2015-2016 Annual Report to Parliament

on the *Personal Information Protection and Electronic Documents Act* and the *Privacy Act*

TIME TO MODERNIZE 20TH CENTURY TOOLS

Office of the Privacy Commissioner of Canada

2015-2016 Annual Report to Parliament on the *Personal Information Protection and Electronic Documents Act* and the *Privacy Act*
Time to Modernize 20th Century Tools

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. IP51-1E-PDF

1913-3367

Follow us on Twitter: @PrivacyPrivee

Privacy Commissioner of Canada

30 Victoria Street
Gatineau, Quebec
K1A 1H3
Tel.: (819) 994-5444
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. : (819) 994-5444
1-800-282-1376
www.priv.gc.ca

September 2016

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

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Personal Information Protection and Electronic Documents Act* for the period from January 1, 2015 to March 31, 2016 and the *Privacy Act* for the period from April 1, 2015 to March 31, 2016.

Sincerely,

Original signed by

Daniel Therrien
Privacy Commissioner of Canada

Privacy Commissioner of Canada

30 Victoria Street
Gatineau, Quebec
K1A 1H3
Tel.: (819) 994-5444
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. : (819) 994-5444
1-800-282-1376
www.priv.gc.ca

September 2016

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

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Personal Information Protection and Electronic Documents Act* for the period from January 1, 2015 to March 31, 2016 and the *Privacy Act* for the period from April 1, 2015 to March 31, 2016.

Sincerely,

Original signed by

Daniel Therrien
Privacy Commissioner of Canada

Table of Contents

Commissioner's Message

Privacy in 2016: Time to modernize 20th century tools

It is my pleasure to present my Office's 2015-2016 Annual Report to Parliament. Beginning this year, our reports on the *Privacy Act*—which applies to the federal public sector—and the *Personal Information Protection and Electronic Documents Act* (PIPEDA)—which applies to private sector organizations—are combined. An amendment to PIPEDA in June 2015 aligned its reporting period with that of the *Privacy Act*, enabling us to prepare one annual report, as opposed to having two reports tabled at different points of the year.

There was **no Internet** when the *Privacy Act* was proclaimed in 1983.

A key theme of this report is the constant and accelerating pace of technological change and its profound impact on privacy protection. In both the public and private sectors, it's clear that we need to update the tools available to protect Canadians' personal information. Not doing so, in my view, risks eroding the trust and confidence citizens have in federal institutions and in the digital economy.

New technologies enable businesses and governments to collect and analyze exponentially greater quantities of information using complex computer algorithms, leading to advances in areas ranging from the tailored treatment of diseases to the optimization of traffic flows.

At the same time, they have created the potential for information to be used in possibly questionable ways. In the private sector, businesses can track and analyze customer behaviour like never before, opening the door to invasive marketing and differentiated services based on inferred characteristics. And in the public sector, federal departments and agencies involved in national security now have increased powers to share information about any or all Canadians' interactions with government—and potentially, with the assistance of Big Data analytics, to profile ordinary Canadians with a view to identifying security threats among them.

Keeping up with all these changes to succeed in our mission to protect and promote the privacy rights of individuals has been a challenge—especially when operating under privacy legislation that predates many of these technological innovations. There was no Internet when the *Privacy Act* was proclaimed in 1983. Facebook had yet to be imagined when PIPEDA came into force in 2001.

... **90 percent** of Canadians feel they are losing control of their personal information and expect to be better protected.

We are left with 20th century tools to deal with 21st century problems. And in the meantime, 90 percent of Canadians feel they are losing control of their personal information and expect to be better protected. That Canadians would feel uninformed and not able to control their personal information given the speed and breadth of technological change and the resulting impact on their privacy rights is hardly surprising. This suggests greater action is needed from regulators, legislators, the courts, business leaders and policymakers to protect citizens.

This is the backdrop against which we present this annual report on the activities undertaken by my Office in carrying out our mission over the period covered—including investigations of complaints; advice to Parliament; Privacy Impact Assessments (PIAs) and audits; public education; conducting and supporting research on key issues; international and federal-provincial-territorial cooperation; and court action.

This report details some of the key work we have done and will continue pursuing to modernize Canada's legislative, legal and regulatory frameworks to protect privacy in the face of challenges brought forth by new technological realities.

Privacy Act Reform

Ongoing technological evolution has had a significant impact on privacy. Keeping up with all these changes has been a struggle, especially when operating under privacy legislation that predates many impactful technological innovations.

