA). This latter Act provides all federal institutions with the discretion to share personal information collected from Canadians with any of 17 specifically enumerated federal departments and agencies that have a mandate (or part of a mandate) in respect of "activities that undermine the security of Canada" - as long as the information is relevant to the recipient institution's mandate in that regard.

Before Bill C-51 was introduced, the Commissioner and his provincial and territorial counterparts asked in a joint resolution that an evidence based approach be followed before new legislation was adopted to extend powers of national security agencies.

Following its introduction, our Office raised a number of concerns with SCISA, expressed by the Commissioner in submissions to Parliament,[3] and we followed the lively and ongoing public debate over Bill C-51 with great interest.

With its August 2015 coming into force, SCISA provides 17 government institutions involved in national security with virtually limitless powers to monitor and, with the assistance of Big Data analytics, profile ordinary Canadians, with a view to identifying security threats among them.

Among other changes, the Office recommended the Bill state that federal institutions share personal information only when it is considered "necessary or proportional" to a recipient institution's legal mandate in respect of "activities that undermine the security of Canada," and not merely "relevant." As well, rather than putting the onus on the sending department to decide what information may be necessary to national security, the Bill should explicitly require the department receiving the information—which presumably would have the expertise to make such a determination—to decide if the information was indeed necessary for purposes relating to its "security" mandate, and if not, require it to destroy the information immediately.

3 https://www.priv.gc.ca/parl/2015/parl_sub_150305_e.asp
https://www.priv.gc.ca/parl/2015/parl_sub_150416_e.asp
https://www.priv.gc.ca/parl/2015/parl_20150423_e.asp

Other parliamentary appearances and submissions on public sector issues – 2014-2015

Apart from the issues discussed in detail, our Office advised parliamentarians on numerous other public sector issues listed below:

- **Appearance before the Standing Senate Committee on National Security and Defence on CBSA border security measures** - April 28, 2014
- **Appearance before the Standing Senate Committee on National Finance on Bill C-31: Economic Action Plan 2014 Act, No. 1** - May 13, 2014
- Bill C-247, An Act to Expand the Mandate of Service Canada in Respect of the Death of a Canadian Citizen or Canadian Resident - **Submission to the Standing Committee on Human Resources, Skills and Social Development and the Status of Persons with Disabilities (HUMA)** - October 29, 2014
- **Appearance before the Senate Standing Committee on Social Affairs, Science and Technology on Division 17, Bill C-43**, Economic Action Plan 2014, No. 2 Amendments to the DNA Identification Act - November 5, 2014
- Bill C-32, An Act to enact the Canadian Victims Bill of Rights and to amend certain Acts – otherwise known as the Canadian Victims Bill of Rights - **Submission to the Standing Committee on Justice and Human Rights (JUST)** - November 13, 2014
- **Appearance before the House of Commons Standing Committee on Finance on Part IV, Bill C-43 (Economic Action Plan 2014, No 2)** - November 24, 2014
- **Appearance before the Standing Senate Committee on National Finance (NFFN) on Bill C-520 (Supporting Non-Partisan Offices of Agents of Parliament Act)** - January 28, 2015
- **Appearance before the House of Commons Standing Committee on Justice and Human Rights (JUST) on Bill C-26, the Tougher Penalties for Child Predators Act** - February 16, 2015
- **Appearance before the House of Commons Standing Committee on Finance on Terrorist Financing in Canada and Abroad** - March 31, 2015

Our submission also raised concerns that the Bill:

- set no clear limits on how long information is to be kept;
- failed to require that information sharing be subject to written agreements; and
- provided individuals no judicial recourse for improper collection, use or disclosure of their personal information.

These concerns were exacerbated by the lack of provision for any kind of dedicated oversight or review of the sharing, collection, use and retention of personal information enabled under Bill C-51. Indeed, of the 17 departments and agencies authorized to receive information, only three are subject to dedicated independent review or oversight of any kind. Independent review is particularly critical because information-sharing will often occur secretly.

Bill C-13

In November 2014, in a submission to and appearance before the Senate Standing Committee on Legal and Constitutional Affairs, the Commissioner detailed a number of concerns with Bill C-13, the *Protecting Canadians from Online Crime Act*. The Office supported the Bill's primary aim, specifically the sections that create new criminal offences to address cyber-bullying and other forms of Internet exploitation and harassment—all activities that clearly present grave risks to individual dignity and privacy for all citizens who use social networks and communicate online.

At the same time, however, the authority to collect Canadians' personal information– extended in the Bill—goes too far, lowering the threshold at which authorities may obtain a production order compelling an Internet Service Provider (ISP) to hand over subscriber information. In such cases, a public officer need only *suspect* people are doing something illegal in order to delve into their digital lives, as opposed to the higher legal threshold of "reasonable belief" that such a search will provide evidence of a specific crime.

In relation to this concern, Bill C-13 too broadly defined what constitutes "public officers" who, under the Bill, could trigger the collection of personal information for a wide range of purposes. In other words, the Bill could provide not just police, but anyone from a township reeve to a fisheries officer to a mayor with lawful access to our personal information under reduced thresholds.

In addition, while presenting before Committee in November 2014, the Commissioner raised concerns about the Bill lacking a reporting mechanism that "would allow Canadians to hold government to

account for the use of" C-13's "significant new powers as well as requests without a warrant." The Commissioner also underlined his concern with C-13's immunity provision designed to protect from legal liability those voluntarily disclosing personal information in response to warrantless government requests. It was noted that this provision was ambiguous as it came just months following the Supreme Court's unanimous decision in *R. v. Spencer* that clearly limited warrantless searches to situations where there were exigent circumstances, a reasonable law, or where the information involved did not attract a reasonable expectation of privacy.

Bill C-13 was enacted without amendment in December of 2014.

Bill C-44

Bill C-44, *An Act to amend the Canadian Security Intelligence Service Act and other Acts*, was introduced in the House of Commons in October 2014. It proposed giving the Canadian Security Intelligence Service (CSIS) explicit authority to operate outside Canada. It is not inconceivable—indeed, it seems likely—that this would result in greater information-sharing with foreign partners.

As we have seen, information-sharing with foreign governments can lead to human rights violations and even torture—most famously in the case of Maher Arar, an innocent Canadian citizen, held and tortured in Syria for almost a year. In 2006, the O'Connor Inquiry found that it was very likely that Canadian officials gave inaccurate information about Mr. Arar to U.S. authorities, leading to his rendition to Syria.

In submissions to both the Senate Standing Committee on National Security and Defence and the House of Commons Standing Committee on Public Safety and National Security, the Commissioner recommended that the Bill should include provisions to prevent CSIS from sharing information that would result in a violation of Canada's international obligations, including as a signatory to the United Nations *Convention Against Torture*.

Bill C-44 was passed without amendment and received Royal Assent in April 2015.

****

On the whole, all of the bills discussed here are tied together by a common thread. Each will increase the power of the government and its agents to collect, use and share our personal information without our knowledge or consent, and without a commensurate increase in oversight or independent review to help to assure these powers are not misused or abused.

Taken together, these initiatives have resulted in what can only be described as a sea change for privacy rights in Canada. Ensuring government powers under these new Acts are exercised in a manner which respects privacy

will be an ongoing focus of the Office in the months and years to come.

Stemming from our priorities-setting exercise, we have established the goal of contributing to the adoption and implementation of laws and other measures that demonstrably protect both national security and privacy.

Already, regarding Bill C-13's lawful access provisions, we have worked with others to provide guidelines to the private sector to establish standards for transparency and accountability reports related to the communication of personal information by companies to law enforcement agencies. Our Office has also asked federal institutions to begin issuing their own transparency reports about requests to private sector organizations for customer information.

Last year, following a review of the Royal Canadian Mounted Police's (RCMP) warrantless collection of subscriber information from telecommunication service providers, we recommended that the RCMP implement a means to monitor and report on its collection of this data. The progress in implementing this recommendation has been slower than expected. We hope that the new government will take action in this area given its commitment to promoting openness and transparency amongst federal institutions.

LOOKING AHEAD

In the short term, through recommendations following review of Privacy Impact Assessments, we will seek to reduce the privacy risks associated with the recently adopted *Anti-Terrorism Act, 2015*.

Going further, we will examine and report on how recently enacted national security legislation is implemented. We will use our review and investigative powers to examine the collection, use and sharing practices of federal institutions involved in surveillance activities to ensure that they respect the *Privacy Act*. We will report our findings to Parliament and the public, and issue recommendations for potential improvements to policies or legislation, as warranted.

Data breaches:
Rising incentive to better manage risks and prevent losses of data and trust

With new ways and new authorities to collect personal information, federal institutions hold an ever-increasing amount of our personal information—data that is stored in different places, in different ways and used and shared and moved around in a variety of formats and for a growing array of purposes.

Every one of these and countless other data transactions adds another layer of risk that our personal information may be disclosed, whether by accident, design, or technological failure.

Canadians' personal information is regularly collected and used by federal institutions as a matter of legal necessity and not by individual choice. Often times, this information is extremely sensitive. As a result, institutions' duty of care needs to meet the highest standards. While expecting absolute perfection may not be reasonable, institutions need to ensure they develop, implement and follow strong procedures to protect personal information according to the level Canadians expect. Falling short of this risks compromising public trust and confidence.

In a series of focus groups commissioned by the Office in fall 2014, many participants cited data breaches to underscore their concern about the government's ability to handle their personal information with the care it deserves.

Similar concerns were expressed in a survey of some 1,500 Canadians conducted for the Office last fall in which close to one third of respondents said they lacked confidence in the government's ability to assure their information would not be lost, stolen or misused.

2014-2015: BEGINNING OF MANDATORY REPORTING

In the last fiscal year, federal institutions reported a total of 256 data breaches to

our Office. This is an increase from the 228 breaches reported the year before—which itself was double the number reported the year before that.

As mentioned in the Commissioner's Message, this was the first year in which institutions were required to report data breaches, unlike the voluntary reporting regime from previous years. This new requirement could provide a clearer baseline for comparison in the future.

The updated Treasury Board President's *Directive on Privacy Practices* that requires reporting of all material privacy breaches to both our Office and Treasury Board of Canada Secretariat (TBS) came into force in May 2014. It includes guidance for differentiating a "material breach" from a breach with a lesser impact that can be risk-managed internally without formal reporting. In short, material breaches are those that involve sensitive personal information and could reasonably be expected to cause serious injury or harm to the individual and/or involve a large number of affected individuals.

While mandatory reporting of material data breaches is a welcome development, we cannot say categorically that the increase in the number of breaches reported in 2014-2015 was attributable entirely to the revised Directive—institutions may simply be taking more care to report. We note that 10 percent of institutions subject to the *Privacy Act* reported a breach in the past year, consistent with the voluntary reporting rate in the previous cycle.

Mandatory breach notification coming to the private sector

Just over a year after the Treasury Board President's Directive on mandatory reporting of material breaches by federal institutions came into effect, Bill S-4, the *Digital Privacy Act* gained Royal Assent.

It brought amendments to the *Personal Information Protection and Electronic Documents Act* (PIPEDA) including a requirement for organizations to inform affected individuals and our Office of data breaches that pose a "real risk of significant harm."

An organization will also be required to notify any other organization or government institution if it believes that the other body may be able to reduce the risk of harm. For example, a retailer could notify a credit card issuing bank or law enforcement agency.

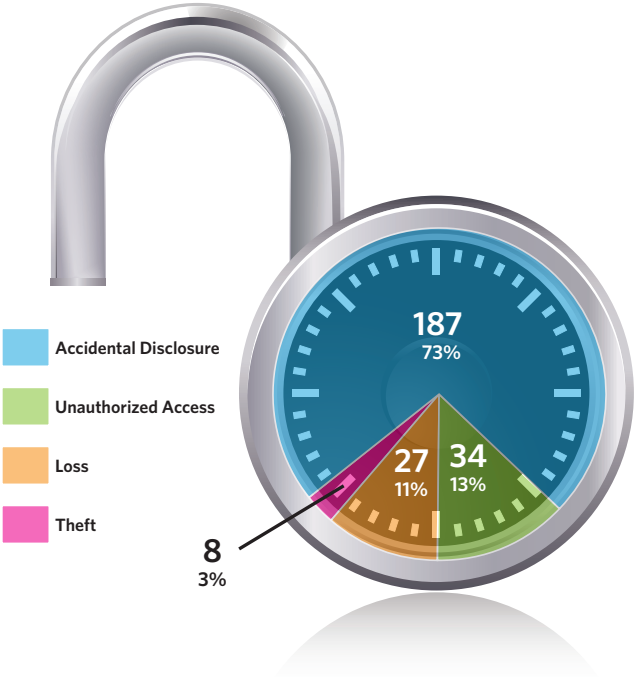
At the time of this report's writing, the federal government was in the midst of working on regulations to provide more details about the new requirements. Only after the regulations are finalized will the requirement to report breaches come into force.

