Annual Report to Parliament 2013-14

TRANSPARENCY AND PRIVACY IN THE DIGITAL AGE

Report on the *Privacy Act*

Office of the
Privacy Commissioner
of Canada

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. IP50-2014E-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

October 2014

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

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Privacy Act* for the period from April 1, 2013 to March 31, 2014.

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

October 2014

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

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Privacy Act* for the period from April 1, 2013 to March 31, 2014.

Sincerely,

Original signed by

Daniel Therrien
Privacy Commissioner of Canada

Table of Contents

1. Commissioner's Message 1

2. Privacy by the Numbers in 2013-2014 6

3. Feature: From surveillance revelations to a seminal Supreme Court of Canada ruling: 12 months of privacy at centre stage 9

4. Review of the Royal Canadian Mounted Police - Warrantless Access to Subscriber Information 17

5. The Year in Review 25
Privacy Impact Assessments (PIAs) 25
Data breaches 28
Parliament 30
Privacy compliance audits 32
Investigations 33

Appendix 1 — Definitions **41**

Appendix 2 — Statistical tables **43**

Appendix 3 — Investigation process **50**

Appendix 4 — Report of the Privacy Commissioner, *Ad Hoc* **52**

1 Commissioner's Message

The right to privacy is one of our fundamental rights and freedoms as Canadians. And amidst ever-evolving technological capacity to both collect and analyse personal information, this needs to be protected with continuing commitment and care.

I was appointed Privacy Commissioner after the end of the 2013-2014 period covered by this annual report on the *Privacy Act*. And while I was not at the organization's helm, the year gone by shows that the profile of privacy has gained prominence and for good reason. Never before in human history has personal information been as available as it now is and consequently never before has protecting personal information been as important.

Against this backdrop, the period under review was a time of mounting privacy concerns.

The year in particular was marked by the continuation of a long-running debate in Canada about lawful access to subscriber information along with a series of ongoing revelations about state surveillance activities that had impact globally as well as within our borders.

As another indicator, statistics show there was a continued rise in the number of complaints. Also continuing are complaints from a large number of individuals that arise from a single event. For example, the Office is currently investigating 339 complaints over a mass mailing by Health Canada which allegedly exposed the names and mailing addresses of some 40,000 people involved in the marijuana medical access program.

In a year where perhaps unprecedented attention was paid to public sector data breaches, the 228 separate data breaches voluntarily reported across the federal government in 2013-2014 were more than double those from the previous fiscal year. This marked the third consecutive year where a record high was reached for such reports. Accidental disclosure was provided as the reason indicated by reporting organizations behind more than two-thirds of the breaches.

Important lessons learned

Much of the attention about public sector data breaches was generated by the loss of a hard drive containing information about more than 500,000 student loan recipients from Employment and Social Development Canada (ESDC, then known as Human Resources and Skills Development Canada – HRSDC). A March 2014 Special Report to Parliament on the incident underscored the lesson that once organizations develop formal privacy and security policies, so too they must be put into practice and monitored regularly.

The OPC produced tip sheets for public servants on how to protect against data breaches when using external hard drives and other portable storage devices (see section 5). In addition, our Office is currently auditing how well personal information on such portable storage devices is being protected in 17 selected government agencies and departments.

As noted in previous years, because data breach reporting to the OPC has been voluntary, the Office could never say categorically that the number of incidents had really risen from one year to the next. The increase might simply have been the result of more diligent reporting. From now on, however, such uncertainty should be reduced, thanks to a revised *Directive on Privacy Practices* from the Treasury Board Secretariat (TBS).

The Directive makes mandatory the reporting of any "material" data breach to both the TBS and the OPC. The OPC worked with TBS to define what constitutes a material breach and also created a web-based form housed on the OPC website for federal institutions to report such breaches.

This work followed a number of breaches that highlighted the need for increased vigilance in safeguarding personal information held by organizations. For example, this year's report includes a look at the Office's investigation of ESDC and Justice Canada concerning a lost USB key. The portable device with the personal information of 5,045 people appealing their disability entitlements under the Canada Pension Plan disappeared from an office at ESDC where it was being used by a Justice lawyer. After an investigation, the resulting OPC recommendations echoed those made in the special report following the student loan hard drive loss.

Invasive security screening

While data breaches remained a key focus of 2013-2014, a key trend noted in Privacy Impact Assessments (PIAs) reviewed during the past year was that of some government institutions developing more invasive security screening techniques going beyond the existing security requirements of the federal government. In several cases, these enhanced screening standards involved collecting personal data from social media and other open sources.

For example, the Canada Revenue Agency (CRA) submitted a PIA for its "Reliability Status+" personnel security screening standard, which proposed a number of new, more intrusive screening measures including open social media content, law enforcement records checks, and a reliability questionnaire. After consulting with our Office, the Agency amended its program considerably (for more on this, see section 5).

In addition, the Canada Border Services Agency (CBSA) implemented its High Integrity Personnel Security Screening Standard (focused on in last year's Annual Report), which includes an "integrity interview" that collects a significant amount of personal information.

RCMP Review

One of the liveliest and most important public discussions around privacy in Canada for many years has been the lawful access debate. Seeking to advance it, our Office launched a review to determine whether the RCMP had appropriate controls in place to ensure its collection of subscriber information from companies without a warrant was in compliance with the *Privacy Act*.

In the end, we were disappointed to find that limitations in how the RCMP recorded this information meant we were unable to assess whether such controls were in place. It was impossible to determine how often the RCMP collected subscriber data without a warrant. Nor could we assess whether such requests were justified. The review is included in this report in section 4.

State surveillance

Over-shadowing all of the issues already described has been a much higher profile for the ongoing challenge in Canada and other democratic states about conserving the right of privacy of individuals in a digital era while also pursuing effective national security. Public concern has been heightened by revelations about state surveillance activities, especially among the so-called "Five Eyes," which is an intelligence alliance comprising Canada, Australia, New Zealand, the U.K. and the U.S.

The fallout from the revelations is examined in some additional detail in our Feature, found in section 3. In particular, we consider their impact on public expectations for greater transparency from security agencies about how they operate and use personal information within reason, given the sensitivity of their activities.

An OPC Special Report to Parliament in January 2014 entitled *Checks and Controls: Reinforcing Privacy Protection and Oversight for the Canadian Intelligence Community in an Era of Cyber-Surveillance* examined many of these issues. Introducing 10 detailed recommendations, the report stated:

> *The aim of renewal in this area should be to protect privacy in a complex threat environment; oversee collection so that it is reasonable, proportionate and minimally intrusive; ensure appropriate retention and access controls (among both public and private sectors); ensure accuracy of analysis; and control the scope of information requests and disclosures through specific safeguards, agreements and caveats.*

Looking ahead

In addition to issues involving privacy and national security, the OPC will also be closely watching developments on several other federal government privacy fronts. We have concerns about the potential adverse privacy impact of Bill C-13, the *Protecting Canadians from Online Crime Act*, which were detailed in my June 2014 appearance before the House of Commons Justice and Human Rights Committee (see section 5).

Just days afterwards, the Supreme Court of Canada ruled that there is indeed a reasonable expectation of privacy in Internet subscriber information (*R. v. Spencer*). The Court agreed that this information could, in many cases, be the key to unlocking sensitive details about a user's online activities and is therefore worthy of constitutional protection.

Our Office will be closely monitoring the progress of C-13 to see what impact our recommendations and the Supreme Court ruling will have on the government's approach. We will also be tracking data breaches in government departments and agencies to assess the impact of the new mandatory reporting rules.

Continuing emphasis on the border

In the coming year, the Canada-U.S. border will remain one of our key points of focus. The 2011 Beyond the Border Declaration and 2012 Perimeter Security Action Plan, committed the Government of Canada to a reinforced vision of continental security, while also making it easier for people and goods to cross the border.

Under the Action Plan, the continued roll-out of the entry/exit program means that the record of someone entering the U.S. from Canada by land will automatically become a record of their exit from our country. Until the initial phases of this program, which has already started collecting information about the exits of foreign nationals and temporary residents, Canada had previously not collected such information.

The CBSA justified the program's first phases by indicating it was necessary for immigration enforcement. In future phases, the program is planned to collect information about all Canadian and U.S. citizens crossing the border by any means. In its final phase, it will also capture exit information for all individuals leaving Canada by air to any destination. As the lead responsible for this program, CBSA now also proposes sharing exit records much more widely across government so they may potentially be used to ensure the integrity of social benefit programs, for taxation and general law enforcement and intelligence purposes.

As the details of these programs unfold, our Office expects the CBSA and any other department involved to submit PIAs for such proposed new uses of the personal information with evidence that any potential adverse impacts on privacy are being addressed accordingly (see section 5). We will also urge the government to be fully transparent about any intended uses of these records, including how they could be combined with other collected data.

In closing

Finally, as noted earlier, I was not Commissioner during the 2013-2014 period, and I wish to recognize the efforts and achievements of my predecessor, Jennifer Stoddart, who served as Commissioner for a decade rich with rising challenge and achievement. I also wish to recognize Chantal Bernier who acted as Commissioner upon Ms. Stoddart's departure and served as Assistant Commissioner from 2008 to 2013.

Under Ms. Stoddart's leadership, the Office had undertaken an exercise to identify strategic priority areas to guide its proactive work, which served the organization well for several years.

Even before I joined the Office, there was a plan in place to take another look and identify strategic priorities for the next few years.

We are currently embarking upon a priority-setting exercise to help ensure that we focus on the privacy issues that matter most to Canadians. As part of this initiative, we will be meeting with various stakeholders and groups to seek their input.

As I continue the first year of my term as Commissioner, I look forward to meeting Canadians' privacy priorities in an increasingly challenging environment. And thankfully, I do so with the support of a talented and knowledgeable team dedicated to protecting Canadians' privacy rights.