The first chapter highlights our work over the past year to pursue reform of the *Privacy Act*. After more than three decades, this law is out of step with today's existing and emerging privacy risks. In March 2016, I appeared before Parliament and shared recommendations for amending the Act in three broad categories:

- Technological change;
- Enhancing transparency; and
- Legislative modernization.

The *Privacy Act* came into force in a time when information was collected and shared in paper form and federal offices were filled with filing cabinets—decades before email, mobile devices and social media. Today, vast amounts of personal information can be collected effortlessly and lost far more easily. In recent years, we have seen massive government breaches affecting tens, even hundreds of thousands of citizens. Among our recommendations, we call for an explicit requirement for federal institutions to safeguard personal information under their control—and to report material data breaches to my Office, both mandatory obligations that private sector organizations already have or will soon face.

Citizens today have grown to expect greater and clearer details on the use of their personal information by organizations, and rightfully so. People increasingly want to know what departments do with their information, with whom they share it, and why. In its current form, the *Privacy Act* does little to help

Canadians find answers and it's why we have recommended strengthening transparency reporting requirements for government institutions and limiting exemptions to access to personal information requests under the Act.

Among our recommendations, we also ask that departments be legally required to carry out PIAs and to consult our Office before tabling legislation with potential privacy implications, so issues can be addressed early, before they affect individuals. And we recommend creating an explicit necessity requirement for personal information collected by a government program or activity to avoid the over-collection made possible by new technology.

My Office's work to encourage the modernization of the federal public sector privacy law is detailed further in this report.

Strategic Privacy priorities

Last year, my Office conducted a priority-setting exercise, following extensive consultations with stakeholders and the public. As a result, in May 2015, we announced four strategic privacy priorities that would help guide our work for the next five years:

- the economics of personal information;
- government surveillance;
- reputation and privacy; and
- the body as information.

This report provides important updates on our work in all these key and emerging areas.

Consent and the economics of personal information

In addition to the changes needed on the public sector front, it is clear that we also need to address new challenges on the private sector side as well – in particular, for example, the notion of consent, which has been a cornerstone of PIPEDA.

Personal information has become a highly valuable commodity, leading to the proliferation of new technologies and the emergence of new business models. In this increasingly complex market, many are questioning how Canadians can meaningfully exercise their right to consent to the collection, use and disclosure of their personal information.

The Internet of Things raises further questions about our ability as individuals to provide meaningful, informed consent. Everything—from cars to refrigerators—is being connected to the Internet. These machines are constantly collecting information about our habits, and organizations are finding ways to analyze and combine it with data collected by other devices in our homes and elsewhere. With so much that can be done with this information, organizations find it challenging to explain their intentions, which they may not yet fully know themselves, further compounding the complexities around obtaining meaningful consent.

We recently launched an examination and consultation on the foundational issue of consent in today's digital world. We hope to identify potential enhancements to the current model and bring clearer definition to the roles and responsibilities of the various

players –individuals, organizations, regulators and legislators – who could implement them. We will then apply those improvements within our jurisdiction and recommend other changes to Parliament as appropriate. Our discussion paper on the topic, and certain potential solutions, are described further in this report.

Government surveillance and Bill C-51

We know the risks to our security are real and complex. Canadians want to feel secure, but they do not want this goal to come at any and all cost to their privacy. They want a balanced and reasonable approach. Our goal in relation to this priority is to contribute to the adoption and implementation of laws and other measures that protect both national security and privacy.

In the past year, we contributed to the development of transparency reporting guidelines for telecommunication service providers by Innovation, Science and Economic Development Canada. Going forward, we continue to call for similar guidelines to be developed for federal institutions.

In the months leading up to the passage of Bill C-51, the *Anti-Terrorism Act*, 2015, I made a number of representations to Parliament detailing serious privacy concerns with certain provisions in the Bill, which was then unfortunately enacted without amendment.

Since the adoption of Bill, we have begun using our audit and review powers to examine how information sharing is occurring between federal institutions to ensure the implementation of the new provisions respects the *Privacy Act*. Outlined fully in chapter two, our first phase surveyed departments which reported using the legislation's new information sharing powers to generate 58 disclosures and 52 receipts of personal information all with regard to individuals they said were suspected as posing threats to security.

Looking forward, our next phase will focus on reviewing and verifying the circumstances of this sharing. Our goal is to provide as clear a picture as we can of the use of SCISA and other laws, to inform the public and Parliamentary debate that will take place in the course of the review of Bill C-51 that was announced by the government. Our hope is that this review will result in the adoption of measures that will effectively protect privacy in relation to the collection and sharing of national security information.