In cases where a material breach is reported to our Office, we may, with reasonable grounds, open a Commissioner-initiated investigation

to determine what happened and why, and recommend improvements to personal information management practices to guard against a similar future incident.

As the incidents summarised below demonstrate, in most cases, data breaches can be prevented—but only if the security of Canadians' personal information is made a primary consideration and an integral part of an institution's organizational culture. It is equally important, that, when breaches do occur, institutions are prepared to respond effectively and appropriately to mitigate the impact on the individuals affected.

Breach breakdown



BREACHES AT THE CANADA REVENUE AGENCY

Given its mandate, the Canada Revenue Agency (CRA) handles a vast amount of sensitive personal information about Canadians. The Agency reported numerous breaches to our Office in 2014-2015, with causes ranging from accidental disclosure, to theft and unauthorized access. Examples of each follow.

Accidental disclosure of taxpayer data to the Canadian Broadcasting Corporation

The CRA notified our Office of a privacy breach in November 2014, stating that the personal information of more than 1,000 individuals and businesses had been accidentally delivered to a Canadian Broadcasting Corporation (CBC) journalist. The CBC released a story based on the information, including the names of some of the individuals affected, as well as details of their claims of a particular tax credit. Nine people filed complaints with our Office against the CRA. Several also complained that the CBC disclosed personal information without consent.

Our investigation confirmed the information delivered to the CBC was intended for the Administrative Tribunals Support Service of Canada (ATSSC). It arrived at the CBC due to a mix-up of package cover letters. While the initial error

that ultimately lead to the breach had been caught and corrected the previous day by some employees in the CRA's ATIP Office, unknowing staff compounded the error in the absence of employees who had made the corrections.

Had procedures been in place compelling the CRA ATIP personnel to register and check the status of information requests, this data breach could have been avoided. Following our investigation, we concluded that the complaints against the CRA were well-founded. As for the complaints against the CBC, we concluded they were not well-founded, as the *Privacy Act* does not apply to personal information collected, used or disclosed by CBC for journalistic, artistic or literary purposes.

Staunching the Heartbleed vulnerability

Network intrusion is a constant threat to personal information stored in public and private databanks alike. Proper risk management includes being ready to respond in the event a breach does occur. In April 2014, an intruder took advantage of the Heartbleed vulnerability (a security weakness found in certain software that secure websites use to encrypt user names, passwords and financial information) and accessed the Social Insurance Numbers (SIN) and additional personal information of some 900 taxpayers. While the CRA was the victim of the intrusion, the Agency was able to respond swiftly and decisively.

Its measures included shutting down its EFILE system as the income tax filing deadline neared, stepping-up monitoring of its IT systems to detect intrusions, sending a registered letter to each of the individuals affected by the intrusion, and providing a dedicated 1-800 number they could call. The CRA also provided those affected with access to credit protection services, and flagged their CRA accounts to monitor for any unauthorized activity. As an additional step, the CRA informed Employment and Social Development Canada of the SINs that had been compromised so it could monitor its accounts as well.

Unauthorized access to taxpayer files

During 2014-2015, the CRA reported two incidents of unauthorized access which took place in 2012, that underscore the risk of a wide range of employees having access to taxpayers' personal information.

In August 2012, a CRA employee at the Windsor-London Tax Services Office was found to have accessed the accounts of 170 individuals. A few months later, in January 2013, an employee in the same office accessed 169 accounts. Individuals' accounts contain a wealth of sensitive personal information—from names, addresses and

SINs to income and banking information. In both cases, changes were made to the information in some of the accounts.

The CRA notified the affected individuals of the breaches and of their right to complain to our Office. It disciplined the employees involved in the two incidents and is providing additional privacy training for its employees. Our 2013 audit of the CRA identified the need to strengthen its National Audit Trail System and process capability to further guard against unauthorized access to taxpayers' personal information. The CRA indicated that it was working toward meeting that recommendation.

In the examples recounted from the past year, the CRA has made efforts to inform us of incidents, and shows that it takes the issues seriously. In some cases, such as its response to Heartbleed, the Agency took quick, robust measures to protect personal information. But at the same time, in other examples cited, problems of the past repeated themselves due to inadequate processes which the Agency has committed to correcting and on which we will be following-up.

As noted earlier, in 2013 our Office conducted an audit of the CRA focused on its access controls to personal information. We made 13 audit recommendations on a number of matters including privacy breach reporting, monitoring of employee access rights, threat and risk assessments for IT systems and ensuring that Privacy Impact Assessments are completed for new programs involving changes to the management of personal information.

The CRA agreed with our recommendations and shared a plan outlining its corrective actions. We will be following up on the CRA's progress in meeting their commitments in the winter of 2016 and will continue to communicate with the Agency in relation to its personal information-handling practices.

BREACHES BROUGHT BY WINDOWED ENVELOPES

Health Canada - Marihuana Medical Access Program

In 2013, Health Canada sent letters to more than 41,000 people across the country to advise them of upcoming changes to the Marihuana Medical Access Program (MMAP). Health Canada's pre-printed envelopes were not compatible with automated equipment at Canada Post, so the letters went out in windowed envelopes that revealed not only the recipient's name and address, but the fact the letter was from the MMAP.

Health Canada did not report this as a data breach, but posted a notice on its website stating that, "as a result of an administrative error the envelopes were labelled to indicate that they were sent by the Program." The Commissioner determined there were reasonable grounds to initiate an investigation against the department—an investigation that covered the 339 complaints from people who received the letters.

The complainants alleged that Health Canada disclosed their personal information without consent, and noted a number of potentially damaging consequences, from the impact on their reputation to concerns for their livelihood if their employer learned they were using medical marihuana.

Our investigation concluded that Health Canada, however inadvertently and despite its arguments to the contrary, had disclosed sensitive personal information without consent. Since this unauthorized disclosure, Health Canada has put in place strict procedures for mail-outs to protect its clients' personal information.

Public Prosecution Service of Canada – SINs seen from tax slips

Windowed envelopes also resulted in an unauthorized disclosure of personal information by the Public Prosecution Service of Canada (PPSC), although this institution's response to the breach was far more proactive.

In February 2015, the PPSC reported that it had mailed tax slips to 65 employees in windowed envelopes that were too big, allowing the recipients' SINs to be seen through the address window. As soon as the mistake was noticed, PPSC notified the affected individuals verbally and followed up with a letter explaining the breach, offering the use of a protection service to monitor credit activity for fraud and identity theft for one year, and advising them to watch their financial accounts for any suspicious activity. The letter also informed the employees of their right to complain to our Office.

PPSC was able to verify that all but two of the envelopes were delivered to the intended recipients. Of those two, one went to an

address in a building that has since been demolished and the other was not located PPSC has advised that from now on, in addition to no longer using windowed envelopes for tax slips, it will also include a return address so that undeliverable mail can be returned to the organization.

CITIZENSHIP AND IMMIGRATION CANADA – CROSS-BORDER DATA BREACH

As part of their cooperation on security matters, Canada and the United States set up a computer system to exchange information on visa and travel permit applicants from other countries. In Canada, this information is stored in the Global Case Management System (GCMS) at Citizenship and Immigration Canada (CIC). On occasion—when someone's immigration status changes, for example—a second file may be created for the same person. The GCMS is programmed to identify them as "duplicate clients" to ensure personal information that is out-of-date or protected is not shared with the U.S.

On five occasions in 2014, due to a technical glitch, when the U.S. queried the system on clients who happened to have duplicate records, the system provided both files. For each of these individuals, one file showed them as having been refused a visa to visit Canada, and the other indicated they had Permanent Resident status in Canada. A Canada-U.S. agreement prohibits sharing information on Canadian or U.S. citizens or permanent residents, so the fact they had been refused visas in the past should not have been disclosed.

The first of these five breaches occurred in April 2014—two months after CIC made changes to the GCMS to address this very glitch—but were not discovered until July, during a manual quality control check that CIC conducts on a quarterly basis.

Following the most recent breaches, CIC implemented another technical fix to address the issue, and now checks the transactions with the U.S. on a weekly basis. Had a similarly aggressive monitoring schedule been in place after the first fix, the breaches that occurred between April and July might have been avoided. Following our review, we recommended that CIC continue to monitor the transactions with the U.S. on a weekly basis to help ensure the GCMS remains free of technical issues of this nature—and that any future changes to the system be followed by a period of more frequent checks so that any future anomalies can be rectified quickly.

NATIONAL RESEARCH COUNCIL OF CANADA – NETWORK INTRUSION

While putting the appropriate protocols for handling personal information in place can guard against human error, a major data breach at the National Research Council of Canada (NRC) points to the importance of ensuring information is not vulnerable to weaknesses in information and technology (IT) infrastructure.

In July 2014, the NRC reported an intrusion of its computer network. Beyond forcing a shutdown of the network for an extended period, the NRC advised our Office that, potentially, the intruder would have been able to access the personal information of both employees and current and former clients—some 50,000 people in all.

During our review, we noted the NRC had already started implementing an action plan, including rebuilding its IT infrastructure and developing a more robust NRC security culture. We were satisfied that no further action was required by our Office at that time. We do expect the NRC will conduct the appropriate security risk assessment exercises as it rebuilds its infrastructure and transitions to a new operating system. This should include a progressive certification and accreditation of all systems or services, and conducting Privacy Impact Assessments and Threat and Risk Assessments as necessary in order to mitigate all identified privacy risks.

****

As digital activity increases and public organizations continue finding new ways of using personal information for new initiatives, the emphasis on securing that data must increase in lockstep.

When planning new initiatives, institutions need to learn about past incidents such as those included in this report in order to proactively implement measures to prevent data breaches as much as possible.

Doing so means striving to not only protect the data they collect, but also earn and maintain the trust of the citizens they serve.

Audit: Privacy and Portable Storage Devices

MAIN POINTS

Portable storage devices (PSDs) are widely used within federal institutions. Although policies, processes and controls surrounding the use of these devices are in place, there are significant opportunities for improvement in the management and protection of PSDs. Of the entities selected for review:

- approximately 70 percent have not formally assessed the risks surrounding the use of all types of PSDs;
- over 90 percent do not inventory and track all PSDs throughout their lifecycle;
- over 85 percent do not retain records verifying the secure destruction of data retained on surplus or defective PSDs; and
- approximately 55 percent have not assessed the risk to personal information resulting from the absence of controls to prevent the use of unauthorized PSDs.

Although there is a record of active smart phones, the identity of specific users is unknown in many cases. Moreover, standardized controls have yet to be uniformly applied.

Federal entities which allow the use of PSDs without proper controls run the risk of:

- losing or exposing confidential data or personal information, resulting in harm to the government and individuals;
- eroding public confidence and exposing themselves to significant reputational risk; and
- incurring substantial costs for data losses and recovery efforts.

INTRODUCTION

PSDs are electronic devices designed to hold digital data. They are generally small in size and easy to use. Such devices include, but are not restricted to: laptops; tablets; smartphones; external hard-drives; USB memory sticks; and optical discs.

The storage capability of PSDs, along with their portability and ease of use, make them popular and valuable tools. In many cases, data from government networks can be copied to such devices quickly and easily.

Although PSDs offer a number of benefits, they also present certain inherent privacy and security risks. By virtue of their size and portability, PSDs can be easily lost, misplaced or stolen. Their use can increase an institution's risk of data loss and by extension, the risk of data exposure. The exposure could have serious consequences for individuals, including financial loss, reputational harm and risk to personal safety.

When information stored on a PSD is sensitive, the impact of losing the device can increase. The magnitude of the government's personal information holdings–and the sensitivity of that data–make the privacy risks stemming from the loss of PSDs in government all the more critical.