Daniel Therrien
Privacy Commissioner of Canada

Privacy by the Numbers – 2013-2014

Information requests received relating to PA	**2,147**
Complaints accepted (access, time limits, privacy)	**1,777**
Closed through early resolution investigations (access, time limits, privacy)	**345**
Closed through standard investigations (access, time limits, privacy)	**1,740**
PIA reviews reviewed as high risk	**65**
PIAs reviewed as lower risk	**36**
Public sector audits tabled	**2**
Public interest disclosures by federal organizations under section 8(2)(*m*)	**296**
Legislation affecting federal public sector reviewed for privacy implications	**8**
Public sector policies or initiatives reviewed for privacy implications	**35**

Parliamentary committee appearances on public sector matters	**5**
Formal briefs submitted	**4**
Other interactions with parliamentarians or staff (for example, correspondence with MPs or Senators)	**28**
Speeches and presentations delivered	**107**
Visits to main Office website	**2,080,099**
Visits to Office blogs and YouTube channel **Blog visits –** **YouTube visits –**	 **623,163** **21,842**
Tweets sent	**235**
Twitter followers as of March 31, 2014	**7,636**
Publications distributed	**5,709**
News releases and announcements issued	**25**

3

Feature

From surveillance revelations to a seminal Supreme Court of Canada ruling: 12 months of privacy at centre stage

Here we examine what was certainly the biggest privacy story of the past year in Canada, and focus on the genesis of one of the year's biggest stories internationally – of any kind, not just about privacy.

From June 2013 to June 2014, terms like "metadata" and "Five Eyes," previously found almost exclusively in blogs read by privacy technologists and policy experts, were vaulted into mainstream news headlines and leads. And while revelations about state surveillance provided an unprecedented view into the operations of intelligence agencies, they also raised and continue to raise important questions calling for greater transparency.

In all, June 2013 through June 2014 was a 12 month span that began with reports that seemed to suggest privacy might be hopelessly besieged and ended with the Supreme Court of Canada recognizing that a reasonable expectation of privacy applies to subscriber information like IP addresses. And there were many twists and turns in between.

Through it all, the importance Canadians place upon privacy protection proved unequivocal. At the same time however, no one should disregard the priority Canadians place upon the government protecting their security and safety.

In the end, it's not a question of "either, or" – it is possible to have both. And Canadians want greater transparency to see that these objectives are being sufficiently respected.

Looking back and assessing the impact

In June 2013, highly technical, classified details began emerging from documents supplied to news media outlets by Edward Snowden, a former contractor with the National Security Agency (NSA), the American signals intelligence organization.

In the following months, more releases exposed covert operations by the NSA to monitor the private communications of world leaders. They also revealed a vast capability to capture, store and analyze metadata on private communications and internet transactions – all with an aim to detailing where and when conversations or interactions took place between individuals anywhere in the world.

The revelations also uncloaked specific actions taken by the four other "Five Eyes" member countries – Australia, Canada, New Zealand and the U.K. – whose intelligence agencies collaborate and share information with their American counterparts.

For Canadians, details from documents were reported to reveal specific operations carried out by our domestic signals intelligence agency, the Communication Security Establishment Canada (CSEC). These ranged from monitoring world leaders' communications at the G20 Summit in Toronto to tracking individuals from an unnamed Canadian airport in 2009.

In the wake of revelations, media coverage and Parliamentary debate were intense and ongoing. During the second session of the 41st Parliament (October 16, 2013 to June 19, 2014), parliamentarians raised more than 50 questions about CSEC in the House of Commons and the Senate.

Focusing on intelligence activity oversight

As Parliamentary debate and headlines roiled, the intricacies of such surveillance came under scrutiny. One question, however, towered above the rest, the age-old "who watches the watchers?" And further, "how were parliamentarians and the Canadians they serve being informed about how this oversight is taking place and getting results?"

The challenge of intelligence activity oversight turned a spotlight on the work of CSEC's oversight body, the Office of the CSE Commissioner (OCSEC), and also on the Security Intelligence Review Committee (SIRC), which oversees the Canadian Security and Intelligence Service (CSIS).

In early December, the Senate Committee on National Security and Defence convened hearings about intelligence activity oversight, hearing initially from our Office, OCSEC and SIRC, and later from the heads of CSEC and CSIS, and the National Security Advisor to the Prime Minister.

On December 9, 2013, Interim Privacy Commissioner Chantal Bernier testified about

the privacy implications of information-sharing among Canada's intelligence agencies. She reminded the Committee that the heads of both OCSEC and SIRC had pointed out publicly their inability under the law to jointly review large-scale, ongoing information-sharing between members of the intelligence community.

This gap arose partly because, contrary to the agencies they oversee, these two oversight bodies face fairly rigid statutory and security limits on how they can work together.

In January 2014, a report by our Office was tabled in Parliament entitled, *Checks and Controls: Reinforcing Privacy Protection and Oversight for the Canadian Intelligence Community in an Era of Cyber-Surveillance.* Its general objective was to inform and encourage a greater public discussion of issues surrounding intelligence activity oversight and transparency. Among its recommendations was that the government address previous concerns expressed by oversight bodies with respect to their ability to conduct joint reviews.

The Senate Committee is expected to conclude its hearings and issue a report later in 2014.

Checks and Controls: Reinforcing Privacy Protection and Oversight for the Canadian Intelligence Community in an Era of Cyber-Surveillance : http://www.priv.gc.ca/information/sr-rs/201314/sr_cic_e.asp

Revealing the private-to-public-sector pathway

While the revelations about state surveillance gave ordinary citizens unprecedented glimpses into the largely opaque world of intelligence activities, they also brought to light something that hit closer to home for most. On June 5, 2013, these particular revelations began with a report about telecommunications service provider Verizon being legally compelled by the NSA to provide duplicates each day of all its subscribers' call logs, thus opening the public debate on metadata.

In the same week, news emerged about the NSA's PRISM program through documents which detailed the Agency's capacity to tap into data from major online service providers, including many where Canadians held email and social networking accounts.

Days later, in Canada, news surfaced about CSEC's own metadata program under which, *the Globe and Mail* reported, "CSEC 'incidentally' intercepts Canadian communications, but takes pain to purge or 'anonymize' such data after it is obtained."

These media reports added to the discussion about online privacy. In the months that followed, our Office commissioned an analysis to explore the legal status of metadata.

While security agencies on both sides of the 49th parallel maintain that collecting and analysing metadata en masse is not the same as scanning an individual's email or listening in on a conversation, at a minimum this log data details what time a communication was made, from what location and to whom. Collecting such data over a long period of time can begin to paint detailed portraits of the activities and

https://www.priv.gc.ca/metadata

social lives of individuals. For this reason, our analysis concludes that "[i]n many cases, courts have recognized that metadata can reveal much about an individual and it deserves privacy protection, all the while recognizing that context matters."

A metadata primer

In simple terms, metadata is data that provides information about other data. However, as an OPC technical and legal overview makes clear, there's much more to metadata than meets the eye.

Every time you make an electronic communication be it a phone call or an email, metadata is produced. For instance the simple act of sending an email can generate a dozen different pieces of metadata, ranging from the names and email addresses of the sender and the recipient to the message subject, priority and status.

The sender's IP address is also exposed and when this is linked to other basic telecommunications subscriber information, that can reveal someone's interests, ideological leanings, the people they associate with and where they travel. Indeed, as the OPC overview emphasizes, metadata can sometimes be more revealing than the actual content of a communication.

Of further concern is that metadata can be a great destroyer of anonymity. For example, using a metadata search engine, a newspaper reporter in Vancouver was able to compile a detailed profile of a 16-year-old female starting with only a randomly selected, geo-tagged tweet.

The OPC overview also chronicles a rapid evolution in how the courts have defined metadata, culminating in the judicial view that in many cases metadata may permit the drawing of inferences about an individual's conduct or activities. This potential privacy sensitivity and metadata's ubiquitous nature means it must be handled with care by both the private and public sectors.

Quantifying warrantless disclosures

In April 2014, a few months after the reports of metadata collection by the NSA and CSEC, privacy concerns were stoked further by the disclosure of how often Canadian telecommunications service providers turned over subscriber information to authorities, on simple request without a warrant. Aggregate data from telecom companies supplied to the OPC by a law firm acting on behalf of nine telecommunications carriers indicated that 1.2 million requests had been filed by investigators in 2011, an average of more than 3,200 a day.

In addition, our Office launched a review of the RCMP's warrantless access requests during the past year. The objective of the review was to determine whether the RCMP had implemented appropriate controls, including policies, procedures and processes, to ensure that its collection of subscriber data without a warrant was in compliance with sections 4 and 5 of the *Privacy Act*.

Furthermore, we were hoping to provide additional transparency by answering the following questions:

- How frequently does the RCMP collect subscriber data without a warrant?; and
- Did the RCMP have appropriate justification for its warrantless requests of subscriber data?

As the RCMP's information management systems were not designed to identify files which contained warrantless access requests to subscriber information, we were unable to select a representative sample of files to review. Consequently, we were unable to assess the sufficiency of controls that may exist or if the collection of warrantless requests from Telecommunications Service Providers (TSPs) was, or was not in compliance with the collection requirements of the *Privacy Act.*

In addition, we could not determine:

- How frequently the RCMP collects subscriber data without a warrant; or
- Whether the RCMP had appropriate justification under the *Privacy Act* to request subscriber data without a warrant.

Our Office therefore recommended that , in order to promote greater transparency surrounding warrantless requests for subscriber information made by the RCMP to Telecommunication Service Providers, the RCMP should implement a means to monitor and report on its collection of this information. While the review focused on the RCMP, the resulting recommendation is one that all federal institutions should follow.

The full text of the review can be found in section 4 of this report.

In the weeks following the reports of about the 1.2 million telecommunications requests, the House of Commons Standing Committee on Justice and Human Rights began hearings on Bill C-13, the latest federal attempt at "lawful access" legislation.

When Bill C-13 was initially introduced in November 2013, our Office noted that it did not contain the much-criticized provision of its predecessors to compel telecom companies to provide subscriber information to authorities upon request without a warrant. Bill C-13 did however raise other concerns including its relatively low threshold for obtaining a warrant in certain cases, and a new immunity clause that, as Privacy Commissioner Daniel Therrien explained in his June 10th appearance before Committee, "could lead to a rise in additional voluntary disclosures and informal requests."