Chapter two also includes our review and recommendations concerning the Communications Security Establishment's (CSE) sharing of metadata with "Five Eyes" partners. After the CSE discovered that more information about Canadians was being shared than intended due to a reported technical failure, the Minister of Defence put the program on hold. Nevertheless, the CSE assessed the risk to privacy of this incident as low because the data being shared was metadata rather than the content of communications and Five Eyes partners are mutually committed to not spy on each other's citizens. We questioned that assessment, given our research that shows metadata can indeed be very sensitive, and included among our recommendations the need to amend the *National Defence Act* to include specific legal safeguards to protect Canadians' privacy.

Reputation and privacy

Canadians recognize the personal and professional benefits of participating in the online world, however they are increasingly concerned about their online reputation and we are seeing new privacy challenges in this area, both in the public and private sectors.

With this strategic privacy priority, my hope is that we can help create an environment where individuals may use the Internet to explore their interests and develop as persons without fear that their digital trace will lead to unfair treatment.

We launched a discussion paper in January 2016 and sought submissions on the privacy issues related to online reputation with a view to ultimately developing a concrete position on the means of addressing these issues, including the right-to-be-forgotten, and to help inform public and Parliamentary debate.

The body as information

The growing popularity of wearable technologies, such as fitness trackers; along with smart vests and other connected health-related products adds a new and even more personal dimension to the Internet of Things.

A global industry has arisen capitalizing on information about the body. While some promise real benefits for both individuals and the health care system as a whole, technologies used to extract information about and from our bodies carry the most sensitive personal information.

This area is developing quickly and it is not clear that appropriate privacy protections are always in place.

We want to raise awareness about the potential privacy risks associated with technology designed to read information from and about our bodies. And we want to conduct research and offer helpful guidance in this emerging area. In the short term, we have scanned current and emerging health applications and digital health technologies, such as fitness apps and heart rate monitors. We plan to test some of these products in our technology lab to better understand their privacy implications and inform consumers accordingly.

Year in review

The final chapter of this report details all the other important work undertaken by my Office to protect and promote privacy over the last reporting period.

New technologies and business models have led to privacy issues which were not necessarily envisioned at the time our current privacy laws were conceived or that challenge the relevance of existing frameworks. To add to this situation, my Office has been provided new responsibilities, further stretching our resources and challenging our ability to do the kind of proactive work we believe is necessary.

Certainly, establishing our strategic privacy priorities has helped us to ensure we focus on today's current and emerging issues, and to be strategic about how we devote our resources.

... technologies used to extract information about and from our bodies carry the most **sensitive** personal information.

However, breach reports to my Office are growing year over year, particularly since 2014 when government reporting of material breaches was deemed mandatory under Treasury Board policy. And Bill S-4, the *Digital Privacy Act*, will soon make reporting by private organizations a legal obligation.

Despite these challenges, we work to ensure that the resources and tools we do have can make the greatest impact on Canadians. We make, for example, increased use of early resolution. Following a diagnostic review of our *Privacy Act* compliance activities, we are implementing a new risk management framework under which matters posing the greatest impact on privacy will receive higher investigative priority. We will also work more closely with federal institutions to support stronger compliance.

Meanwhile, we continue efforts to raise public awareness, to help organizations and individuals understand their rights and responsibilities. This past year, for example, we launched new multi-year outreach strategies to connect with youth, seniors and small businesses. We know that individuals and organizations overwhelmingly go online first for privacy information, be it about asserting rights or fulfilling their responsibilities. As a result, we have also been working to modernize our website to better meet Canadians' needs.

... the tools we have to do our work to **protect and promote privacy** are increasingly insufficient.

Recognizing that privacy issues increasingly cross borders within and beyond Canada, my Office continues to work with provincial, territorial and international counterparts. In the past year, for example, we collaborated with our counterparts in Alberta and British Columbia to provide new guidance to organizations on Bring Your Own Device (BYOD) and an updated online security checklist.

On the international front, we coordinated the activities of 29 privacy authorities around the world engaged in the third annual Global Privacy Sweep which examined the privacy communications of companies marketing online to children. We also co-sponsored an international resolution which was unanimously adopted by data protection authorities around the world to encourage greater transparency around government institutions' warrantless collection of organizations' customer and employee personal information.

A final word

As the challenges presented by 21st century technologies mount and business models evolve, we face the reality that, despite our best efforts to find efficiencies and focus efforts, the tools we have to do our work to protect and promote privacy are increasingly insufficient.

Changes to legislation, legal frameworks, business and departmental practices, as well as individual awareness levels are required for Canada to once again emerge as a leader in privacy protection and ultimately for Canadians to have better control of their personal information.