Following a number of data breaches, including the 2012 loss of a portable hard drive containing personal information about student loan recipients, our Office announced its intention to conduct a government-wide audit of federal practices concerning PSD management.

AUDIT OBJECTIVE

Our objective was to assess whether federal entities have implemented adequate controls to protect personal information stored on PSDs.

In order to protect against data loss or theft of data stored on PSDs, we expected federal entities using such devices to have established appropriate measures to protect privacy. In our view, entities using PSDs should have a governance regime to support their management and use. They should also have administrative processes in place to inventory and track PSDs throughout their lifecycle. Most importantly, entities should have controls in place, including physical and technical safeguards, to protect against the exposure of sensitive data.

In May 2014, six months following the commencement of our audit, the Treasury Board of Canada Secretariat (TBS) issued an Information Technology Policy Implementation Notice (ITPIN or "Notice")[4] for the secure use of PSDs in government. The ITPIN provides direction to institutions regarding the management of PSDs,

4 https://www.tbs-sct.gc.ca/it-ti/itpin-ampti/2014-01-eng.asp

including the establishment of appropriate physical and security controls. Many of the provisions contained in the Notice mirror our audit expectations, and serve to support the importance of safeguarding PSDs and the information they hold.

SELECTION OF AUDIT ENTITIES

Our audit commenced with a survey of 49 federal entities. The survey participants, selected because of the type of personal information under their control, were asked to respond to a series of questions related to their use of PSDs. The inquiries focused on three specific areas: physical controls, security controls, and privacy management and accountability.

Based on the responses, 16 entities were selected for examination. Various factors were considered in this regard, including the extent to which PSDs were deployed within an institution, the volume and sensitivity of the entity's personal information holdings, the existence of controls—or lack thereof—to protect personal information residing on PSDs, and the use of privately-owned PSDs for work related purposes.

In addition to the 16 entities, Shared Services Canada (SSC) was included as it is responsible for managing data centres (e.g. network servers) and telecommunication services (e.g. the provision of smart phones) on behalf of 43 federal institutions. The examination focused on SSC's role in this regard.

OBSERVATIONS

The audit findings are highlighted below; not all observations apply to all entities. For additional details, readers are referred to the audit summary examination reports, which are available on our website. All of the entities have accepted the audit recommendations and agreed to address them.

Most entities do not have an administrative process in place to inventory and track all types of PSDs throughout their lifecycle

All of the entities record and track the issuance of laptops and tablets. In contrast, administrative processes for the management of USB storage devices—portable hard drives and memory sticks—as well as CDs/DVDs were largely absent or only in the early stages of implementation. Consequently, the extent to which these devices are used remains largely unknown.

In the absence of a formal administrative process to track all PSDs, it was impossible to determine the extent to which government-owned devices have been deployed, and for what purposes. It also presents a challenge in terms of confirming whether PSDs are returned at the end of their lifecycle (including when employees leave an organization). While most entities have procedures in place for the

secure destruction of data stored on defective, returned and surplus PSDs, without a formal tracking mechanism, there is no assurance that all PSDs are cleansed of corporate and personal data prior to disposal.

Federal institutions have an obligation to protect personal information entrusted to them. In fulfilling this obligation, they must be cognizant of where data is held. The identification and tracking of PSDs is critical in this regard. Without such a mechanism, institutions lack the ability to determine what devices are being used, by whom, and for what purposes. By extension, it impedes their ability to minimize the risk of a data loss.

In light of our introductory remarks about the risks associated with unintended data loss or personal information exposure, the unaccounted inventory of all types of PSDs presents a potential threat to Canadians' privacy.

Most entities have frameworks in place for the secure disposal of PSDs to support their management, but there are gaps

A secure disposal method provides assurance that information cannot be retrieved or reconstructed. In terms of PSDs, this is achieved by either sanitizing (wiping) the device with a secure (certified) cleansing mechanism or physically destroying it.

Most entities have established formalized processes for the disposal of surplus or defective PSDs. A number of them have adopted a centralized approach that requires the shipment of non-sanitized devices from various sites to a central location for disposal. This presents a potential risk of data exposure in the event that devices are lost or stolen in transit. With one exception among the entities that have centralized disposal processes, this risk has not been assessed.

While there is no evidence to suggest entities are disposing of PSDs in an unsecure manner, almost all of them do not, as standard practice, retain documentary evidence as verification that all data on surplus or defective devices has been destroyed. Such evidence provides an organization with the ability to demonstrate that it has exercised due diligence in ensuring personal information is disposed of in a secure manner.

Many entities have not assessed the privacy risks surrounding the use of certain types of PSDs

In order to have an effective governance structure in place for PSD management, it is critical that the risk of using such devices is fully assessed. This would include an analysis of whether the potential privacy and security risks surrounding PSDs are proportional to the benefits derived from their use. Such analysis supports the decision and conditions under which PSDs are deployed and the establishment of appropriate security controls to protect privacy. Moreover, it may potentially impact the development of PSD inventory

management processes, as well as employee training and awareness programs.

While there were exceptions, entities have completed risk analysis on the use of laptops, tablets and USB storage devices. However, the majority of entities have not assessed the risk to personal information resulting from the lack of technical controls on the connection of unauthorized USB storage devices, and the use of CDs/DVDs to store data. In some instances, risk analysis was also lacking in terms of the ability to download and run unauthorized applications on devices.

Many entities have not implemented adequate controls to protect against the exposure of sensitive data residing on USB storage devices

Physical and logical safeguards ensure the security and confidentiality of personal information residing on PSDs. Laptops and tablets are generally equipped with encryption, strong password parameters, and controls to prevent the installation of unauthorized applications. In contrast, safeguards and controls to protect data stored on other PSDs are lacking. Despite the range of software and hardware encryption solutions available, one-quarter of the entities do not enforce the use of encrypted USB storage devices. Moreover, two-thirds of the entities do not have technical controls in place to prevent the connection of unauthorized PSDs (e.g. privately-owned device) on their networks.

Adequate logical controls are essential to protect data residing on PSDs. If such controls are not in place, there is an increased risk of an unauthorized disclosure of personal information. This could result in harm to the impacted parties and erode public trust in an institution's ability to protect privacy.

Entities have policy frameworks in place to support the management of PSDs

Sound policies are essential to protect organizational assets, including personal information. They establish accountability and associated responsibilities, and provide the mechanism through which security and privacy protection are integrated into day-to-day operations. The absence of well-defined policies may result in inconsistent and inadequate information-handling practices that place privacy at risk.

Within the audited entities, PSDs are supported by a policy—or suite of policies—governing their management and use. These governance instruments prescribe the proper use and protection of devices. Roles and responsibilities for PSD management were generally well defined, and accountability for their use was clearly established.

However, certain gaps were identified. We expected that, at minimum, policies would address the use of all PSD types, the obligation to safeguard devices and the information stored on them, the requirement to report the loss

or theft of a device, and the use of privately-owned devices for work related purposes. The policies implemented by one-quarter of the entities did not address one or more of the above-referenced elements.

The effectiveness of a policy—or suite of policies—can be determined, in part, by the extent to which employees are aware of them. With one exception, all of the entities have implemented training programs that include modules dedicated to the use of PSDs. However, there are opportunities for improvement in this regard. Specifically, employee participation in the training programs offered by approximately one-quarter was not mandatory. Other notable gaps included training materials that did not cover all types of PSDs, the loss or theft of devices, and the policy governing the use—or prohibition—of privately-owned devices.

Employees must be aware of organizational policies and complementary procedures surrounding PSD usage. Without a clear understanding, there is a risk that employees will not exercise the appropriate level of due diligence in managing personal information stored on PSDs. This could result in a privacy breach.

The government's central registry of smart phone users is incomplete

SSC is responsible for the management of smart phones across 43 federal institutions (termed 'partner organizations'). Of these, 10 were selected for inclusion in the audit.

In carrying out its mandate, SSC has developed a registry to track the issuance of all new devices. The registry is intended to serve as a mechanism to provide a full accounting of all smart phones in use at partner organizations. Currently, the registry does not accurately reflect the full inventory of devices in use.

SSC reports that at the time of transition (transfer of responsibility for the management of mobile phones from partner organizations), it was not provided with comprehensive listings of its partner organizations' smart phone inventories. SSC has embarked on a number of initiatives to update the registry. Despite its efforts, a complete listing of smart phone users will not, in all likelihood, be available before September 2016.

Organizations are obligated to safeguard personal information throughout its lifecycle, regardless of how it is stored. The absence of a mechanism to identify smart phone users impedes an institution's ability to ensure devices are handled in accordance with established policy—including the return of devices when no longer required. Without such assurance, there is a risk that devices will

not be cleansed in a secure manner, potentially resulting in exposures of personal data.

Uniform security controls are not yet in place for the management of registered smart phones

Prior to SSC's creation, partner organizations were responsible for managing their smart phone inventories. This included establishing and implementing security settings to protect the data held on the devices. The settings implemented by the 10 partner organizations selected for examination were reviewed as part of the audit. While three of the entities have implemented sound controls, weaknesses were noted in the security settings established by the remaining seven. These weaknesses existed at the time SSC assumed responsibility for smart phone management.

SSC has adopted a multi-step approach in transitioning the responsibility for managing smart phones, including security settings. It has established a number of configuration profiles in this regard; all of the profiles enforce baseline controls (e.g. encryption, strong password parameters, etc.).

At the time our audit concluded, the baseline settings had not been installed on all devices and may not be implemented on certain devices before September 2016. In the interim, known security gaps and weaknesses remain unaddressed, placing data held on the affected devices at risk of exposure.

Risks surrounding the connection of unauthorized USB storage devices to network servers have not been assessed

SSC manages network servers on behalf of its partner organizations. The servers may contain significant amounts of personal information. There are no technical controls in place to prevent the transfer of this information to unauthorized USB storage devices (e.g. devices not equipped with security features prescribed by the organization). Considering the sensitivity and volume of information stored on many of these servers, a data exposure resulting from the use of such devices could have negative consequences for thousands of individuals, as well as the government.

CONCLUSION

Although there is an awareness of the privacy risks associated with the use of PSDs following data breaches reported in the media, the risk of a loss or unintended disclosure of personal information remains a real possibility. The solution to this is not to preclude or prohibit the use of PSDs in government. In fact, it is quite the opposite. PSDs are important and valuable tools in an age of increased employee mobility.

Our horizontal audit was undertaken to assess current practices surrounding the use of PSDs within selected federal organizations.

Although entities have implemented frameworks to manage PSDs, there is a need to improve controls—including policies, procedures and processes—to protect privacy. The extent to which improvements are required varies among the entities. However, there are a number of observations that are common to most, including the absence of both risk analysis and an inventory tracking mechanism for all types of devices, as well as the retention of records verifying the secure destruction of data stored on surplus or defective devices. These, along with the other identified gaps and weaknesses have potential privacy implications. Addressing them will assist entities in mitigating the risk to personal information transmitted to, and stored on, PSDs.

FOLLOW-UP

As part of our audit methodology, we will be conducting a follow-up in two years with the 17 entities selected for examination. At that time, the progress made to implement the audit recommendations will be assessed.

As previously stated, in May 2014 the TBS issued an ITPIN for the secure use of portable data storage devices across government. Where implemented, the Notice should serve as a touchstone for privacy protection and management of PSDs. Going forward, we encourage institutions to fully implement and monitor compliance with the ITPIN.

ABOUT THE AUDIT

Authority

Section 37 of the *Privacy Act* empowers the Privacy Commissioner to examine the personal information handling practices of federal government organizations.

Objective

To assess whether the selected entities have implemented adequate controls – including policies, procedures and processes – to protect personal information transmitted to, and stored on, PSDs.

Criteria

Audit criteria were derived from the *Privacy Act* and TBS policies, directives and standards related to the management of personal information.

We expected to find that the selected entities had:

- assessed the security and privacy risks inherent to the use of PSDs;
- implemented adequate physical and logical controls to protect personal information transmitted to, and stored on, such devices;
- established policies and procedures—governing the use of PSDs—that were consistent with Government of Canada security requirements and best practices;
- put formalized procedures in place for the secure disposal of surplus or defective PSDs;
- educated employees on the acceptable uses of, and the associated risks surrounding, PSDs; and
- implemented incident response procedures to address data breaches (inappropriate disclosures of personal information) resulting from the loss or theft of PSDs.