Transparency builds trust

While testifying on Bill C-13, Commissioner Therrien also said, "Canadians expect that their service providers will keep their information confidential and that personal information will not be shared with government authorities without their express consent, clear lawful authority or a warrant."

The essence of privacy is the ability of individuals to control their own personal information. Essential to informing this ability is transparency, which formed a major part of the privacy discussions in the public sector during the past year.

Advocates on both sides of the debate ignited by the surveillance revelations agreed that, by and large, the data divulged were mere snapshots of activity and lacked the context of the bigger picture.

Being more open about their operations to the extent possible given the sensitivity of their activities, would allow national security and intelligence agencies to dispel Canadians' fears and gain their trust. Such efforts would help achieve the important objective of building Canadians' confidence in the conduct of their national security agencies. Doing so would also help these organizations meet citizens' expectations as forged by today's information age.

But, while recognizing that some secrecy will always be a necessary element of their activities, intelligence agencies have been slower in raising their levels of transparency.

In a letter to CSEC Chief John Foster, former Privacy Commissioner Jennifer Stoddart raised the importance of greater transparency, noting that "open and accountable government is a laudable goal in all contexts, critical for gaining and maintaining the trust of its citizens." In response, CSEC committed to getting its Personal Information Banks (descriptions of personal information held by federal organizations and retrievable for administrative purposes) online (which it did in 2013) and proceeded to expand the materials on its website, providing Canadians with more information about how the agency works.

Our January 2014 Special Report *Checks and Controls* called for further means of enhancing the transparency of intelligence activities carried out by Canadian federal institutions.

An international call for greater transparency

At the 35th International Conference of Data Protection and Privacy Commissioners, which took place in September 2013 in Warsaw, Poland, our Office joined other data protection authorities in agreeing upon and issuing a resolution calling for increased openness on the part of federal agencies.
http://www.priv.gc.ca/resource/int/conf_13_e.asp

Privacy spotlighted as never before and a seminal ruling

In retrospect, it's difficult to think of a year where privacy issues were as dominant in the media and Parliament as the one chronicled in this report.

Apart from the surveillance revelations themselves, our Office noted a general upswing in interest about privacy from the media, across the board. Media calls to our Office were up 40 percent from April 1, 2013 to March 31, 2014 compared to the same period a year before. And that increase came before the news about the 1.2 million access requests made to Canadian telecommunications companies, which generated unprecedented interest from reporters.

Just over a year after the surveillance revelations began, this intense 12-month period was capped by a seminal ruling from the Supreme Court upholding the right to personal privacy in *R v. Spencer*.

The Court ruled that there is indeed a reasonable expectation of privacy attached to information about telecom company subscribers when such information could be used to unlock sensitive details about an individual's online activities. And therefore, unlike simple phonebook information alone, a name and address when linked with an IP address is worthy of constitutional protection. On a practical level this means that, outside exigent circumstances or a reasonable law providing lawful authority, authorities need prior court authorization to obtain such information.

Our Office greeted this ruling with immense satisfaction, as it affirmed the sensitivity of subscriber information and recognized the escalation of risks to privacy which have dawned with the onset of the online age. It should also serve to provide clarity to law enforcement and telecommunications service providers to adjust their processes and practices accordingly.

Looking over the horizon

While the year featured revelations that some people found concerning and even disturbing from a privacy perspective, it was also 12 months where such concerns led to positive

Broader implications of *R v. Spencer*

Some key policy principles and privacy lessons reinforced by the Supreme Court's ruling include:

a) Lawful access and government searches cannot be regulated solely on the basis of the data viewed in isolation – what the gathered information can, in turn, reveal must also be considered as a critical factor [par.26, 30-33];

b) The invasiveness of a search must be determined by the potential impact upon the individual – not the illicit nature of the material sought or crime thwarted [par.18, 36];

c) Contemporary conceptions of informational privacy as protected by the *Charter* must include elements of secrecy, control and anonymity [par. 38];

d) Much of the information citizens exchange in both the real world and online is done with the specific understanding these ideas and opinions will not be recorded and linked specifically to them [par. 42-43, 45].

Since the ruling, many Canadian telecommunications providers have adopted new policies stating that they will only provide subscriber information to authorities when the requests have been authorized by the courts.

As well, in the wake of the surveillance revelations, many online service providers have begun offering annual transparency reports revealing how many requests they receive for subscriber information from authorities.

changes that gave the public and policymakers greater insight into how personal information may be collected by authorities.

Yet important questions still remain about how that information is used by authorities, calling for greater transparency not only from private sector companies, but also from public sector organizations. On that front as well, the year gone by may have provided an inkling of hope, as reflected in testimony by CSEC Chief John Forster to the Senate Committee on Defence and National Security in January 2014. Noting that CSEC had been "a well-hidden organization for tens and tens of years" Foster continued:

> *"One of the challenges I have, as the chief of that organization, is for us to be far more transparent and open as far as we can be within the confines of national security about what we do. We think that's important as another way of ensuring public trust and confidence in the work we're doing."*

A similar sentiment was voiced by former CSE Commissioner Robert Décary who, in his 2013 annual report, stated that "the greater the transparency, the less sceptical and cynical the public will be" about intelligence activities. The same position has been echoed by current CSE Commissioner Jean-Pierre Plouffe, who in his inaugural annual report stated that, "transparency is important to maintain public trust," and that "it is my goal to carry on my predecessor's work to be more informative and transparent about the activities of my office and of CSEC."

The closing months did indeed bring reasons to hope that the heightened public interest and discussion might lead to greater transparency and more security for personal information in the year ahead.

Looking forward, at the time of this report's writing, there is legislation before Parliament holding potentially significant impacts upon privacy in the form of the aforementioned Bill C-13. It contains measures that seek to ease the ability of organizations to comply with authorities when faced with requests seeking access to subscriber information.

As it stands, we are concerned that these proposed measures would lead to excessive disclosures that would be invisible to the individuals concerned and to our Office.

In preparing for future appearances before Committee examining this Bill, we are considering how to best advise parliamentarians on the significance of the Spencer decision and the importance of transparency for government in building and maintaining trust with citizens.

4 Review of the Royal Canadian Mounted Police – Warrantless Access to Subscriber Information

Section 37 of the *Privacy Act*

Introduction

For over a decade, the Government of Canada has been studying various proposals that would authorize specified government agencies to obtain personal information held by Telecommunication Service Providers (TSPs). Since 2005, these lawful access proposals have been set out in eight separate bills introduced by the Government of Canada. As of this writing (October 2014) Parliament is still considering legislation that would modernize police investigative techniques, but also have far-reaching implications for online privacy. As of this writing, Bill C-13, *An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act* (also known as the *Protecting Canadians from Online Crime Act*), is at the Report stage before the House of Commons.

Representatives of Canadian law enforcement agencies have been calling for new police powers to be codified in lawful access legislation for some time. They have stated that Internet use and evolving telecommunication infrastructures in Canada have created hurdles for investigations. As part of their mandated responsibilities, law enforcement agencies seek to identify criminal activity and those carrying out criminal activity online, in the context of a lawful investigation. As a result, law enforcement agencies may seek subscriber information for a wide range of criminal investigations, including child exploitation, drugs and organized crime, abducted persons, cyberbullying and financial crimes, or other public safety emergencies such as suicide threats or missing persons. The legal requirements for obtaining subscriber information may vary depending on the nature of the information sought. As well, the information requested varies, and may be limited to the name and address associated with a phone number, or includes the name associated with an Internet Protocol (IP) address.

Importance for Canadians

There is significant public interest concerning government surveillance and requests by law enforcement bodies to obtain subscriber information without prior judicial authorization.

Prior to the Supreme Court of Canada's decision in *R. v. Spencer*, many Telecommunications Service Providers released subscriber information in response to law enforcement requests without prior judicial oversight. Some of these requests involved information which could allow government agencies to access information that could be subsequently linked to personal information and other sensitive information, such as Internet usage.

The practice of law enforcement agencies seeking subscriber information without prior judicial authorization is not well understood by Canadians. Indeed, limited information is available about such requests, including the frequency with which they were made, and what information was sought.

It was in this context that our office decided to review the Royal Canadian Mounted Police (RCMP) in order to provide greater clarity regarding the practice of obtaining subscriber information from Telecommunications Service Providers (TSPs) without a warrant.

About the RCMP

The RCMP operates under the authority of the *RCMP Act*. A Commissioner heads the organization under the direction of the Minister of Public Safety Canada. The RCMP is the largest police force in Canada. It has a broad mandate which covers international and domestic roles.

The RCMP enforces federal laws across the country, and provincial/territorial laws in all provinces and territories - excluding Ontario and Quebec. The RCMP also provides investigative, operational and technical support services to more than 500 Canadian law enforcement and criminal justice agencies.

The RCMP operates in approximately 150 municipalities, 600 aboriginal communities and at three international airports. The RCMP has approximately 29,000 employees, including regular and civilian members, and public service personnel both in Canada and abroad.

In the course of carrying out its mandate, the RCMP gathers various data and requests information from a wide variety of individuals, as well as from public and private sector sources. More specific to our review, the RCMP, in the course of law enforcement investigations, may make requests to TSPs without a warrant to obtain subscriber information.

Background

On October 24, 2013, the Privacy Commissioner issued a notice of review to the RCMP Commissioner under section 37 of the *Privacy Act*. The notice indicated that we would conduct preliminary work that may lead to an audit of the RCMP's collection of subscriber data without a warrant from TSPs.

Objective

The objective of the review was to determine whether the RCMP had implemented appropriate controls, including policies, procedures and processes, to ensure that its collection of subscriber data without a warrant was in compliance with sections 4 and 5 of the *Privacy Act*.

Furthermore, we were hoping to provide additional transparency by answering the following questions:

- How frequently does the RCMP collect subscriber data without a warrant?; and
- Did the RCMP have appropriate justification under the *Privacy Act* for its warrantless requests of subscriber data?

Given the federal government's statements and commitments to openness and transparency, we expected to find that the RCMP's records would enable reporting on the above questions.

Observations

The *Privacy Act* restricts the collection of personal information by federal entities to that which is related to an operating program or activity. During our review, we wanted to assess whether the RCMP's warrantless access requests to Telecommunication Service Providers (TSPs) for subscriber information were made in keeping with the above requirement.