Privacy by the numbers

Information requests related to PIPEDA matters*	4,747
Information requests related to *Privacy Act* matters	1,539
Information requests related to neither Act	3,810
PIPEDA complaints accepted*	**381**
PIPEDA complaints closed through early resolution*	**230**
PIPEDA complaints closed through standard investigation*	**121**
PIPEDA data breach reports*	**115**
Privacy Act complaints accepted and processed for investigation	1,389
Privacy Act complaints accepted and placed in abeyance	379
Privacy Act complaints closed through early resolution	460
Privacy Act complaints closed through standard investigation	766
Privacy Act data breach reports	298
Privacy Impact Assessments (PIAs) received	88
PIAs reviewed as "high risk"	39
PIAs reviewed as "lower risk"	35
Public sector audits concluded	1
Public interest disclosures by federal organizations	441
Bills and legislation reviewed for privacy implication (private sector)*	1
Parliamentary committee appearances on private sector matters*	2
Formal briefs submitted on private sector matters*	3
Other interactions with parliamentarians or staff (for example, correspondence with MPs' or Senators' offices) on private sector matters*	3
Bills and legislation reviewed for privacy implication (public sector)	7
Parliamentary committee appearances on public sector matters	6
Formal briefs submitted on public sector matters	2
Other interactions with parliamentarians or staff on public sector matters	3
Speeches and presentations delivered	116
Visits to main web site	1,819,835
Blog visits	318,136
YouTube site visits	11,647
Tweets sent	650
Twitter followers as of March 31, 2016	10,869
Publications distributed	**26,512**
News releases and announcements issued	19

* Indicates statistics collected from January 1, 2015 to March 31, 2016. All other displayed statistics were collected from April 1, 2015 through March 31, 2016.

Chapter 1:

Privacy Act Reform

Canadian society and its federal institutions have experienced profound technological advances since 1983 when the *Privacy Act* first came into force. In accelerating fashion, the explosive growth in information and communication technologies over the past three decades has made it much easier and cheaper for governments to collect and retain personal information about their citizens.

The *Privacy Act* has remained virtually unchanged, while second- and even third-generation privacy laws have since been adopted at the provincial level and internationally.

The importance of keeping pace with the privacy protections in other countries—our trading and security partners in particular—cannot be overlooked. Data protection laws in the European Union (E.U.), for example, forbid disclosing personal information from an E.U. member to entities in other countries unless (among other exceptions) those countries have been deemed to have "adequate" data and privacy protections. It used to be that the examination of adequacy of protection provided by a foreign country looked squarely at its private sector privacy law. But given revelations over the last three years unearthing significant sharing between private sector organizations and government institutions in North America especially, such an examination going forward will take into consideration a country's full privacy legal regime, including in relation to its national security activities and the right of recourse for foreign nationals. E.U. officials will pay attention to standards as they review Canadian laws on the question of adequacy.

Since **1983**, the *Privacy Act* has remained virtually unchanged.

Late in the last fiscal year, Parliament took an important first step toward reforming what were once world-leading information laws. Currently, the House of Commons Standing Committee on Access to Information, Privacy and Ethics is studying both the *Access to Information Act* and the *Privacy Act*. In March 2016, our Office appeared before the Committee and provided a submission with recommendations for changes to the latter. In contributing to the dialogue, our Office brings over 30 years of practical knowledge interpreting and applying our current law, experiencing first-hand all of its limitations.

Bringing the *Privacy Act* into the 21st century

Our submission on modernizing the *Privacy Act* included 16 recommendations covering three broad themes: responding to technological change; legislative modernization; and the need for transparency.

TECHNOLOGICAL CHANGE

Technological change has allowed government collection, storage and sharing of information to increase exponentially. Existing legal rules are simply not sufficient to regulate this kind of massive data sharing or assure personal information held by federal institutions is adequately protected from unauthorized disclosure. Given the often-passionate public debate over Bill C-51, the *Anti-Terrorism Act, 2015* (see Chapter two), which enables even broader sharing of personal information among many federal departments and agencies, it is clear this subject is of interest to a great many Canadians.

Information sharing should be based on written agreements

In its current form, the *Privacy Act* allows federal institutions to share personal information under their control with other federal institutions, provincial governments, or foreign governments for a variety of reasons, including "for a use consistent with the purpose for which the information was collected." In our experience, and given the current wording, organizations have historically argued for a very broad interpretation of "consistent use."