Scope and Approach

As part of the audit planning process, the nature, extent and sensitivity of personal information held by federal institutions were assessed; descriptions of their respective personal information bank holdings were used for assessment purposes. As a result of this analysis, 49 institutions were asked to participate in a survey.

The survey was designed to facilitate the selection of organizations for audit examination. A risk scoring tool was designed for this purpose. Each survey question was assigned a weight (based on its relative importance). The participants' responses were assessed using a rating scale and the

cumulative results produced a total score for each institution; institutions were subsequently placed within one of five categories.

Where applicable, selection criteria for institutions falling within the same category included:

- the sensitivity and volume of personal information held by the organization – and by extension, the potential impact of a data breach/exposure;
- the number and types of PSDs issued by the organization; and
- the control frameworks in place to protect personal information residing on PSDs.

Audit evidence was obtained through various means, generally involving on-site observations, interviews and information obtained through correspondence. We also reviewed policies and procedures, threat and risk assessments, and training materials.

The audit was primarily carried out at the entities' head offices. Examination activities were also conducted at selected regional sites where accountability for the management of PSDs has been decentralized. The examination was substantially completed on November 28, 2014.

Standards

The audit was conducted in accordance with the legislative mandate, policies and practices of the Office of the Privacy Commissioner of Canada, and followed the spirit of the audit standards recommended by the Canadian Institute of Chartered Accountants.

Audit team

Director General: Steven Morgan
Dan Bourgeault
Garth Cookshaw
Sylvie Gallo Daccash
Michael Fagan
Gaétan Létourneau
Anne Overton
Kyle Sprysa
Bill Wilson

LIST OF SURVEY PARTICIPANTS

	Name of Institution
1	Aboriginal Affairs and Northern Development Canada
2	Agriculture and Agri-Food Canada
3	Atlantic Canada Opportunities Agency
4	Bank of Canada
5	Business Development Bank of Canada
6	Canada Border Services Agency
7	Canada Deposit Insurance Corporation
8	Canada Mortgage and Housing Corporation
9	Canada Post Corporation
10	Canada Revenue Agency
11	Canadian Air Transport Security Authority
12	Canadian Food Inspection Agency
13	Canadian Human Rights Commission
14	Canadian Security Intelligence Service
15	Canadian Transportation Agency
16	Citizenship and Immigration Canada
17	Commission for Public Complaints Against the RCMP
18	Correctional Service Canada
19	Elections Canada
20	Employment and Social Development Canada
21	Farm Credit Canada
22	Fisheries and Oceans Canada
23	Foreign Affairs, Trade and Development Canada
24	Health Canada
25	Immigration and Refugee Board of Canada
26	Justice Canada
27	Library and Archives Canada
28	Military Grievances External Review Committee
29	Military Police Complaints Commission
30	National Capital Commission
31	Office of the Ombudsman – National Defence and Canadian Forces
32	Office of the Commissioner of Lobbying of Canada
33	Office of the Correctional Investigator
34	Office of the Taxpayers' Ombudsman
35	Office of the Public Sector Integrity Commissioner of Canada
36	Parole Board of Canada

37	Public Health Agency of Canada
38	Public Works and Government Services Canada
39	Royal Canadian Mounted Police
40	Security Intelligence Review Committee
41	Shared Services Canada
42	Social Security Tribunal of Canada
43	Statistics Canada
44	Transport Canada
45	Transportation Safety Board of Canada
46	Veterans Affairs Canada
47	Veterans Review and Appeal Board
48	VIA Rail Canada
49	Western Economic Diversification Canada

To read the reports prepared for each audited entity, go to:
https://www.priv.gc.ca/information/pub/ar-vr/ar-vr_index_e.asp

LIST OF ENTITIES SELECTED FOR REVIEW

	Name of Institution
1	Aboriginal Affairs and Northern Development Canada (AANDC)
2	Agriculture and Agri-Food Canada (AAFC)
3	Bank of Canada (BoC)
4	Business Development Bank of Canada (BDC)
5	Canada Border Services Agency (CBSA)
6	Canada Deposit Insurance Corporation (CDIC)
7	Canada Mortgage and Housing Corporation (CMHC)
8	Canada Revenue Agency (CRA)
9	Canadian Human Rights Commission (CHRC)
10	Citizenship and Immigration Canada (CIC)
11	Farm Credit Canada (FCC)
12	Fisheries and Oceans Canada (DFO)
13	Immigration and Refugee Board of Canada (IRB)
14	Public Health Agency of Canada (PHAC)
15	Parole Board of Canada (PBC)
16	Statistics Canada (StatCan)
17	Shared Services Canada (SSC)

SUMMARY OF COMMON RECOMMENDATIONS

Recommendations	AANDC	AAFC	BoC	BDC	CBSA	CDIC	CIC	CHRC	CMHC	CRA	FCC	DFO	IRB	PBC	PHAC	StatCan
Ensure that the issuance of all portable storage devices—that may be used to retain personal information—is recorded for identification and tracking purposes.	●	●		●	●	●	●	●	●	●	●	●	●	●	●	●
Retain documentary evidence—either the confirmation report generated by a certified cleansing mechanism or confirmation of physical destruction—as verification that all data on surplus or defective portable storage devices has been destroyed in a secure manner.	●	●			●	●	●	●	●	●	●	●	●	●	●	●
Assess the current disposal process—insofar as the shipment of surplus and/or defective portable storage devices from various locations to a central site (e.g. head office)—to ensure appropriate controls are in place to mitigate the risk of a data exposure.				●		●	●	●	●	●	●	●		●	●	●

Recommendations	AANDC	AAFC	BoC	BDC	CBSA	CDIC	CIC	CHRC	CMHC	CRA	FCC	DFO	IRB	PBC	PHAC	StatCan
Assess the risk to personal information resulting from the lack of controls on the connection of unauthorized USB storage devices and implement appropriate controls to address identified gaps and weaknesses.	●	●		●		●		●			●		●	●	●	
Assess the risk to personal information resulting from the use of CDs/DVDs to store data and implement appropriate controls to address identified gaps and weaknesses.	●	●		●	●	●		●		●	●	●	●	●		
Ensure that encryption is deployed on all portable storage devices that may contain personal information.	●	●				●		●	●		●			●		
Ensure that all employees, including contract personnel, are aware of the policies governing the use of portable storage devices, and provide guidance to mitigate the risks inherent to the use of the devices.						●		●	●		●	●	●	●	●	●

Recommendations Specific to SSC	
In collaboration with partner organizations, ensure that all active smart phones are captured, either by user or contact name, in a registry by January 2016.	●
Ensure that baseline security controls are implemented on all smart phones in use at partner organizations by January 2016.	●
Assess the risk to personal information resulting from the lack of controls on connection of unauthorized USB storage devices on servers, and implement appropriate controls to address identified gaps and weaknesses.	●

The year in review

Privacy Impact Assessments

Privacy Impact Assessments (PIAs) are used to identify potential privacy risks that may be associated with new or redesigned federal government programs or services. According to the Treasury Board of Canada Secretariat (TBS) *Directive on Privacy Impact Assessments*, federal government institutions are responsible for undertaking PIAs for new or substantially-modified programs or activities involving the use of personal information for decision-making purposes which affect individuals. They must demonstrate that privacy risks have been identified and mitigated effectively.

Institutions provide copies of their PIAs to TBS and our Office, which we review and, when appropriate, advise on ways to improve personal information-handling practices. While our recommendations are not binding, in most cases institutions do accept and implement our advice.

In 2014-2015, the Office received 70 new PIAs and completed reviews of 73 files. We sent detailed recommendations for 51 PIAs on initiatives that held a potentially high risk for privacy, as well as for 22 activities seen as lower risk.

We also opened 19 new consultation files and advised several federal institutions on the privacy risks of a number of initiatives still in the early stages of development. Among these were projects to test the use of facial recognition technology at Canadian borders; to make the reporting of an individual's Social Insurance Number (SIN) a mandatory part of the Census; and initiatives for increased government use of information from publicly available sources, including open social media feeds.

The following summaries provide an overview of some of the high priority PIAs we reviewed during 2014-2015.

Canada Border Services Agency - Entry/ Exit Initiative

As we have for the past several years, we continued to review PIAs and consult on a number of programs and activities related to the Canada-U.S. Beyond the Border initiative, including consultations with Public Safety Canada and the Canada Border Services Agency (CBSA) on implementing the next phases of the Entry/Exit Initiative.

Under Phases I and II of this initiative entry information of third country nationals and permanent residents crossing the border by land began being collected respectively by the CBSA and the Department of Homeland Security. Phase III (which has yet to be implemented) would expand the surveillance to Canadian and U.S. citizens crossing by land.

In Phase IV, the CBSA plans to expand the program to include collecting information on people, including Canadian citizens, leaving Canada by air. The data will be used by the Canadian government for a variety of domestic purposes, including law enforcement and determining eligibility for residency-based social benefits and tax treatment. Exit information may also be shared with the U.S. and other countries on a case-by-case basis.

At least five federal institutions are planning initiatives that would use this information— the CBSA, the Canada Revenue Agency (CRA), the Canadian Security Intelligence Service (CSIS), Citizenship and Immigration Canada (CIC), Employment and Social Development Canada (ESDC) and the Royal Canadian Mounted Police (RCMP). We are waiting to receive PIAs from these institutions for each of their proposed expanded uses.

Canada Border Services Agency – Expanded Use of Facial Recognition Technology

The CBSA consulted our Office in 2014-2015 regarding its plans to use facial recognition technology at ports of entry. The system compares the facial features of incoming travellers against photographs of individuals known to be inadmissible to Canada and who appear on CBSA watch lists. The CBSA is undertaking projects to evaluate the effectiveness of the technology in live border situations, and under various lighting and crowd movement conditions.

We have provided high-level advice on the potential privacy risks, including that of "false positives," which could result in unwarranted scrutiny and secondary screening for some individuals. We have also pointed out the need for the CBSA to undertake a Threat and Risk Assessment (TRA) to evaluate technical risks, along with the need for privacy risks and implications to be taken into account during the evaluation of the technology's necessity and effectiveness. Our Office will continue to consult with the CBSA on this file as more information becomes available through the proof of concept trials and subsequent analysis.

Canada Border Services Agency – Scenario Based Targeting

In 2014-2015, we reviewed a PIA conducted by the CBSA for its adoption of Scenario Based Targeting (SBT), its new method for assessing the risk levels of passengers arriving in Canada by air.

Under Canadian law, all commercial air carriers are required to provide the CBSA with a range of information for all persons travelling to Canada, including name, date of birth, citizenship, contact phone numbers, seat number, payment information and more. The CBSA loads this data into the Passenger Information System (PAXIS) and uses it to identify individuals who are or may be involved with terrorism or terrorism-related crimes or other serious offences that are transnational in nature.

In the past, the CBSA used an individual risk scoring method that analyzed specific passengers and gave them a risk value based on their distinct data elements and passengers with a high risk score would be flagged for further review.

The new scenario-based method uses Big Data analytics to evaluate all data collected from air carriers against a set of conditions or scenarios. Designed to harmonize with the system used by the U.S., it could allow the operator to, for example, search for all males aged between the ages of 18-20 who are Egyptian nationals and who have visited both Paris and New York. Our Office's concern with the new method is that travellers may now be targeted for increased scrutiny if they fit the general attributes of a group—and individuals may be subjected to recurring and unnecessary attention at the border because of characteristics they cannot change, such as age, gender, nationality, place of birth, racial and/or ethnic origin.

In reviewing the PIA, we made a number of recommendations, including:

- demonstrate the necessity of SBT, beyond the general purpose of harmonizing our system with that of the U.S.;
- in the interests of public transparency, add to the PIA general descriptions of the types of scenarios that might be used to identify potentially high risk travellers;
- conduct regular reviews of the effectiveness and proportionality of scenarios, including an examination of impacts on civil liberties and human rights; and
- prepare a PIA for the entire Advance Passenger Information/Passenger Name Record program used to collect passenger information from air carriers.