During the course of our review work we interviewed over 50 individuals. These included senior RCMP officials, field officers who have made warrantless requests for subscriber information, and information technology specialists who are in charge of managing and extracting information from the RCMP's investigative databases. We also interviewed specialists from the telecommunications industry familiar with these types of requests. As well, we reviewed the RCMP's policy related to the recording of law enforcement activities in their investigative databases.

This policy requires that the collection and use of operational information is subject to the provisions of the *Privacy Act*. Although RCMP policies do not specifically address the practice of requesting subscriber information from TSPs without a warrant, they do apply to the full range of RCMP operational activities, which would include this type of collection.

The RCMP informed us that its primary record management system receives approximately two million new incident entries every year. We undertook searches of this system, and in only limited instances were we able to identify a link between requests made for warrantless access to subscriber information and the files that contained such requests. We found that other than through a manual review of each case file, the RCMP does not currently have the capacity to produce a report that would identify some or all of the particular operational files in which an access to subscriber information was made without a warrant, and report on the frequency of such requests. The RCMP stated that its records management system was not designed for this purpose.

The RCMP indicated that its records management system for operational case files was designed to support investigations and to respond to legislative requirements to report certain crime statistics to Statistics Canada. The RCMP further explained that the systems were not designed to be able to report on all the instances, in the aggregate, where requests for subscriber information without a warrant were made. The RCMP also stated that compiling such information is complicated by the fact that a complex criminal case may involve numerous warrantless requests for customer names and addresses related to phone numbers. In addition, the method and type of information requested varies depending on the nature of the case, and the requirements of the TSP.

The only area where we were able to review files containing warrantless access requests for subscriber data was at the RCMP's National Child Exploitation Coordination Centre (NCECC). However, the NCECC requests only represent a subset of all warrantless requests for subscriber information made by the RCMP. Our review of NCECC files indicated that the warrantless access requests for subscriber data were linked to ongoing investigations. However, we are unable to extrapolate these results beyond these files to areas other than the NCECC.

The RCMP itself recognized the merit in capturing statistical information on warrantless requests for subscriber data. On January 12, 2010 the Assistant Commissioner for Technical Operations issued a memorandum instructing that front line officers begin reporting warrantless requests for subscriber information to TSPs. This memorandum was issued to support the possible reintroduction of Bill C-47, *Technical Assistance for Law Enforcement in the 21st Century Act*.

The RCMP stated that as Bill C-47 did not progress beyond the second reading stage in Parliament, this data collection was never fully operationalized. However, the memorandum noted that at the time it was issued, Bill C-47 had been at the second reading stage before Parliament and had already died on the order paper as Parliament had prorogued in December 2009. Our reading of the

memorandum, and its timing, suggest that the purpose of the request for officers to compile statistics on requests for subscriber information was to gather information to demonstrate the need for lawful access legislation generally, which was eventually reintroduced in November 2010 as Bill C-52, *Investigating and Regulating Criminal Electronic Communications Act* and thereafter as Bill C-30, *An Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and other Acts*, in February 2012.

On June 13, 2014, the Supreme Court of Canada released its decision in *R. v. Spencer*; that decision had a direct impact on our ongoing review activities. In that case, a unanimous Court held that there was a reasonable expectation of privacy under section 8 of the Charter with respect to subscriber information that could link an individual to his or her online activities. The Court concluded that, in that case, the information was unconstitutionally obtained since police did not have any lawful authority to obtain such information in the absence of exigent circumstances or a reasonable law. The RCMP has indicated that it has adjusted its investigative efforts to align them with the *Spencer* decision. Given that the RCMP's primary records management system was not designed to identify warrantless access requests, and the impact that the Supreme Court of Canada's ruling (*R. v. Spencer*) now has on the RCMP's ability to collect subscriber data without a warrant, we decided against proceeding with the review.

Ultimately, our efforts to review files, combined with our interviews with RCMP personnel, did not allow us to determine whether the RCMP, as a whole, was compliant, or non-compliant, with the provisions of the *Privacy Act* with respect to the collection of subscriber information without a warrant. Moreover, other than through a manual review of all case files stored, the RCMP does not have a means to demonstrate its compliance in this regard.

Recommendation: *In order to promote greater transparency surrounding warrantless requests for subscriber information made by the RCMP to Telecommunication Service Providers, the RCMP should implement a means to monitor and report on its collection of this information.*

RCMP Response

The RCMP's primary responsibilities are to preserve the peace, prevent crime and investigate offences against the laws of Canada. In executing its mandate, the RCMP is fully committed to respecting the laws of Canada, including the Privacy Act. The RCMP's records management systems were designed to meet investigative and evidentiary standards and not for the

purpose of reporting aggregate data on the origins of information collected during the course of its investigations. Notwithstanding, to ensure adherence and compliance with the laws of Canada, the RCMP maintains an extensive suite of operational policies, practices and standards.

While it is anticipated that the number of warrantless requests will be reduced in light of the *R. v. Spencer* decision, warrantless access will continue to be sought in specific situations, such as exigent circumstances or where authorized by a reasonable law. The RCMP will establish a working group to explore mechanisms which are both efficient and cost-effective to better monitor and report on warrantless requests for subscriber information. A report in this regard will be presented to our Departmental Audit Committee by April 2015.

Additionally, as a result of the *R. v. Spencer* decision, the Department of Justice and the Public Prosecution Service of Canada are working with the interdepartmental community to examine the decision and its implications. The RCMP will fully comply with all new requirements as the implications of the decision are further determined.

Conclusion

Through our review we had intended to inform Parliament and Canadians about the RCMP's use of warrantless access requests to Telecommunication Service Providers (TSPs) for customer data.

As the RCMP's information management systems were not designed to identify files which contained warrantless access requests to subscriber information, we were unable to select a representative sample of files to review. Consequently, we were unable to assess the sufficiency of controls that may exist or if the collection of warrantless requests from TSPs was, or was not in compliance with the collection requirements of the *Privacy Act*.

In addition, we could not determine:

- How frequently the RCMP collects subscriber data without a warrant; or
- Whether the RCMP had appropriate justification under the *Privacy Act* to request subscriber data without a warrant.

Keeping accurate records of warrantless requests for subscriber information is consistent with the Government of Canada's commitment to transparency. Furthermore, accurate record keeping could provide the necessary evidence to justify the need to implement lawful access related legislation.

ABOUT THE REVIEW

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

Objective
The objective of the review was to determine whether the RCMP had implemented appropriate controls, including policies, procedures and processes, to ensure that its warrantless collection of subscriber data was in compliance with sections 4 and 5 of the *Privacy Act*.

Criteria
Review criteria were derived from the *Privacy Act* and Treasury Board Secretariat policies, directives and standards related to the management of personal information.

We expected to find that the RCMP has:

- Policies, practices and procedures to ensure that warrantless access requests made to Telecommunication Service Providers (TSPs) only collect personal information that is related to operating programs; and

- Consistently documented its warrantless access requests to TSPs, further to the Government of Canada's commitment to openness and transparency.

Scope and approach
Examination activities were conducted at the RCMP's headquarters in Ottawa and with selected RCMP officials across the country.

The review examined policies, practices procedures and electronic files about warrantless access requests. Evidence was also obtained from the examination of records, interviews with 52 officials, demonstrations of systems and other review tests.

The review did not include a review of requests made: with a warrant, using mutual legal assistance treaties (MLAT's), for telephone numbers, or to sites that provide internet search services.

The review commenced on October 24, 2013 and was halted in June 2014 in light of the Supreme Court of Canada's decision in *R. v. Spencer*.

Standards
The review was conducted in accordance with the legislative mandate, policies and practices of the Office of the Privacy Commissioner of Canada.

Review team
Steven Morgan
Tom Fitzpatrick
Sylvie Gallo Daccash
Ivan Villafan

5 The Year in Review

PRIVACY IMPACT ASSESSMENTS

Privacy Impact Assessments (PIAs) are used to identify the potential privacy risks of new or redesigned federal government programs or services. They are meant to eliminate or reduce those risks to an acceptable level.

PIAs take a close look at how federal government institutions protect personal information as it is collected, used, disclosed, stored and ultimately destroyed. These assessments help create a privacy-sensitive culture in government departments. It is important they are prepared well in advance of a new initiative (or changes to an existing one) being implemented in order to address privacy risks early and up front. Organizations that make PIAs a priority stand to benefit by lessening the possibility of adverse events, such as data breaches, while demonstrating an active commitment to transparency and respect for the privacy of Canadians.

According to the Treasury Board Secretariat *Privacy Impact Assessment Directive,* 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 effectively mitigated. Our Office receives copies of these assessments for review, and, when appropriate, we give institutions advice and recommendations for improving their personal information-handling practices. While most institutions accept and follow our advice, our recommendations are non-binding.

Border crossing information

PIAs reviewed by the OPC over the past fiscal year indicate a trend towards an increased collection of personal information at borders and an expansion of the sharing and uses of such information. A large part of this increased surveillance stems from the Entry/Exit initiative, which is one of a number of initiatives that have been developed under the Canada-U.S. Beyond the Border perimeter security agreement. The collection of exit information at land borders is based on an exchange between Canada and the U.S., so that a record of entry into one country becomes a record of exit from the other. Information on individuals exiting Canada has not previously been routinely collected by our government.

Phases I and II of Entry/Exit involved the exchange of entry information between Canada and the U.S. of third country nationals and permanent residents crossing land borders. Upon reviewing the PIA for Phase II, our Office learned that the CBSA planned to retain the personal information collected under the Entry/Exit program for 75 years. We asked the CBSA to provide a justification for the planned retention period. In response to our recommendation, the CBSA reduced the retention period to 30 years, with depersonalization occurring after the first 15 years. However, we have requested and await a justification for the necessity to retain the information for this time period and have asked all other institutions that will also collect this information to justify retention periods.

Should the program move forward, Phase III will expand the surveillance to Canadian and U.S. citizens crossing by land, while Phase IV will include the collection of exit records for all travellers leaving Canada by air. Commercial air carriers will be required by law to give CBSA passenger manifests for outbound flights. It is our understanding that new legislation will need to be passed in Parliament, and regulatory changes will be required for this contemplated expansion.

The CBSA justified the initial phases of the program as necessary for border integrity and immigration enforcement, indicating that enforcement and removal efforts for individuals who overstayed their visa limits would be better focused if the Agency had more information on who had left.

Plans for the next phases of the Entry/Exit program contemplate not only collecting exit data from all travellers, but using that personal information for wider purposes. These include use by law enforcement agencies, Citizenship and Immigration Canada (CIC) for validating residency requirements, and Employment and Social Development Canada for determining employment insurance eligibility. Exit records may also be shared with other government departments, such as the RCMP, the Canadian Security and Intelligence Service (CSIS), and the Canada Revenue Agency. In 2014-2015, the OPC expects to receive specific PIAs for proposed new uses of personal information from the Entry/Exit program. We have recommended that each of these expanded uses be demonstrated as necessary and effective, be undertaken in the least privacy-invasive manner possible and be designed so any loss of privacy is in proportion to a substantial societal benefit.

Our Office continues to meet with officials from CBSA and other departments, and expects more detailed PIAs to come in early 2015.

Cross-border biometrics

Another government initiative raising many of the same privacy concerns is the Temporary Resident Biometrics Project (TRBP), managed jointly by CIC, the CBSA, and the RCMP. Beginning in 2013, citizens from 29 countries

and one territory who apply to visit, study or work in Canada have been required to give their fingerprints and have their photographs taken as part of their visa application.

The TRBP was first presented to our Office as a way to screen applicants for admissibility, confirm their identities during the application process, and verify identities of visa holders when they entered Canada. On that basis, the government demonstrated that such verification was an appropriate use of biometrics and involved minimal privacy risks, so long as appropriate safeguards were used.

However, the project was expanded to allow the RCMP to retain fingerprints and other information collected during the application process for 15 years. These could then be matched against entries in the RCMP's criminal fingerprint database and latent prints lifted from crime scenes.

CIC indicated that visa applicants consent to this use on their application forms. In our continuing work on the PIAs for this project, our Office expressed concerns about whether visa applicants are fully informed of the potential uses of their fingerprints. We also questioned whether the lengthy and uniform retention of fingerprints of individuals not charged with, or convicted of, any criminal offence is justifiable. We recommended that CIC carefully review its consent mechanisms and retention periods.

CIC responded by saying that if a government institution possesses personal information that could identify a person of interest to law enforcement, it should disclose this information. We advised that this is a broad interpretation of acceptable disclosures and that the *Privacy Act* sets specific restrictions on the circumstances under which personal information collected by a government institution may be released to law enforcement. We continue to consult with the involved departments on this initiative.

Canada Revenue Agency security screening

Judging from PIAs reviewed over the past year, there appears to be a trend across government toward more intrusive security screening with regard to government employment. This can include the collection of personal information from social media and "integrity checks," which may include intrusive questions to potential employees about subjects, such as gambling, personal finances, relationships, and drug and alcohol use. These screening measures are in addition to the federal government's existing security requirements.

One example is the Canada Revenue Agency's (CRA) "Reliability Status+" screening process. This enhanced screening applies to an estimated 300 positions said to require a high degree of trust and decision-making power. The process proposed in the PIA included fingerprinting, credit checks, Law Enforcement Records Checks (more extensive

than a criminal records check), tax compliance verification, open source verifications, including social media information, and the completion of an intrusive Reliability Questionnaire.

Our review of the PIA identified risks to privacy posed by the addition of numerous privacy intrusive checks, particularly the questionnaire which contained questions of a broad nature that could lead to over-collection of personal information.

After our consultations, the CRA revised or removed some of the more invasive parts of the screening process and dropped the questionnaire altogether.

Social Security Tribunal

Last year, the Government changed and amalgamated the tribunal system for hearing appeals of Employment Insurance, Canada Pension Plan and Old Age Security decisions, without fully weighing the privacy and security implications to the personal information of thousands of Canadians.

In the past, a board of more than 1,000 part-time referees heard the appeals in three-person panels working from government offices. Under the new system, 74 full-time members of a Social Services Tribunal rule on the appeals by teleworking from home offices.

The OPC received a PIA from Employment and Social Development Canada only after the new tribunal began operating in April 2013. Many of the policies and procedures for safeguarding the personal information of appellants were still under development, including safeguards for teleworking and security assessments of tribunal members' home offices. When this report was being prepared in early September 2014, our Office had still not received the results of these assessments, which are key to addressing any privacy risks.

DATA BREACHES

For the third consecutive reporting period, the number of data breaches voluntarily reported to the OPC by departments and agencies reached a record high.

Any loss or unauthorized disclosure of personal information constitutes a data breach. Sometimes the affected individuals didn't know about the breach; in other cases people were officially told or found out through media reports.

Yet, as noted in previous annual reports, we don't know whether there have really been more data breaches in the year under review, or whether institutions have been more assiduous in reporting them. Such uncertainty should dissipate substantially in the future thanks to the May 2014 updates to the *Directive on Privacy Practices* from the Treasury Board Secretariat (TBS) requiring federal institutions

to report all material data breaches to our Office and TBS.

Our Office also worked closely with TBS to provide guidance about what amounts to a "material breach." At the time of this report's writing, institutions showed that they are still undergoing some growing pains in getting used to the new Directive. Since the Directive's coming into effect, it appears that more breaches are being reported to our Office than to TBS, when in fact each incident should be reported to both of our organizations.

Tips for federal institutions using portable storage devices
https://www.priv.gc.ca/media/nr-c/2014/nr-c_140325_e.asp

A four-page OPC tipsheet on using portable storage devices provides employees in federal departments and agencies with checklists about the four kinds of controls that provide protection against data breaches – physical, technical, administrative and personnel security.

Physical controls, for example, stress the importance of protecting devices not in use by placing them in locked cabinets or in storage areas where access is restricted. Technological controls would include encryption or strong passwords, with training for employees in each.

Under administrative controls, the tipsheet recommends assigning serial numbers to devices so they can be tracked and using portable storage devices to store personal information only as a last resort.

Personnel security controls encompass regular mandatory training about security and privacy, and monitoring the use of personal storage devices by employees to ensure policies and procedures are being followed.

Looking back at 2013-2014 when voluntary reporting prevailed, the OPC received reports of 228 data breaches across the federal government, more than double the 109 from the previous fiscal year. Accidental disclosure (i.e. human error) accounted for just over two-thirds of those breaches.

One particularly enormous data breach was the 2012 loss from Employment and Social Development Canada of an external hard drive containing the personal information of 583,000 student loan recipients.

A special OPC investigative report tabled in Parliament in March 2014 detailed how the hard drive was left unsecured for extended periods of time, not password protected and held unencrypted personal information. Arising out of the investigation, the OPC produced tips for federal institutions on the use of portable storage devices.

No organization is immune from the possibility of a data breach. Even our Office has experienced this type of event, with the loss of a hard drive containing employee information that went missing when we moved our head office from Ontario to Quebec. It is expected that the Privacy Commissioner, Ad Hoc will reference this event in his contribution to our 2014-2015 annual report on the *Privacy Act*.

PARLIAMENT

As an Agent of Parliament, our Office values opportunities to advise parliamentarians on the privacy implications of legislation and the issues they study. The year under review included many important discussions.

Bill C-13: a new iteration of "lawful access"

Vigorous and prolonged debate followed the introduction in November 2013 of Bill C-13, the *Protecting Canadians from Online Crime Act.*

Some critics characterized the legislation as a Trojan horse. Drafted in the wake of widely publicized suicides by young girls who had been subjected to cyberbullying, Bill C-13 would make it illegal to distribute intimate images without consent and remove barriers to getting such pictures scrubbed from the Internet.

However, the proposed legislation would also give police and other authorities new tools to preserve records of computer use and electronic emissions, track and trace various online activities of suspects, make it easier to get court approval for electronic surveillance and expand lawful access for a wider range of investigating agencies.

Following its November 2013 tabling, our Office carried out an extensive analysis of Bill C-13 leading up to the June 10, 2014 appearance of Commissioner Daniel Therrien before the House of Commons Justice and Human Rights Committee.

In his statement, the Commissioner recommended splitting the Bill, with cyberbullying going to Parliament for quick action while allowing for a focused and targeted review of the lawful access provisions. He summarized the OPC's four main concerns:

- Lowering the threshold for state access to electronic personal information from the existing "reasonable and probable grounds" of illegality to only "reasonable suspicion" of illegality;
- Extending the authorities who could use the new surveillance powers beyond police officers to include an ill-defined category of "public officers" such as mayors, reeves, fisheries officers, customs officers and any federal or provincial officer;
- Guaranteeing legal immunity to an individual or organization that voluntarily provides information to an investigator without court authorization; and
- The absence of any transparency regime requiring regular reporting on the use of any of the new powers.

A transcript of the Commissioner's remarks and a further detailed written submission can be found on our website.

Bill C-13 – Commissioner's opening statement: https://www.priv.gc.ca/parl/2014/parl_20140610_e.asp

Submission to Committee: https://www.priv.gc.ca/parl/2014/parl_sub_140609_e.asp

The Committee reported to the Commons on Bill C-13 on June 13; no further action was taken before the summer recess.

Seeking salary figures

The OPC has long been a strong proponent of open government as a means to enhance transparency and accountability commensurate with the protection of personal privacy. On June 5, 2013, then-Commissioner Jennifer Stoddart reinforced this view in an appearance before the Commons Committee on Access to Information, Privacy and Ethics.

The committee was considering Bill C-461, the *CBC and Public Service Disclosure and Accountability Act*, a private member's bill.

The legislation would have amended the *Privacy Act* to make the salaries of the top-paid federal public servants "non personal" so they could be released under an *Access to Information Act* request. It would also have done the same for the salary ranges of all other public servants and for the details of expenses reimbursed to any federal employee.

After reviewing current practices in the public service, provincial governments and the private sector, Commissioner Stoddart told the committee that "the disclosure of the salaries of the most senior officials in the federal public sector does not represent a significant privacy risk relative to the goal of transparency and the broader public interest."