We are pleased to note that the CBSA responded positively to all our recommendations and that we are expecting to receive a more comprehensive PIA on the CBSA's overall collection, analysis, use and disclosure of passenger information during the 2015-16 fiscal year.

Statistics Canada - 2016 Census Tests

Statistics Canada (SC) undertakes a Census of the Canadian population every four years. For the Census coming in May 2016, SC had been considering including the SIN as part of the information respondents must provide. The SINs would be used to link to CRA databases to verify income levels reported in the Census.

We recommended that SC carefully consider whether making the mandatory collection of the SIN for this purpose is necessary. In the 2011 Census, SC asked respondents for permission to link Census information to income data using their biographical information. SC has indicated that 89 percent of respondents consented to this. Given that success rate, we expressed doubts about the need to replace this method with mandatory collection of SINs.

SC has since informed us that mandatory reporting of SINs in its 2014 Census Program Test showed only marginal gains in efficiency and quality of linkages, which would not justify the mandatory collection of the SIN on the 2016 Census questionnaire. As a result, SC informed us that it will not require this going forward.

Royal Canadian Mounted Police – National DNA Data Bank

The National DNA Data Bank (NDDB) was established in 2000 to collect and store the DNA profiles of individuals convicted of certain serious crimes. In December 2014, the *DNA Identification Act* was amended to add five new categories of DNA profiles to the databank, including DNA from victims of crime; individuals who provide their DNA voluntarily; and DNA profiles of missing persons and relatives of missing persons. As of this report's writing, these amendments had yet to come into force.

While the databank was created in 2000, the RCMP did not provide a PIA on the system until 2014, primarily because it predated federal PIA requirements implemented in 2002. That PIA did not include an assessment of any new privacy risks that may arise as a result of the new categories of DNA profiles to be added to the databank. We do expect the RCMP to conduct a new PIA to address this and the Force has committed to doing so.

Royal Canadian Mounted Police - National Centre for Missing Persons and Unidentified Remains

The RCMP provided a PIA on the National Centre for Missing Persons and Unidentified Remains. The Centre provides law enforcement officers, medical examiners and chief coroners across Canada with specialized services to support investigations into missing persons and unidentified human remains.

The amendments to the *DNA Identification Act* noted above also expand the mandate of the Centre by creating new DNA indices of missing persons, relatives of missing persons and human remains. This information may be accessed during investigations.

Our Office issued several recommendations to the RCMP on the operations of the Centre related to limiting disclosure of personal information and safeguards. We expect the RCMP to assess any new potential privacy risks related to the expansion of the Centre via a new PIA, which it has committed to doing.

Going forward, we will continue to closely follow this initiative and that of the NDDB.

Expanding use of social media and "open source" information

In 2014-2015 we received PIAs or were consulted on several federal government initiatives using or planning to use "open source" and "publically available" information. In some cases, this would include personal information collected from social media sites such as Facebook and Twitter.

Initiatives proposing to collect and use this sort of information included the Public Works and Government Services (PWGSC) Integrity Database Services, which provides government procurement officials with background information on businesses bidding for contracts. ESDC is considering using this kind of information to assess satisfaction with government services such as passport applications and employment services.

Our advice included cautions on the risks that such information may be out of date, out of context, or inaccurate. We also raised the issue of consent as individuals making comments via social media may not reasonably expect these to be collected and used by government officials.

In response to our recommendations, and after implementing some changes in program design, PWGSC has advised us that going forward it will only use credible information from authenticated sources, such as court reports, and will not collect "open source" information. In the case of ESDC, we expect to receive a PIA on the collection of personal information from social media sites as a method to survey public satisfaction with government services, if such a project goes ahead.

Investigations

The number of investigations completed by our Office during the past year increased marginally, rising to 1,239[5] from 1,214[6] a year earlier. While the number of cases closed held steady, the increase in complaints received was dramatic—rising by 124 percent from the previous year to a total of 3,977 by far the highest number ever.

Much of the increase can however be attributed to a small number of individuals filing multiple complaints. Of the nearly 4,000 complaints received in 2014-2015, 3,154 came from a small number of people who filed eight or more complaints apiece—in some cases, hundreds more. Discounting these, our Office accepted 1,040 complaints in the past year, similar to the previous reporting period.

To manage the risk that dealing with these files could eclipse other individuals' access to our services, our Office established a multiple complaints strategy. Under it, we strive to work with people who have submitted multiple complaints within a short period of time to prioritize their issues—launching investigations of the complaints most important to the

5 The number of investigations is lower than the number of complaints closed because we excluded two instances where one investigation resulted in the closing of multiple complaints in relation single incidents (Health Canada Marihuana Medical Access Program breach and Employment and Social Development Canada (ESDC)/Justice Canada USB key breach, both totaling 668 closed complaints

6 Excluding 871 complaints tied to the ESDC hard drive investigation

individual while, in some cases, deferring others until the initial investigations have been completed. With this approach, our Office can better balance the needs of all complainants, and ensure complaints are treated in a fair and timely manner.

As the number and complexity of complaints continues to increase, our Office continues to explore ways to modernize and increase our investigations' efficiency. More complaints are being settled through our early resolution process (up over 22 percent compared with 2013-2014). We also conducted a review to identify where further improvements could be made to shorten the time required to investigate complaints.

While increasing efficiency is essential to making the most of our limited resources, we remain committed to maintaining a high standard of investigative excellence.

The case summaries included here demonstrate some of the ways our investigations are uncovering important lapses in privacy protection and helping to protect Canadians' privacy rights, with an emphasis on privacy within employer-employee- and administrative process-related issues.

To read the full versions of each Report of Finding summarized below, go to: https://www.priv.gc.ca/cf-dc/pa/index1415_e.asp

Video surveillance of employees vs. right to privacy—a delicate balance

An CBSA employee alleged that dozens of cameras in place at a Canada-U.S. border crossing facility were being used not only for security purposes, but also to monitor employee conduct and performance.

The CBSA *Policy on the Overt Use of Audio-Video Monitoring and Recording Technology* states that, in addition to security applications, video surveillance may be used to help assure "program integrity and quality assurance." The policy says this could include monitoring interactions between employees of the CBSA and the public, to ensure efficiency, and to gather information to provide evidence of allegations of employee misconduct or illegal activity.

Our Office agrees that the CBSA, as a visible law enforcement agency, must maintain a high level of credibility and public confidence to deliver its programs effectively, and assuring employee compliance with codes of conduct is important to fulfilling its mandate—but this does not mean its assertion that these and

other uses of video described in its policy are consistent with the *Privacy Act*.

A broad range of employee conduct can fall within the scope of "quality assurance," including using video to monitor employee performance—how many travellers an officer processes in an hour, for example.

By its very nature, video surveillance is intrusive. It collects all sorts of personal information, very little of which may have anything to do with the reason cameras were installed in the first place.

In this case, we found the CBSA had not demonstrated that it was necessary to collect the personal information of employees for the broad range of purposes listed as related to program integrity—violating Section 4 of the Act requiring that personal information only be collected if it "relates directly to an operating program or activity of the institution."

The CBSA has updated its policy to clarify how it intends to use video surveillance and clarifying that it will not be used to monitor employee performance. The CBSA has also committed to providing us with updated scenarios to guide staff in the implementation of the policy. Until we receive the scenarios upon our follow-up within one year following this investigation's close and are satisfied they are consistent with the approach in the updated policy, this complaint will be considered well-founded and conditionally resolved[7].

Name tags for border officers not a violation

A CBSA decision to have border service officers wear name tags indicating their surname on their uniforms prompted 43 officers to complain that this was an improper use and disclosure of their personal information.

The complainants alleged that being identified by name rather than a badge number would increase their vulnerability to harassment and intimidation from disgruntled travellers. The CBSA submitted that its policy is in line with those of its partners, including the RCMP, the Canadian Armed Forces, Correctional Service Canada and the United States Customs and Border Protection—all institutions in which frontline officers wear name tags.

We determined that a CBSA front-line employee's surname as displayed on a name tag fell under an exception to the definition of personal information, which in essence permits the use and disclosure of information that would reveal that an individual is, or was, an officer or employee of a government institution. The underlying purpose of this exception is to ensure that the state and its agents are held accountable to the public.

7 The investigation substantiated the allegations and the institution committed to implementing the recommendations made by this Office. The institution must now demonstrate their implementation within the timeframe specified.

Accordingly, the complaints were determined to be not well-founded.

Violating principle of "need-to-know" leads to data breach

In this case, the complainant drew our attention to an article in *La Presse* newspaper, which reported that Aboriginal Affairs and Northern Development Canada (AANDC) had created a document listing the names of people who had made requests, under the *Access to Information Act,* related to a former Minister's expenses. The article mentioned the name of one of the people who had made a request and further indicated the document had been shared with AANDC personnel outside the Department's Access to Information and Privacy (ATIP) division.

AANDC reported the data breach to our Office on the same day, and provided a list of people within the Department who had been given copies of the document. The list included officials in Finance and Contracting Services, Planning and Resource Management and Communications.

Under the *Privacy Act*, personal information collected is to be used by the institution only for the purpose for which the data was obtained. In this instance, individuals' personal information was collected solely to ensure the ATIP division would know where to send its response to their requests. Sharing it beyond the ATIP division violated the *Privacy Act.*

In addition, an AANDC investigation traced the document obtained by *La Presse* to a copy made for an official outside the ATIP division. In this case, AANDC also violated the Treasury Board President's *Policy on Access to Information*, which states that a requester's identity must be protected and only disclosed when there is a clear need-to-know in order to perform duties or functions related to a lawful program or activity.

We recommended that AANDC review its policies and procedures for processing ATIP requests—and advise our Office within six months of the measures it has taken to ensure the need-to-know principle is respected. The Department has since responded and we are satisfied with the steps taken to help prevent a similar breach in the future.

Sharing of health information excessive to meet objectives of the Public Service Employment Act

Our Office undertook an investigation of the Public Service Commission (PSC) which underlined that while the *Privacy Act* allows personal information to be disclosed without consent in certain circumstances, such disclosure must be limited to what is absolutely necessary.

During an investigation by the PSC into allegations of fraud in an appointment process, the complainant to our Office (who was the subject of the PSC investigation) and four

other people were interviewed by a PSC investigator. The complainant provided that investigator with a letter from her doctor that included details about her medical condition at the time of the alleged incident.

Following interviews, the PSC investigator compiled a report, including the doctor's letter, and provided copies to the complainant and each of the four witnesses. This was, according to the PSC, in keeping with its *Investigator's Guide*—giving individuals who may be affected by the investigation a chance to comment prior to the preparation of a final report.

We noted however, that the *Investigator's Guide* also states that, "if a person is affected by only a minor part of the factual report… the investigator may decide that only that part of the factual report needs to be shared with this person."

In our opinion, the PSC investigator should have exercised greater discretion in determining what information in the factual report needed to be shared with witnesses. We therefore concluded the PSC disclosed personal information without consent, in contravention of the *Privacy Act*, and the complaint was well-founded.

The PSC committed to refining its procedures to ensure compliance with the *Privacy Act* when disclosing personal information, with particular attention to applying the "need-to-know" principle in determining how much information should be shared in the reports. Our Office will follow-up with the PSC within the next year to ensure that it has implemented all of the proposed changes to its investigation process and is respecting its obligations under the *Privacy Act*.

Retroactive removal of Privacy Act *provisions leaves gun registry complainant with no recourse*

The complainant alleged that the RCMP used personal information from the now-defunct long-gun registry to locate and seize registered weapons from homes that were evacuated due to flooding in the High River, Alberta area in June 2013.

The complainant stated that an RCMP member could be overheard saying he had "located all the firearms" in a video recording showing segments of its emergency response efforts. The complainant said this indicated the member knew the exact number of weapons in a particular house—something that could have been known only by accessing information in the registry.

All information in the registry was to have been destroyed following the passage of the *Ending the Long-Gun Registry Act* in April 2012. For its part, the RCMP asserted that all information in the registry was indeed destroyed by the end of October 2012. Our investigation sought to determine whether the RCMP continued to use personal information

originating from the registry, such as copies of the registry, after its supposed destruction and, in particular, whether it used such information in connection with the High River incident.