She added that disclosing salary ranges and expense reimbursements also had no serious privacy implications and is something the OPC would readily do in response to an access request.

Bill C-416 died on the Commons order paper in February 2014.

Agents of Parliament combine efforts

The importance of enhancing transparency and accountability to Parliament and Canadians also figured into written comments by Interim Commissioner Chantal Bernier and the six other designated Agents of Parliament, such as the Auditor General and the Commissioner of Official Languages.

These seven individuals, all appointed by Parliament, were commenting on a private member's bill, C-520, the *Supporting Non-Partisan Agents of Parliament Act.*

Among other provisions, the proposed legislation would require that people being considered for jobs in the offices of Agents of Parliament disclose their political affiliations and activities for the last 10 years.

The Bill also states that an Agent, such as the Privacy Commissioner, must examine a written allegation from an MP or Senator that an employee of an Agent's office has been partisan in the performance of their responsibilities. The Agent would be legally obliged to submit a written report to the Senate and Commons speakers.

Letter from Agents of Parliament on Bill C-520: http://www.oic-ci.gc.ca/eng/activites-parlementaires-autres-documents-2014-other-parliamentary-documents_1.aspx

In a written submission to the House of Commons Standing Committee on Access to Information, Privacy and Ethics, the seven Agents, while supporting the general principles of accountability and impartiality, criticized Bill C-520 as being overly broad, vague and conflicting with existing laws covering public service employment.

The Committee reported to the Commons on Bill C-520 on May 26 with amendments; no further action was taken before the summer recess.

PRIVACY COMPLIANCE AUDITS

Under the *Privacy Act*, the Commissioner may audit the relevant privacy practices of federal departments and agencies and recommend remedial actions when needed. Although the *Act* provides no enforcement powers, the Commissioner may publish the findings and recommendations.

The OPC typically follows up with audited institutions two years later, asking what actions they have taken to address our recommendations. In 2013-2014, we launched two new audits and followed up on two others.

Follow-ups: In 2011 we audited two RCMP databases: one stores information on crimes and criminals, which can be retrieved by police agencies across Canada; the other is the primary operational records management system for the RCMP. Details of our audit and recommendations can be found on our website.

2011 - Audit of Selected RCMP Operational Databases: https://www.priv.gc.ca/information/pub/ar-vr/ar-vr_rcmp_2011_e.asp

The RCMP reported that four of our six recommendations had been fully implemented and the other two substantially so. For example, to deal with personal information being kept longer than necessary in the records management system, the RCMP informed us that it purged the backlog of all outstanding records and now erases files daily as required. The RCMP also reported that all police agencies, except for those in Quebec, where provincial legislation prevents individual police services from entering into an agreement with a federal agency, have now signed formal memoranda of understanding, which include provisions for privacy protection of personal information from the crime and criminals database.

In 2011, we also reviewed privacy policies and practices at the Canadian Air Transport Security Authority (CATSA), an organization familiar to all air travellers. Details are available on our website.

2011 - Privacy and Aviation Security: An Examination of the Canadian Air Transport Security Authority: https://www.priv.gc.ca/information/pub/ar-vr/ar-vr_catsa_2011_e.asp

2013 – Audit of CRA: https://www.priv.gc.ca/information/pub/ar-vr/ar-vr_cra_2013_e.asp

CATSA reported that 10 of our 12 recommendations have been fully implemented and the other two substantially so. These include:

- No longer telling police if CATSA finds domestic travellers carrying large sums of money;
- Developing a pamphlet to explain its collection, use, disclosure, retention and disposal of personal information related to boarding passes; and
- Introducing new software in 2013-2014 that shows a stick figure of someone subjected to a full-body scan instead of an outline.

2013 – Audit of FINTRAC: https://www.priv.gc.ca/information/pub/ar-vr/ar-vr_fintrac_2013_e.asp

New: Although portable storage devices, such as USB keys and external hard drives, can provide flexibility and convenience, they can also present inherent security and privacy risks, as government departments, such as Employment and Social Development Canada have discovered.

To obtain a better understanding on the use of portable storage devices within federal institutions, the OPC conducted a survey of departments and agencies and selected 17 for further examination in a cross-government audit. The audit will gauge whether these institutions have established and implemented policies, procedures and adequate controls to protect personal information stored on portable storage devices. We aim to complete the audit in 2014-2015.

Our Office also launched a review of RCMP requests without a judicial warrant to telecom and Internet companies for basic subscriber information. This work and its outcome are detailed in section 4 of this report.

Presented: During 2013-2014, the OPC also published our formal audits of the Canada Revenue Agency and the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), both of which were featured in last year's annual report.

INVESTIGATIONS

A close look at the numbers show that the Office of the Privacy Commissioner continued to profit from measures introduced in previous years to increase efficiency in processing complaints. Against the ongoing challenge of a growing volume of complaints and their increasing complexity, the Office continued to see improvements in treatment times.

The Office accepted 1,777 complaints under the *Privacy Act* during 2013-2014. This was significantly lower than the previous year. The number for the previous year however was unusually high, because over 1,200 complaints were received in relation to two major data breaches at Employment and Social Development Canada (ESDC). Excluding complaints associated with those two breaches,

this leaves a year-over-year increase of approximately 700 complaints in 2013-2014.

On the surface, average treatment times for complaints came to 10.9 months for 2013-2014. Removing the number of ESDC-related breach complaints from the comparisons however shows that average treatment times improved from 8.9 months in the previous year to 8.1 in 2013-2014.

This represents a marked improvement from five years ago in 2008-2009 when the average was 19.47 months. Year over year, trends indicate that complaints are growing in both their volume and complexity. Against this backdrop, average treatment times have generally and steadily continued to improve, thanks to a series of efforts to redistribute internal resources, and improve and modernize processes.

For example, the early resolution investigation process accounted for 345 of our closed files, compared to 299 in 2012-2013. In addition to handling more complaints through such negotiation and conciliation this year, our Office successfully reduced the average treatment time for early resolution cases by four days (from 2.25 months to 2.11 months as shown in the detailed tables found in Appendix 2).

Here are five particularly interesting investigations.

Lost USB key from Employment and Social Development Canada reinforces lessons learned

An earlier investigation into a data breach involving ESDC was featured in an OPC special report tabled in Parliament on March 25, 2014, which noted that the organization did not translate its formal privacy and security policies for the protection of personal information into meaningful business practices.

The OPC investigation concluded that this was a major contributing factor resulting in the loss of a hard drive, which was noticed missing on November 5, 2012. The drive contained the personal information of 583,000 student loan recipients.

That same month, a USB key containing the personal information of 5,045 Canada Pension Plan Disability appellants disappeared from a desk in an ESDC office. As with the hard drive, the USB key was neither password-protected nor encrypted, nor was it ever found.

The missing personal information included each individual's SIN, date of birth, surname, medical conditions, date of birth, education level, type of occupation and whether other payments were being received, such as worker's compensation. In the wrong hands, such information could lead to identity theft or fraud.

An OPC investigation into the disappearance of the USB key found weaknesses in the same four types of privacy management controls considered in the student loan hard drive case; namely physical, technological, administrative and personnel controls.

This disappearance differed from the student loan hard drive case because a Justice Canada lawyer had custody of the USB key when it went missing. The lawyer was working from an office at ESDC to help triage the disability pension appeal cases pending a hearing before the former Review Tribunal. The lawyer had left the USB key lying on a desk in a locked office instead of storing it in a security cabinet.

More generally, our investigation found that the Justice department also failed to translate its security and privacy policies into meaningful business practices.

Both ESDC and Justice accepted OPC's nine recommendations to better protect personal information under their control. Most of the recommendations echo those made in the hard drive case.

Wanted by the CBSA Program

In a complaint to our Office, the Canadian Council for Refugees alleged that the personal information of an individual had been improperly disclosed on the Canada Border Service Agency's (CBSA) website. This disclosure occurred under the "Wanted by the CBSA" program, aimed at enlisting help from the public in finding individuals who were the subjects of active, Canada-wide warrants for removal. The man was one of 30 people described as being "accused of, or complicit in, war crimes or crimes against humanity."

The program website included names, dates of birth and photographs for all 30 individuals. Despite the personal information involved in the program, the CBSA failed to carry out a Privacy Impact Assessment before its launch. This failure posed serious privacy risks, since the potential consequences for individuals listed could be severe.

The OPC investigation found that the disclosure of the man's personal information was permissible under the *Privacy Act* because the purpose for the disclosure was in line with the administration and enforcement of immigration law and therefore a consistent use under the *Act.*

The Agency, however, failed to take all reasonable steps to ensure that the personal information was as accurate, up-to-date and complete as possible, as also required by the *Privacy Act*. For example, in this case, the individual was not convicted of war crimes under criminal law, but rather was determined inadmissible under Canada's immigration law for being an official in an unidentified government suspected of being engaged in war crimes.

Consequently, this one aspect of the complaint was considered well founded.

As a result of our investigation the CBSA accepted our five recommendations in full.

It undertook to:

- revisit the amount of personal information disclosed under the Program, including removing all personal information, except for an individual's picture, name and status, upon being located or removed from Canada. While our investigation concluded that disclosing personal information was necessary to achieve the program's objective, we were not satisfied that the CBSA was adequately limiting the amount of such data needed for that purpose. For example, CBSA did not provide justification for conveying an individuals' full date of birth;

- in future notification letters to our Office under subsection 8(5), demonstrate how the public interest in disclosure clearly outweighs any invasion of privacy that could result from disclosure in a particular case, as well as indicating what information will be disclosed, how it will be disclosed, and for how long it will be publicly available;

- make clear on the website the difference between a conviction under criminal law and a determination under immigration law;

- better enforce its practice of removing profiles from the website within 30 days of an individual's apprehension or removal from Canada, unlike the individual's profile in this case which was still posted for at least six months after his apprehension; and

- revise the relevant personal information bank to explicitly account for the Program's consistent uses of personal information.

The CBSA has since advised our Office that it is in the planning phase and a target PIA-completion date is to be determined in the fall of 2014.

Woman fails in attempt to return personal information to Canada Revenue Agency

When a B.C. woman tried to return another taxpayers' personal information that was mistakenly sent to her, the Canada Revenue Agency (CRA) only took action after the matter was brought to the media.

The story began when a woman asked the CRA in late March 2013 for information needed to complete the tax return of her deceased daughter. About eight weeks later she received a thick package from the Surrey Tax Centre.

Her daughter's requested information slips were inside, but so was the confidential personal information of five other strangers. Included were names, income and benefits, SINs, date of birth, marital status, employment details, etc.

In an interview with CBC, the woman explained that she had tried several times to report the data breach by telephoning the main CRA toll-free number but could not get through. (The CRA says that the "service target for caller accessibility on the general inquiries line" is 85 per cent, meaning that the Agency accepts that one in seven callers would not be answered).

She then tried to deliver the confidential records in person by driving to the tax centre in Surrey. The centre wasn't open to the public however, and a security guard suggested she put the unsealed, unlabelled package of confidential personal information in a drop box outside the building.

Rejecting that idea as unsuitable, she again phoned the main CRA number from her car. She was told she could either seal the information in another envelope marked with the appropriate security designation and place it in the drop box or wait 10 days for the CRA to send her a specially-labelled envelope.

Not satisfied with the choices, the woman suggested she personally hand over the information to someone from the tax centre, but was told this was not possible.

Following this, she got in touch with a CBC news reporter who contacted the CRA. The next day an employee from the B.C. tax office picked up the taxpayers' records at her home.

A report from the CRA confirmed the key details of the incident. Upon learning about this situation, our Office launched a Commissioner-initiated complaint. Our investigation concluded that the privacy rights of the taxpayers had been breached by the CRA and therefore the complaint was well founded.

The CRA promised remedial measures to reduce the chance of similar incidents, including by offering to courier pre-stamped envelopes.

The Agency has now improved its internal procedures regarding client service and misdirected mail. While we are satisfied with the measures taken, we would have liked the CRA to take further steps towards better facilitating breach reporting by the public, particularly during peak periods.

RCMP retention period for disciplinary records questioned

The Supreme Court of Canada's decision in *R. v. McNeil* created an obligation for the Crown to disclose to defence counsel records relating to findings of serious misconduct of the investigating police officers in circumstances where the records are relevant to the proceedings against an accused.

A staff relations representative made a complaint to our Office on behalf of RCMP members. The complainant contended that the disclosure of informal disciplinary records to the Crown was not consistent with the *McNeil* decision, arguing that the Supreme Court only requires the disclosure of disciplinary records in cases where the alleged misconduct has been the subject of a hearing.

The RCMP took the position that police misconduct of varying degrees of severity may be dealt with through either formal or informal disciplinary proceedings, so that the exclusion of all records relating to informal disciplinary proceedings might contravene *McNeil* by keeping potentially relevant records from the Crown and, in turn, defence counsel.

We agreed with this position and emphasized that the obligation rests with the Crown to determine the relevance of the disciplinary records to the particular proceedings.

Although we found the complaint to be not well-founded, we had serious concerns with the RCMP's retention policies regarding disciplinary records, which are retained until each member reaches 100 years of age, whereas most other police services across the country retain disciplinary or misconduct information for a period of between three to five years. We therefore recommended that the RCMP reconsider its retention policies. The Force however has since responded that it will continue to follow its current practice.

Continued concern over time delays

In last year's annual report, we highlighted that time-delay complaints have been consistently high in recent years, and that we received an unprecedented number in 2012-2013, with 437 in all. In 2013-2014, it appears that federal institutions continue to struggle to meet their obligations, as this number increased to 585.

As in previous years, Correctional Services Canada was the organization against which most time delay complaints were made, with a total of 296.

Many organizations highlighted difficulties in meeting timelines due to a lack of resources or challenges in processing requests that seek a broad scope of material.

We continued to work with departments during the year, requesting action plans indicating clear commitment dates for responding to individuals' requests for their personal information.

Public Service school called upon to better protect confidentiality

Senior officials of the Canada School of Public Service, the federal government's main education institution, received a first-hand lesson about the importance of having procedures to protect personal information.

In August 2012, the School received a letter from the Public Sector Integrity Commissioner (PSIC), the federal official responsible for overseeing Canada's whistleblower law, the *Public Servants Disclosure Protection Act.*

The letter said that the Integrity Commissioner was going to investigate numerous allegations of wrongdoing against seven employees at the School, identifying the seven individuals and the alleged wrongdoings.

The School had a copy of the PSIC letter hand-delivered to all seven employees named as alleged wrongdoers, advising them to cooperate fully with the investigation.

One of the seven employees being investigated also complained to the OPC that his personal information, due to his name being revealed via the aforementioned letter, had been made public contrary to *Privacy Act* provisions. Our investigation found his complaint to be well founded.

Following our Office's recommendations, the School has developed procedures to ensure the confidentiality of information associated with the *Public Servants Disclosure Protection Act* and a plan for addressing privacy breaches.

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. This category includes findings formerly classified separately as Well founded/Resolved, in which the investigation substantiated the allegations and the government institution agreed to take corrective measures to rectify the problem.

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

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

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

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

2. Other

Early resolution: Applied to situations in which the issue is dealt with before a standardl 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

Complaints and Investigations under the *Privacy Act*, April 1, 2013 to – March 31, 2014

Privacy Act Complaints 2013-2014

Category	Total
Accepted	
Access	515
Time Limits	585
Privacy	677
Total	**1777**
Closed through Early Resolution Investigations	
Access	148
Time Limits	101
Privacy	96
Total	**345**
Closed through Standard Investigations	
Access	255
Time Limits	446
Privacy	1039
Total	**1740**
Total closed	**2085**
Breaches Received	
Accidental Disclosure	154
Theft	9
Loss	29
Unauthorized Access	36
Total received	**228**

Privacy Act Breaches by Institution

Respondent	Incident
Veterans Affairs Canada	60
Citizenship and Immigration Canada	54
Canada Revenue Agency	33
Correctional Service Canada	22
Department of Foreign Affairs, Trade and Development	9
Royal Canadian Mounted Police	9
Fisheries and Oceans	6
Aboriginal Affairs and Northern Development Canada	4
Statistics Canada	4
Justice Canada	2
Canada Border Services Agency	2
Export Development Canada	2
Natural Resources Canada	2
Office of the Procurement Ombudsman	1
Canadian Heritage	1
Canada Council for the Arts	1
Canadian Human Rights Commission	1
Treasury Board of Canada Secretariat	1
Atlantic Canada Opportunities Agency	1
Public Works And Government Services Canada	1
Communications Security Establishment Canada	1
Shared Services Canada	1
Agriculture and Agri-food Canada	1
Transport Canada	1
Employment and Social Development Canada	1
Canada Post Corporation	1
Canadian Food Inspection Agency	1
Environment Canada	1
Public Safety Canada	1
Public Service Commission of Canada	1
Parole Board of Canada	1
Public Prosecution Service of Canada	1
Grand Total	**228**

Privacy Act Dispositions of Access and Privacy Complaints by Institution

Respondent	Well-founded	Well-founded resolved	Not well-founded	Resolved	ER-Resolved	Discontinued	No Jurisdiction	Settled	Grand Total
Aboriginal Affairs and Northern Development Canada	2	2	3	1	1	5	0	1	**15**
Bank of Canada	0	0	0	0	2	0	0	0	**2**
Canada Border Services Agency	2	2	11	1	4	9	0	1	**30**
Canada Economic Development for Quebec Regions	0	0	0	0	0	0	0	1	**1**
Canada Firearms Centre	0	0	0	0	1	0	0	0	**1**
Canada Post Corporation	2	2	2	1	7	0	0	0	**14**
Canada Revenue Agency	3	1	20	1	14	5	1	1	**46**
Canada School of Public Service	1	0	0	0	1	0	0	0	**2**
Canadian Broadcasting Corporation	0	0	0	0	1	0	0	0	**1**
Canadian Food Inspection Agency	0	0	3	4	0	0	0	0	**7**
Canadian Heritage	0	0	0	1	0	0	0	0	**1**
Canadian Human Rights Commission	0	1	1	0	1	0	0	0	**3**
Canadian Human Rights Tribunal	0	0	0	0	0	0	0	1	**1**
Canadian Museum of Civilization	0	1	0	0	0	0	0	0	**1**
Canadian Security Intelligence Service	0	1	11	0	0	1	0	0	**13**
Citizenship and Immigration Canada	2	1	2	1	11	14	0	1	**32**
Correctional Service Canada	15	2	29	3	97	30	0	9	**185**
Elections Canada	1	0	1	0	1	0	0	0	**3**
Environment Canada	0	1	0	1	0	0	0	0	**2**
Fisheries and Oceans	0	0	1	0	8	2	0	0	**11**
Health Canada	2	0	0	0	4	1	0	2	**9**
Immigration and Refugee Board	0	1	0	0	5	0	0	0	**6**
Industry Canada	0	0	1	0	0	0	0	1	**2**

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

Respondent	Well-founded	Well-founded resolved	Not well-founded	Resolved	ER-Resolved	Discontinued	No Jurisdiction	Settled	Grand Total
Justice Canada	1	3	5	0	3	4	0	1	**17**
Library and Archives Canada	0	0	0	0	1	0	0	0	**1**
National Gallery of Canada	0	1	0	0	0	0	0	0	**1**
Natural Resources Canada	0	0	0	0	3	0	0	0	**3**
Natural Sciences and Engineering Research Council of Canada	1	0	0	0	0	0	0	0	**1**
Office of the Correctional Investigator Canada	0	0	2	0	0	0	0	0	**2**
Office of the Information Commissioner of Canada	0	0	0	0	0	1	0	0	**1**
Parks Canada Agency	0	0	0	0	2	0	0	0	**2**
Parole Board of Canada	0	0	2	0	2	0	0	0	**4**
Passport Canada	11	0	0	0	7	2	0	0	**20**
Public Health Agency of Canada	0	0	0	0	0	3	0	0	**3**
Public Prosecution Service of Canada	0	0	2	0	0	0	0	0	**2**
Public Safety Canada	0	0	0	0	2	0	0	0	**2**
Public Sector Integrity Canada	0	0	0	0	0	1	0	0	**1**
Public Service Staffing Tribunal	0	0	1	0	0	0	0	0	**1**
Public Works And Government Services Canada	2	0	2	0	2	2	0	0	**8**
Royal Canadian Mint	0	0	1	0	1	0	0	0	**2**
Royal Canadian Mounted Police	7	14	20	4	26	5	0	5	**81**
Royal Canadian Mounted Police External Review Committee	0	0	1	0	0	0	0	0	**1**
Security Intelligence Review Committee	0	1	0	0	0	0	0	0	**1**
Shared Services Canada	0	0	0	0	1	0	0	1	**2**
Social Science and Humanities Research Council of Canada	1	0	0	0	0	0	0	0	**1**
Statistics Canada	0	1	16	0	3	1	0	0	**21**