In its representations during our investigation, the RCMP took the position that the registry itself was destroyed in October 2012 and that no RCMP detachments, including the High River RCMP, kept copies. We find it noteworthy that the RCMP indicated that in some instances, personal information taken from the long-gun registry and used prior to the enactment of the *Ending the Long-Gun Registry Act*, may have been retained, for example, in case files, notebooks, or other related investigative records. Further, the use of that personal information in the context of an operational investigation would be consistent with the purpose for which it was compiled, but it did not elaborate further.

We were unable to pursue this matter any further as in the later stage of our investigation, Parliament passed Bill C-59. It included amendments to the *Ending the Long-Gun Registry Act* exempting all registry records and copies of records from *Privacy Act* provisions, retroactive to October 2011. Based on the information gathered to that point, we were unable to conclude that the RCMP had contravened the *Privacy Act*.

The retroactive removal of the protections of the *Privacy Act* is unprecedented. In a June 2015 submission on Bill C-59 to the Standing Senate Committee on National Finance, Commissioner Therrien stressed the importance of allowing individuals an opportunity to challenge the government's treatment of their personal information.

Collection of Royal Canadian Mounted Police member's health information unnecessary

The complainant, an RCMP member, alleged that, in 2003, the organization collected her medical and financial information without her consent.

The complainant applied to Veterans Affairs Canada (VAC) for a disability pension—which VAC adjudicates and administers on behalf of the RCMP under a memorandum of understanding between the two institutions. VAC subsequently notified the complainant that she had been awarded a disability pension in a letter that included the complainant's medical information, as well as the amounts of compensation she would receive. VAC sent a copy of the letter to the RCMP's National Compensation Policy Centre. Another copy was filed with the RCMP's branch dealing with national health services.

It is our view that the National Compensation Centre, which is part of the RCMP's Human Resources branch, does not need the complainant's personal medical information in order to administer her pension benefits—nor does the RCMP's National Health Services Branch require her personal financial

information in order to provide health services. We found this to be a violation of Section 4 of the *Privacy Act*—personal information collected by a government institution must relate directly to an operating program or activity of the institution—and so this complaint was well-founded.

During the course of our investigation of this complaint, we were presented with evidence that, in 2005, the RCMP and VAC agreed—at the RCMP's request—that VAC would stop sending disability claimants' medical information to the RCMP National Compensation Policy Centre. Despite this agreement, VAC continued to send—and the National Compensation Centre continued to collect—this personal information until VAC finally ended the practice in 2010.

We strongly recommended that this agreement be updated to provide comprehensive guidance on the proper flow of such sensitive personal information between the two institutions. We will follow-up with the RCMP in one year in order to verify that the MOU has been updated accordingly.

Records deemed "transitory" prematurely destroyed

The complainant was released from his employment with the Department of National Defence (DND) following a hearing that recommended termination of his enrollment in a Canadian Armed Forces training program. The complainant appealed the decision, and asked DND for a copy of the audio recording of the hearing in which he participated. DND informed him that the recording had been erased.

The complainant alleged this violated Section 6(1) of the *Privacy Act,* that a government institution must retain personal information that has been used for an administrative purpose for at least two years following the last time the information was used unless the individual to whom it relates consents to its disposal. This provision exists to ensure the affected individual has a reasonable opportunity to obtain access to the information.

DND submitted that the audio recording was a "transitory" record, used only by the secretary of the Progress Review Board (PRB) to draft the hearing minutes, which constituted the "official" record of the proceeding. The complainant argued that the minutes were inaccurate and incomplete, but without the recording, he was unable to substantiate this allegation.

At issue was whether the audio recording of the hearing was subject to the retention requirements set out in the *Privacy Act*—in which the term "transitory" does not appear. In this instance, there is no question the audio recording would have contained the complainant's personal information and that it was used for an administrative purpose: to

determine his future in the training program. Consequently, it was subject to the retention provisions in the *Act*. We concluded this complaint was well-founded.

During this investigation, we discovered that DND keeps the audio recordings of some hearings and not others, with no apparent rationale for keeping one and not another. We encouraged DND to develop and implement procedures with respect to the collection, retention and disposal of information collected as part of PRB hearings—and in the meantime, retain either the recordings or verbatim hearing transcripts for at least two years, unless the affected individual consents to earlier destruction.

EARLY RESOLUTION

The proportion of complaints dealt with through negotiation and conciliation to the satisfaction of parties involved increased in 2014-2015. In all, 422 complaints were closed through the early resolution process, compared to 345 in the previous year. Although there was a slight increase in the average time to resolve a complaint in this way—from 2.11 months in 2013-2014 to 3.24 months in the year just passed—the process is by all accounts playing its intended role in reducing the number of standard investigations being conducted.

Of all complaints closed during 2014-2015, 34 percent were settled by early resolution. Standing out however is the fact that close to 60 percent (101 of 176) of the access to personal information complaints against the Correctional Service of Canada (CSC) during the last fiscal year were resolved through this process, an exceptional outcome demonstrating a clear willingness by all parties to resolve such disputes in a more efficient and effective manner.

EARLY RESOLUTION IN ACTION

Complaint of unauthorized disclosure against Correctional Service Canada

In this matter, the complainant alleged that all outgoing personal correspondence and request forms including protected information at a Saskatchewan penitentiary were placed in an unsecured tray accessible to anyone in the reception area. Following the complaint and resulting inquiries made by our Office, CSC installed a new locked box to replace the tray and to address the privacy concern. As a result, the complaint was resolved.

Denial of access complaint against the Department of Foreign Affairs, Trade and Development (DFATD)

An individual alleged that there were missing records as part of the response he received to his personal information request from DFATD. Our Office made an inquiry to the Department, which conducted another search, found the record at issue and provided it to the complainant, thereby resolving the matter.

PROGRESS ON TIME DELAYS

Under the *Privacy Act*, federal institutions must respond to an individual's request for access to their personal information within 30 days. In certain circumstances, institutions can request the time limit be extended for an additional 30 days.

Complaints about institutions failing to adhere to these time limits have been consistently high in recent years. In 2014-2015, they reached another record high of 2,612—more than four times as many as in the previous year—although much of this massive increase was due to multiple complaints filed by individual complainants. If the multiple complaints are removed from the equation, the number of time limit complaints actually decreased from the previous year (from 585 to 377), due in part to a 35 percent reduction in the number of time limit complaints against CSC.

The Office continues to work collaboratively with institutions, such as CSC, to address time limit problems, including requesting action plans and commitment dates for the production of personal information requested by an individual. Going forward, we will continue our efforts and monitor developments closely to determine if the momentum of 2014-2015 is a one-time showing or the start of a larger trend.

Audits

Under the *Privacy Act,* the Commissioner may review the privacy practices of federal institutions and recommend remedial actions when needed. Although the *Act* provides no enforcement powers, the Commissioner may publish the findings and recommendations. As well, our Office typically follows up with audited institutions two years after the original audit report was issued, asking what actions they have taken to address our recommendations.

Results of follow-up at Veterans Affairs Canada

In 2014-2015, we followed up on our 2012 audit of the personal information handling practices at VAC. In its response, VAC reported that it had implemented all 13 of the recommendations in our audit report. For example, a system for its primary Client Service Delivery Network is now in place that assures only those employees with a need to know can access a client's medical and other sensitive personal information.

VAC has also set up a record disposal process to ensure personal information collected on the Network is not retained any longer than necessary. It has also set up a new function for employees to record and confirm receipt of client consent in the Network. This will help to ensure VAC clients are informed, understand

and agree to how and why their information may be collected, used and disclosed.

Follow-up to come on Canada Revenue Agency audit of 2013

As noted in chapter four, we audited the CRA's personal information handling practices in 2013. We will be following up on the CRA's response to our recommendations in the audit in the winter of 2016.

Releasing audit on portable storage devices

As mentioned earlier in the Commissioner's message, a number of significant data breaches involving portable storage devices in recent years—such as memory sticks and portable hard drives—led the Office to initiate an audit of the management of these devices within federal institutions in 2014. More information can be found in chapter five.

New audit - Employment and Social Development Canada/Shared Services Canada

The Office began an audit of personal information handling practices at ESDC and Shared Services Canada (SSC) in February 2015, with a focus on areas of privacy risk within the Old Age Security program. We expect to conclude the audit and issue a public report in 2016.

Public interest disclosures, including those made under paragraph 8(2)*(m)*

Paragraph 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 head of the institution:

- 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.

Any institution intending to make a disclosure under this provision is required to notify our Office in writing, prior to the disclosure if possible or immediately afterwards.

Once notified, our Office reviews the disclosure and may express any concerns or recommend that the institution, if it has not already done so, notify the individual affected by the disclosure. If the department declines to notify the individual, the Commissioner is empowered to do so. However, the decision to release personal information in the public interest rests solely with the head of the institution and the Commissioner has no authority to prevent it.

In 2014-2015, we handled 266 notifications under paragraph 8(2)(m) of the *Privacy Act* or under other similar provisions in other federal legislation. While this was similar to the number received in the previous year, the total received in 2013-2014 was up some 300 percent from each of the two years prior. This increase is in large part due to improved reporting by some institutions. ESDC in particular has made it a practice to report disclosures made to police in cases where clients of the Department have threatened serious harm to themselves or others.

Outreach Activities

PIA workshops

Our Office continued to offer seminars to federal institutions interested in enhancing their capacity to conduct and submit thorough and effective PIAs to our Office. In response to feedback from institutions in the previous year, we changed our approach somewhat, using smaller, more intimate lunch and learn sessions in order to facilitate discussion. The sessions were geared to different audiences, with some providing a basic introduction to and overview of the PIA process and others covering more advanced topics such as the risks to privacy associated with technology.

Feedback was very positive and we plan to continue offering these sessions in the future, using different formats and covering various subjects according to the needs of the community.

What to expect when filing a complaint

In late 2014-2015, we posted on our website a new document designed to help Canadians understand how the *Privacy Act* complaint process works.

Entitled, "What to expect during a complaint investigation under the *Privacy Act*," the new publication uses a question-and-answer format to cover the basics, from the organizations covered by the *Privacy Act* to how our early resolution process works. The guide will also help organizations better understand the process and the expectations of our Office during the course of an investigation.

Speeches, presentations and exhibits

Commissioner Therrien delivered speeches to public sector privacy professionals in December at both the Canadian Access and Privacy Association (CAPA) Conference and the Access to Information and Privacy Community Meeting.

Meanwhile, our Office's exhibiting activity reaching the public sector included presence at the 2014 APEX Annual Conference, a forum highly attended by federal Public Service executives.

Representatives from our Office also made several presentations to federal employees during 2014-2015, including, for example, those on:

- cross-border information sharing at the Biometrics Community of Practice Workshop hosted by Defence Research and Development Canada;
- protecting privacy in the human resources context at a meeting of HR practitioners hosted by the HR Council; and
- privacy and confidentiality matters within the realm of federally regulated health research before Health Canada's Research Ethics Board.

Appendix 1 – Definitions

GENERAL COMPLAINT TYPES

1. Access

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

Correction/Notation – The institution is alleged to have 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 is alleged to have not been provided in the Official Language of choice.

Fee - Fees are alleged to 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) is alleged to not adequately describe the personal information holdings of an institution.

2. Privacy

Accuracy – The institution is alleged to have failed to take all reasonable steps to ensure that personal information that is used for an administrative purpose is as accurate, up-to-date and complete as possible.

Collection - Personal information collected is alleged to have not been 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 alleged to have not been 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 alleged to have been 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 is alleged to have not responded within the statutory limits.

Extension notice – The institution is alleged to have not provided 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 is alleged to have failed to correct personal information or has not placed a notation on the file within 30 days of receipt of a request for correction.

GENERAL 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.

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

Well founded and conditionally resolved: The investigation substantiated the allegations and the institution committed to implementing the recommendations made by this Office and demonstrated their implementation within the timeframe specified.

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.

Settled: The OPC helped negotiate a solution that satisfied all parties during the course of 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.

No jurisdiction: Based on the preliminary information gathered, it was determined that the *Privacy Act* did not apply to the institution or to the complaint's subject matter. As a result, no report is issued.

2. Other

Early resolution: Applied to situations in which the issue is dealt with before a standard investigation is undertaken. For example, if an individual complains about an issue the OPC has already investigated and found to be compliant with the *Privacy Act*, we explain this to the individual. We also receive complaints in which a standard 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."

Appendix 2 – Statistical tables

***Privacy Act* Complaints 2014-2015**

Category	Total
Accepted	
Access	382
Time Limits	377
Privacy	281
Total accepted and active	**1040**
Total accepted and in abeyance*	2937
Closed through Early Resolution	
Access	225
Time Limits	71
Privacy	126
Total	**422**
Closed through Standard Investigation	
Access	225
Time Limits	409
Privacy**	851
Total	**1485**
Total closed	**1907**
Breaches Received	
Accidental Disclosure	187
Theft	8
Loss	27
Unauthorized Access	34
Total received	**256**

* *These complaints in abeyance were submitted by a small number of individual complainants. The 2937 complaints include: 690 Access, 2236 Time Limits, 11 Privacy*

** *includes several series of related complaints Employment and Social Development Canada (164), Justice Canada (165), Health Canada (339).*

Privacy Act Breaches by Institution

Respondent	Incident
Aboriginal Affairs and Northern Development Canada	9
Agriculture and Agri-Food Canada	1
Canada Revenue Agency	38
Canadian Environmental Assessment Agency	1
Canadian Heritage	1
Canadian Human Rights Commission	1
Citizenship and Immigration Canada	76
Communications Security Establishment Canada	1
Correctional Service Canada	19
Employment and Social Development Canada	4
Fisheries and Oceans	3
Foreign Affairs, Trade and Development Canada	7
Justice Canada	2
National Defence	2
National Research Council	1
Natural Resources Canada	1
Privy Council Office	1
Public Prosecution Service of Canada	2
Public Service Commission Canada	1
Royal Canadian Mounted Police	5
Statistics Canada	3
Transport Canada	7
Treasury Board of Canada Secretariat	1
Veterans Affairs Canada	65
Veterans Review and Appeal Board Canada	4
Grand Total	**256**

Privacy Act Treatment Times - All Closed Files by Disposition

Complaint Type	Count	Average Treatment Time (Months)
Well-founded*	406	7.06
Not well-founded	189	13.66
Discontinued	129	10.92
Well-founded resolved	40	19.14
Settled	29	12.03
Resolved following a standard investigation	24	13.13
Resolved via the ER investigation process	422	3.24
Grand Total	**1239**	**7.79**

* *Includes one representative complaint for each of the following breach related complaints and excludes the remainder in brackets: ESDC (164), JC (165), HC (339)*

Privacy Act Treatment Times - Standard Investigations by Complaint Type

Complaint Type	Count	Average Treatment Time (Months)
Access		
Access	220	14.59
Correction-Notation	3	7.44
Language	2	10.05
Time Limits		
Time Limits	375	5.35
Extension Notice	34	4.02
Privacy		
Use and Disclosure*	152	15.45
Collection	22	18.26
Retention and Disposal	7	21.35
Accuracy	1	0.95
Other	1	4.52
Grand Total	**817**	**10.15**

* *Includes one representative complaint for each of the following breach related complaints and excludes the remainder in brackets: ESDC (164), JC (165), HC (339)*

PA Treatment Times - Early Resolution Cases by Complaint Type

Complaint Type	Count	Average Treatment Time (Months)
Access		
Access	222	2.78
Correction – Notation	2	1.39
Language	1	2.00
Time Limits		
Time Limits	70	2.01
Correction – Time Limits	1	7.25
Privacy		
Use and Disclosure	99	5.24
Collection	19	1.94
Retention and Disposal	6	3.98
Accuracy	2	9.48
Grand total	**422**	**3.24**

PA Dispositions of Access and Privacy Complaints by Institution

Respondent	Well-founded	Well-founded resolved	Not well-founded	Resolved following a standard investigation	Discontinued	Resolved via the ER investigation process	Settled	Grand Total
Aboriginal Affairs and Northern Development Canada	2	1		2	9	3		17
Agriculture and Agri-Food Canada	0	0				1		1
Atomic Energy of Canada Limited	0	0				1		1
Canada Border Services Agency	1	7	48	1	7	23		87
Canada Economic Development for Quebec Regions	0	0		1				1
Canada Mortgage and Housing Corporation	0	0				1		1
Canada Post Corporation	0	3	2			10		15
Canada Revenue Agency	0	5	9	8	5	22		49
Canadian Air Transport Security Authority	0	0	2					2
Canadian Broadcasting Corporation	0	1				3		4
Canadian Food Inspection Agency	0	1				4		5
Canadian Heritage	1	0	1					2
Canadian Human Rights Commission	0	0			1			1
Canadian Security Intelligence Service	0	1	6	1		10		18
Citizenship and Immigration Canada	1	1	4		3	8		17
Communications Security Establishment	0	0	1	0				1
Correctional Service Canada	9	11	26	4	16	101	9	176
Department of Foreign Affairs, Trade and Development	0	0			1	1		2
Department of National Defence	3	0	8	2	6	13	5	37
Employment and Social Development Canada	170	1	1		8	38	1	219
Environment Canada	0	0				5		5
Farm Credit Canada	0	0			1	1		2
Fisheries and Oceans	0	0			3	3	2	8
Health Canada	340	0	1	1	1	5	1	349
Immigration and Refugee Board	0	0				1		1

PA Dispositions of Access and Privacy Complaints by Institution

Respondent	Well-founded	Well-founded resolved	Not well-founded	Resolved following a standard investigation	Discontinued	Resolved via the ER investigation process	Settled	Grand Total
Industry Canada	0	0				3		3
Justice Canada	167	1	2	1	6	8		185
Military Police Complaints Commission	0	0	2					2
National Research Council Canada	0	0			1			1
Natural Resources Canada	0	0			2	1		3
Nunavut Water Board						1		1
Office of the Commissioner of Official Languages	1	0						1
Office of the Correctional Investigator Canada	0	1						1
Office of the Information Commissioner of Canada	0	1						1
Office of the Superintendent of Financial Institutions Canada	0	0				1		1
Parole Board of Canada	0	0	2			3		5
Passport Canada	0	0	1					1
Public Health Agency of Canada	0	0	1		2			3
Public Safety Canada	1	0						1
Public Service Commission of Canada	0	0	2			2		4
Public Works and Government Services Canada	0	0	4		5	7		16
Royal Canadian Mint	0	0				1		1
Royal Canadian Mounted Police	18	2	20	1	25	54	9	129
Service Canada	2	0	3	1	1	4		11
Shared Services Canada	0	0				3		3
Statistics Canada	0	0	1			4		5
Transport Canada	1	0	2			1		4
Treasury Board of Canada Secretariat	0	0	1				1	2
Veterans Affairs Canada	4	1	8		2	3	1	19
Veterans Review and Appeal Board Canada	1	0			1	1		3
Grand Total	**722**	**38**	**158**	**23**	**106**	**351**	**29**	**1427**

PA Top 10 Institutions by Complaint Accepted

Respondent	Access		Time limits		Privacy		Grand Total
	Early resolution	Investigation	Early resolution	Investigation	Early resolution	Investigation	
Correctional Services Canada	58	33	34	158	20	11	314
Royal Canadian mounted Police	48	26	3	33	4	26	140
Canada Revenue Agency	10	12	11	12	12	49	106
National Defence	14	16	1	25	5	7	68
Canada Border Services Agency	28	10		18	2	8	66
Citizenship and Immigration	6	8	3	14	4	7	42
Employment and Social Development Canada	5	6	3	3	16	2	35
Canada Post Corporation	4	5		3	12	8	32
Canadian Security Intelligence Service	10	9	1	1			21
Aboriginal Affairs and Northern Development	2	6	1	5		5	19
Grand total	**185**	**131**	**57**	**272**	**75**	**123**	**843**

PA Top 10 Institutions in 2014-2015 by Complaints Accepted Year-Over-Year

Organization	2011-2012	2012-2013	2013-2014	2014-2015
Correctional Services Canada	326	284	514	314
Royal Canadian mounted Police	117	182	265	140
Canada Revenue Agency	65	76	61	106
National Defence	115	90	84	68
Canada Border Services Agency	55	88	56	66
Citizenship and Immigration	22	17	53	42
Employment and Social Development Canada	26	1030	78	35
Canada Post Corporation	22	21	14	32
Canadian Security Intelligence Service	32	19	17	21
Aboriginal Affairs and Northern Development	11	18	10	19
All Other Federal Departments and Agencies	195	448	625	197
Grand Total	**986**	**2273**	**1777**	**1040**

PA Complaints Accepted by Institution

Respondent	Early resolution	Investigation	Grand total
Aboriginal Affairs and Northern Development Canada	3	16	19
Agriculture and Agri-food Canada	1		1
Atomic Energy of Canada Limited	1		1
Canada Border Services Agency	30	36	66
Canada Mortgage and Housing Corporation	1		1
Canada Post Corporation	16	16	32
Canada Revenue Agency	33	73	106
Canada School of Public Service	1	1	2
Canadian Broadcasting Corporation	4	9	13
Canadian Food Inspection Agency	3	2	5
Canadian Heritage	1		1
Canadian Human Rights Commission		3	3
Canadian Nuclear Safety Commission		1	1
Canadian Radio-Television and Telecommunications Commission	2		2
Canadian Security Intelligence Service	11	10	21
Canadian Transportation Agency		1	1
Citizenship and Immigration Canada	13	29	42
Communications Security Establishment		1	1
Correctional Service Canada	112	202	314
Department of Foreign Affairs, Trade and Development	3	2	5
Department of National Defence	20	48	68
Employment and Social Development Canada	24	11	35
Environment Canada	6	1	7
Farm Credit Canada	2	1	3
Fisheries and Oceans	2	12	14
Health Canada	5	10	15
Immigration and Refugee Board	1	3	4
Industry Canada	4	7	11
Justice Canada	7	7	14
National Research Council Canada		2	2
Natural Resources Canada	1	2	3

PA Complaints Accepted by Institution

Respondent	Early resolution	Investigation	Grand total
Nunavut Water Board	1		1
Office of the Commissioner of Lobbying of Canada	1		1
Office of the Commissioner of Official Languages	1		1
Office of the Information Commissioner of Canada		1	1
Office of the Superintendent of Financial Institutions Canada	1		1
Parole Board of Canada	2	12	14
Privy Council Office	2	2	4
Public Health Agency of Canada	1		1
Public Prosecution Service of Canada	1		1
Public Sector Integrity Commissioner of Canada		2	2
Public Service Commission of Canada	2		2
Public Works and Government Services Canada	5	4	9
Royal Canadian Mint	1		1
Revera Inc.		1	1
Royal Canadian Mounted Police	55	85	140
Service Canada	5	6	11
Shared Services Canada	3		3
Statistics Canada	3	2	5
Transport Canada	4	8	12
Treasury Board of Canada Secretariat	2	1	3
Veterans Affairs Canada	6	4	10
Veterans Review and Appeal Board Canada	1	1	2
VIA Rail Canada		1	1
Grand total	**404**	**636**	**1040**

PA Complaints Accepted by Province/Territory

Province/territory	Early resolution		Investigation		Total Count	Total percentage
	Count	Percentage	Count	Percentage		
Alberta	39	3.75%	29	2.79%	68	6.54%
British Columbia	55	5.29%	122	11.73%	177	17.02%
Manitoba	13	1.25%	34	3.27%	47	4.52%
New Brunswick	9	0.87%	21	2.02%	30	2.88%
Newfoundland and Labrador	5	0.48%	3	0.29%	8	0.77%
Northwest Territories		0.00%		0.00%	0	0.00%
Not specified	2	0.19%		0.00%	2	0.19%
Nova Scotia	12	1.15%	12	1.15%	24	2.31%
Nunavut		0.00%	2	0.19%	2	0.19%
Ontario	141	13.56%	214	20.58%	355	34.13%
Other (not US)	8	0.77%		0.00%	8	0.77%
Prince Edward Island		0.00%	1	0.10%	1	0.10%
Quebec	82	7.88%	158	15.19%	240	23.08%
Saskatchewan	22	2.12%	22	2.12%	44	4.23%
United States	1	0.10%	4	0.38%	5	0.48%
Yukon	4	0.38%		0.00%	4	0.38%
Blank	11	1.06%	14	1.35%	25	2.40%
Grand total	**404**	**38.85%**	**636**	**61.15%**	**1040**	**100.00%**