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

Respondent	Well-founded	Well-founded resolved	Not well-founded	Resolved	ER-Resolved	Discontinued	No Jurisdiction	Settled	Grand Total
Transport Canada	1	1	1	0	3	0	0	10	**16**
Transportation Safety Board of Canada	1	0	0	0	0	0	0	0	**1**
Treasury Board of Canada Secretariat	0	0	1	0	0	0	0	0	**1**
Veterans Affairs Canada	6	1	5	1	2	0	0	0	**15**
Service Canada	0	0	0	0	4	0	0	2	**6**
Department of Foreign Affairs, Trade and Development	1	1	0	0	0	1	0	2	**5**
Employment and Social Development Canada	872	0	3	0	16	7	0	0	**898**
Department of National Defence	1	2	8	3	8	3	2	2	**29**
Public Service Commission of Canada	0	1	0	0	0	0	0	0	**1**
Grand Total	**935**	**41**	**155**	**22**	**244**	**97**	**3**	**41**	**1538**

Privacy Act Treatment Times - Early Resolution Cases by Complaint Type

Complaint Type	Count	Average Treatment Time (Months)
Access		
Access	143	2.17
Correction – Notation	4	1.20
Denial of Access	1	0.16
Time Limits		
Time Limits	97	1.97
Correction – Time Limits	3	3.01
Extension Notice	1	1.67
Privacy		
Use and Disclosure	74	2.46
Collection	18	1.42
Retention and Disposal	3	1.15
Policy	1	0.23
Grand Total	**345**	**2.11**

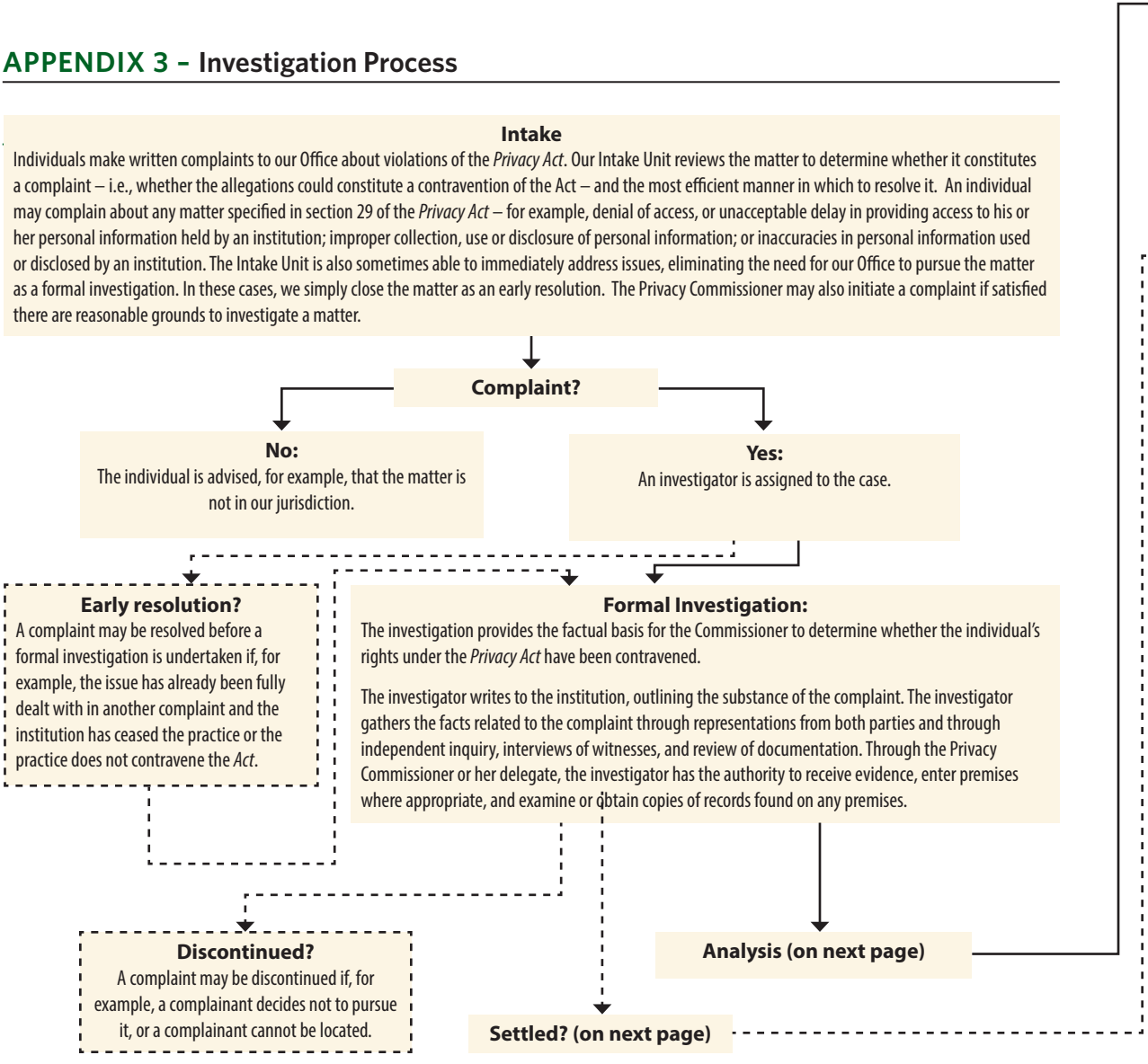
Privacy Act Treatment Times - Standard Investigations by Complaint Type

Complaint Type	Count	Average Treatment Time (Months)
Access		
Access	253	11.29
Correction – Notation	2	1.61
Time Limits		
Time Limits	433	4.52
Extension Notice	11	4.81
Correction – Time Limits	2	5.39
Privacy		
Use and Disclosure	1024	13.59
Collection	10	10.12
Retention and Disposal	5	8.20
Grand Total	**1740**	**10.87**

Privacy Act Treatment Times - All Closed Files by Disposition

Complaint Type	Count	Average Treatment Time (Months)
Formal Complaints		
Well-founded	1318	11.13
Not well-founded	193	10.56
Discontinued	118	6.66
Well-founded resolved	42	18.25
Settled	41	8.40
Resolved	25	13.01
No Jurisdiction	5	3.29
ER-Resolved	343	2.11
Grand Total	**2085**	**9.43**

APPENDIX 3 – Investigation Process



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 2013-14

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 has 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 has 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 am the fourth person to hold this office since 2007. This is the first time I have contributed to the Privacy Commissioner's Annual Report.

Five new complaints were received and investigated this year. Three of these were disposed of before March 31, 2014. The other two investigations were still outstanding at that date, but were completed shortly after the reporting period ended.

In the first complaint, the issue was whether the OPC had acted quickly enough when it sought to extend the deadline for replying to the requester. Institutions must respond within 30 days, unless they extend the time for doing so on proper grounds by "giving notice" to the individual within 30 days. The OPC mailed the notice on the 28th day and it arrived at the complainant's address on the 35th day. The question here was whether the requirement to "give" notice is satisfied by the Head sending written notice, or whether the individual making the request must actually receive the notice, within the 30 days. After considering the statutory scheme, it was concluded that the duty is met by the head sending the notice within 30 days. Accordingly, this complaint was **not well-founded.**

In a second complaint by the same individual, the issue was whether the OPC had had proper grounds to extend the time for responding to the request. The relevant part of the test under the *Privacy Act* in this case was whether meeting the original time limit would "unreasonably interfere with the operations of the institution". The investigation showed that the OPC had to review an exceptionally large number of records, approximately 100 times more than in an average request, and that it would have been unreasonable for an analyst to have to process so many pages within 30 days. OPC assigned additional resources to the task even to complete it within the extended time. This complaint, too, was found to be **not well-founded.**

In the third, related complaint from the same individual, the requester's main allegation was that the OPC had not met its obligations under the Privacy Act because it had not searched for emails and attachments in so-called backup tapes. Backup systems are designed for data protection (for example against inadvertent data deletion, fire, system crashes, etc.). They do not provide an archiving system, equipped with a fast search and retrieval capacity. Our investigation concluded that the search for information on backup tapes under any circumstance is difficult. In this particular instance, the general difficulty was exacerbated because the requester did not provide "sufficiently specific information on the location of the information to make it reasonably retrievable" by the OPC. Therefore, this complaint, too, was found to be **not well-founded.**

The main issue in each of the last two complaints concerned the proper application of section 22.1 of the *Privacy Act*, which concerns provides a mandatory exemption in some circumstances for information obtained or created by the OPC during an investigation. Much of the work on these investigations was done, although not completed, in 2013-2014. The final conclusions will be reported in the next annual report.

In addition to these three complaints, this Office also received a complaint from an individual who was dissatisfied with how the OPC had investigated his complaint about how another government department had dealt with his personal information. This Office does not have jurisdiction to investigate such cases. Our mandate is limited to receiving and investigating complaints that personal information under the control of the OPC itself may have been improperly handled.

The existence of an independent Privacy Commissioner, *Ad Hoc* ensures the integrity of the complaints process, itself an essential element in any access to information regime. We remain ready to investigate any future complaints regarding the OPC thoroughly and independently.

It is a privilege to serve as Privacy Commissioner, *Ad Hoc.*

Respectfully submitted,

John H, Sims, Q.C.