PA Dispositions by Complaint Type

Complaint type	Well-founded	Well-founded resolved	Not well-founded	Resolved following a standard investigation	Discontinued	Resolved via the ER investigation process	Settled	Grand total
Access								
Access	6	35	77	17	65	222	20	442
Correction - Notation			2		1	2		5
Language		1				1	1	3
Time limits								
Time limits	336	2	19		18	70		445
Extension	16		12	1	5			34
Correction - Time limits						1		1
Privacy								
Use and disclosure	711	1	72	5	24	99	7	919
Collection	4	1	4		12	19	1	41
Retention and disposal	1		3		3	6		13
Accuracy				1		2		3
Other					1			1
Grand total	**1074**	**40**	**189**	**24**	**129**	**422**	**29**	**1907**

PA Dispositions of Time Limits by Institution

Respondent	Well-founded	Well-founded resolved	Not well-founded	Resolved following a standard investigation	Discontinued	Resolved via the ER investigation process	Grand total
Aboriginal Affairs and Northern Development Canada	2		3			1	6
Canada Border Services Agency	13		2				15
Canada Post Corporation	1		2				3
Canada Revenue Agency	8		4			11	23
Canadian Security Intelligence Service			1			1	2
Citizenship and Immigration Canada	14		2		2	3	21
Correctional Service Canada	200	2	7		8	37	254
Department of Foreign Affairs, Trade and Development	1						1
Department of National Defence	24		1		1	4	30
Employment and Social Development Canada	7		1		1	3	12
Environment Canada						1	1
Farm Credit Canada						1	1
Fisheries and Oceans	8		1		2		11
Health Canada	5		1			1	7
Industry Canada	1			1	5	1	8
Justice Canada	1				1		2
Parole Board of Canada			2				2
Privy Council Office	13		2				15
Royal Canadian Mounted Police	45		2		1	4	52
Service Canada					2	1	3
Transport Canada	5						5
Veterans Affairs Canada	4					2	6
Grand total	**352**	**2**	**31**	**1**	**23**	**71**	**480**

Appendix 3 – Investigation process

Intake

Individuals make written complaints to our Office about violations of the *Privacy Act*. Our Intake Unit reviews the matter to determine whether it constitutes a complaint – i.e., whether the allegations could constitute a contravention of the Act – and the most efficient manner in which to resolve it. An individual may complain about any matter specified in section 29 of the *Privacy Act* – for example, denial of access, or unacceptable delay in providing access to his or her personal information held by an institution; improper collection, use or disclosure of personal information; or inaccuracies in personal information used or disclosed by an institution. The Intake Unit is also sometimes able to immediately address issues, eliminating the need for our Office to pursue the matter as a standard investigation. In these cases, we simply close the matter as an early resolution. The Privacy Commissioner may also initiate a complaint if satisfied there are reasonable grounds to investigate a matter.

Complaint?

No:
The individual is advised, for example, that the matter is not in our jurisdiction.

Yes:
An investigator is assigned to the case.

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

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

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

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

Analysis (on next page)

Settled? (on next page)

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 4 – Report of the Privacy Commissioner, Ad Hoc

For the 2014-2015 reporting period, this role was filled by two individuals who each submitted the following reports.

JOHN H. SIMS, Q.C. FOR THE PERIOD BETWEEN APRIL 1 AND DECEMBER 15, 2014

This is the second year that it has been my pleasure to report on the activities of the Office of the Privacy Commissioner, Ad Hoc. On April 1, 2007, the Office of the Privacy Commissioner (OPC) became subject to the *Privacy Act*. The law that brought this about did not create at the same time a separate mechanism to investigate any complaints that an access request to the OPC might have been improperly handled.

Since it is a cardinal principle of access to information law that decisions on the disclosure of government information should be reviewed independently, the office of an independent Privacy Commissioner, *Ad Hoc* was created and given the authority to investigate any such complaints in respect of the OPC.

More specifically, pursuant to subsection 59(1) of the *Privacy Act*, the Privacy Commissioner delegated to me, as Privacy Commissioner, Ad Hoc*:*

> *The powers, duties and functions of the Privacy Commissioner set out in sections 29 through 35 and in section 42 of the Act, subject to the following restrictions or limitations:*
>
> *Pursuant to paragraph 59(2)(a), the delegate shall not investigate any complaint resulting from a refusal to disclose personal information by reason of paragraph 19(1)(a) or (b) or section 21 of the Act.*

I was the fourth person to hold this office.

Two complaints from last year were still outstanding as this year began, and three new ones were received. Three of the five complaints were disposed of; of these, **none was well-founded.** The investigation of the last two complaints (both relating to the same incident) was not completed before the end of the fiscal year. The results of that investigation will be included in the next annual report.

The main issue in all three of the completed complaints concerned the proper application of section 22.1 of the *Privacy Act*. In the first instance, this mandatory exemption prevents the disclosure of personal information both obtained or created by the OPC during an investigation. Once the investigation and all related proceedings are finally concluded, however, the exemption is partially lifted. At that point, subsection 22.1(2) of the Act provides that the OPC shall not refuse to disclose any personal information that was created by the Commissioner or on his behalf.

In each of the three resolved complaints, an individual requested files related to an OPC investigation. In one situation, the OPC investigations had been concluded by the time the requests for information were made. In a second situation, the investigation was still on-going at the time the requester asked for the information.

Our review of the complaints showed that, in each case, the OPC had applied the exemption properly. In the case of the concluded investigations, the OPC exempted only the personal information obtained by it during the course of that investigation.

In the case of the on-going investigation, the OPC exempted all documents related to that file, whether obtained or created by it during the investigation.

All three complaints also raised secondary issues. In some instances, for example, the OPC properly exempted certain records from disclosure on the basis that they did not contain personal information about the requester but personal information about another individual (section 26) or that they did not contain personal information at all (section 12).

Finally, one of the three resolved complainants also raised concerns about how two other government departments had handled the requester's personal information, and about how the OPC had investigated these complaints about the other departments. This Office, however, does not have jurisdiction to address these issues. Our mandate is limited to receiving and investigating complaints that personal information under the control of the OPC itself may have been improperly handled. We cannot review how the OPC conducts its investigations or how other departments manage personal information.

The fourth and fifth complaints both concern the loss of a portable hard drive containing sensitive personal information relating to staff of the Office of the Privacy Commissioner and of the Office of the Information Commissioner. This investigation was not finished before the end of the fiscal year, although, as of the date of writing this report, it is largely completed. The results will be reported in the next annual report.

It has been a privilege for me to serve a term as the Privacy Commissioner, Ad Hoc. The existence of this Office ensures the integrity of the complaints process, which is an essential element in any access to information regime. It has been an honour to be part of this.

Respectfully submitted,

John H. Sims, Q.C.

DAVID LOUKIDELIS, Q.C., DECEMBER 16, 2014 TO MARCH 31, 2015

The role of Privacy Commissioner, Ad Hoc was created after the Office of the Privacy Commissioner (OPC) became subject to the *Privacy Act* in 2007. The law that brought this about did not create a separate process for investigating complaints about OPC responses to access requests made to it as an institution under the law.

Since it is a fundamental principle of access to information law that decisions on the disclosure of government information should be reviewed independently, the office of an independent Privacy Commissioner, Ad Hoc was created and given the authority to investigate any such complaints about the OPC. The role of my office is to investigate and respond to complaints that the OPC has not responded appropriately to access requests made to it as an institution.

I am the fifth person to hold this office since 2007, having been appointed in December 2014, so this is the first year for which it has been my pleasure to report on the activities of my office.

Outstanding complaints from previous year

Two complaints from last year were still outstanding as this year began. They are related to the ongoing investigation into the hard-drive that the OPC lost 2014. This matter is being investigated by my predecessor, John Sims, who will conclude these complaints once his investigation is complete.

New complaints this year

Three complaints were received at the start of my mandate, two of them from the same person.

One complainant requested an investigation of the format of the response to the individual's access request to the OPC, as well as an investigation of the exemptions applied, specifically sections 22.1 and 26 of the *Privacy Act*. The complainant also alleged that his personal information had been intercepted and monitored by a foreign government.

My investigation was limited to the complaint about the exemptions applied, the format of the request and the search process. Allegations that the complainant's personal information was intercepted and monitored by foreign government agencies are outside my mandate.

The complainant's concern about the format of the OPC's response caused me to consider whether the OPC had complied with section 17.1 of the *Privacy Act*. The complainant wished to have paper copies of the responsive records, not electronic copies, as the OPC had provided.

Section 17.1 does not specify whether requested personal information is to be provided in electronic or paper form. It only indicates that the individual must be provided "with a copy thereof." In the age of computers, most records responsive to a request are provided electronically and, where paper copies are provided, they are scanned into software used specifically to process access requests. To be more environmentally conscientious and to minimize cost, most Government of Canada institutions provide access to records by providing a CD-ROM when there is a large volume of records. It is the policy of the OPC to provide a CD-ROM when the request yields more than 100 pages. This was the case here. The OPC did, however, indicate that they would have provided the requested format had the complainant asked.

The individual's complaint about the exemptions applied concerned the proper application of sections 22.1(1) and 26 of the *Privacy Act*. Section 22.1(1) exempts from disclosure to an applicant any information "obtained" or "created" in the course of an OPC investigation. This is a mandatory exemption: if it applies, the OPC has no choice but to refuse disclosure. Once the investigation and all related proceedings are finally concluded, however, the exemption is partially lifted. At that point, the exemption no longer applies to documents created during the investigation. My investigation revealed that the disputed documents had been obtained during the course of the OPC's own investigations. The OPC therefore properly applied the mandatory section 22.1(1) exemption in refusing to disclose these documents.

Section 26 of the *Privacy Act* provides that personal information requested under section 12(1) about an individual other than the individual who made the request must be withheld if disclosure is prohibited under section 8. Review of the records to which section 26 was applied in this case confirmed that the exempted information was not the complainant's personal information. Section 26 had been applied to protect the names of individuals who are not employees of the Government of Canada, and I found that this complied with section 26.

The two other complaints to be mentioned here were made by the same individual in connection with the same request to the OPC. The complainant alleged that the OPC had improperly withheld personal information under section 22.1(1). The complainant also alleged that the OPC had not properly taken an extension of the time to respond and, further, had responded late.

As in the first complaint discussed above, my investigation revealed that the disputed documents had been obtained during the course of the OPC's own investigations. I therefore found that the OPC had appropriately applied section 22.1(1) in refusing to disclose these documents.

As for the time extension and response time, my investigation revealed that the request yielded 8,850 responsive pages. The OPC's access and privacy division is comprised of one director and two senior analysts. During fiscal year 2013/2014, this division received 130 access requests, 25 access consultations, 32 privacy requests and seven privacy consultations. The OPC took the position that meeting the 30-day time limit would have interfered unreasonably with its operations, including because it would have, it argued, prevented it from meeting its legislative obligations regrading other requests that it was handling at the relevant time.

There is no doubt that it would be at best challenging for one (or even both) of the senior analysts to review 8,850 pages of records, and decide which portions could be disclosed and which could not, within 30 days. Further, the OPC's access and privacy division will have, in the ordinary course, other requests that must be processed at the same time. The division also will, again in the ordinary course, have other ongoing tasks at that same time. Trying to respond to the complainant where such a large volume of records was involved would, it can be concluded, have an adverse impact on the division's ability to do its other work. To try to 'drop everything' to respond within 30 days would have adversely affected the rights of other individuals.

In the end, I concluded that responding to the request within 30 days would have unreasonably interfered with the OPC's operations and therefore that the OPC was authorized under section 15 to extend the time for response by 30 days.

As for the complaint into the lateness of the response, taking the 30-day extension into consideration, the OPC was required to provide a response within 60 calendar days. The time it takes for the response to reach a requester by mail or any other means of delivery is not included in the allotted time. In this instance, the OPC used Canada Post Expedited Parcel to send its response to the complainant. The service timelines may vary depending on destination and other factors, and the amount of time a letter or parcel takes to reach its destination is beyond the control of the sender. Ultimately, I concluded that this aspect of the complaint was also not well founded.

David Loukidelis, Q.C.