We have recommended that the *Privacy Act* be amended to require all such information sharing to be subject to written agreements. Among other things, these would: describe the precise purpose for which the information is being shared; limit secondary use and onward transfer; and outline other measures to be prescribed by regulations, such as specific safeguards, retention periods and accountability measures. Above all, written agreements would provide Canadians with transparency in explaining how federal institutions use their personal information. We also recommended that our Office be given the authority to review, comment on and assess compliance with these agreements.

A legal requirement to safeguard personal information

Our Office has received hundreds of reports of data breaches from federal institutions, pointing to a lack of adequate safeguards. With advances in technology, government departments are collecting and using ever-greater amounts of personal information without necessarily having the adequate safeguards in place, increasing the risk and potential consequences of privacy breaches.

Over the years, we have seen massive government breaches affecting tens, even hundreds, of thousands of citizens. In 2012, for example, the department then known as Human Resources and Skills Development Canada (HRSDC) reported the loss of an external hard drive, holding the personal information of close to 600,000 people who'd participated in the Canada Student Loan program—names, dates of birth, social insurance numbers, addresses, phone numbers and financial information.

Surprisingly—given the amount of personal information individuals have no choice but

... the *Privacy Act* does not impose a specific legal obligation on departments to **safeguard** the personal information they hold.

to share with the federal government—the *Privacy Act* does not impose a specific legal obligation on departments to safeguard the personal information they hold—a universal data protection principle found in most privacy laws around the world including PIPEDA. We believe it should be included in the *Privacy Act* as well.

In some cases, significant privacy breaches have not even been reported to our Office. In 2013, Health Canada sent letters to more than 41,000 people across the country in windowed envelopes that showed not only the recipient's name and address, but the fact the letter was from the department's medical marijuana program. The department did not report this as a data breach. Several hundred people who received the letters felt differently, complaining to our Office that Health Canada had revealed sensitive personal information without their consent.

Today, Treasury Board of Canada Secretariat (TBS) policy requires federal institutions to report "material" data breaches to our Office. In 2015-2016, the second full fiscal year in which federal institutions faced this requirement, we received 298 reports, up from 256 the year before—and up from 109 in 2012-2013, the last fiscal year where reporting was voluntary. The time has come for this breach notification requirement to be elevated from the level of policy directive to that of law. Placing a specific legal obligation on federal institutions to report such privacy breaches to our Office would ensure we have a better picture of the current scope of the problem, and that we are consulted in the process of responding to the breach and mitigating its impact on individuals.

Such a change would avoid an emerging disconnect between Canada's federal public and private sector privacy laws. Under recent amendments to PIPEDA, data breach reporting will soon be mandatory for private sector organizations. Mandatory privacy breach notification is a feature of many modern laws and was included as part of the revised Organization for Economic Development and Cooperation (OECD) Privacy Guidelines in 2013.

LEGISLATIVE MODERNIZATION

The shift from paper-based to digital format records has led to a dynamic of over-collection—the federal appetite for our information has grown in direct proportion to the ease with which that information can be collected, a trend we have seen in numerous programs. As a first step, to ensure we do not again have a badly out-of-date law in the future, we have recommended a requirement for ongoing Parliamentary review of the *Privacy Act* every five years.

Limit collection to what is necessary

The *Privacy Act* states that, "no personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution." We have interpreted this to mean that the collection of information must be necessary for the operating program or activity, an interpretation consistent with the TBS Directive on Privacy Practices and an

important factor to be measured by the E.U. looking at the question of adequacy.

This interpretation is not consistently followed across the Government of Canada. In fact, in a recent court submission, the Attorney General of Canada explicitly rejected necessity as a standard for the collection of personal information under the Act, arguing instead for a broader interpretation of the term "unless it relates directly," which would allow greater collection of personal information. This question is now before the Federal Court of Canada.

Furthermore, the Standard on Security Screening, which is set by TBS, has recently been amended to allow for much broader collection than had previously been the case. Our Office has obtained leave to intervene in a court challenge to the new standard launched by the Union of Correctional Officers of Canada. Our intervention will be as a neutral party, to help the court in its interpretation of this particular section of the *Privacy Act*. We also reviewed TBS' privacy assessment of the new standard and are investigating a number of related complaints.

Considering privacy protection up front to prevent privacy risks

The TBS Directive on Privacy Impact Assessment (PIA) is meant to ensure privacy risks will be appropriately identified, assessed and mitigated before a new or substantially modified program or activity involving personal information is implemented. The Directive requires institutions to submit a copy to our Office for review and comment. We have found—and institutions have told us—that this process is invaluable in identifying and mitigating privacy risks prior to project implementation. However, application of this policy requirement does not have force of law. As a result, the practice, quality and timeliness of PIAs can be very uneven across institutions. Some institutions that handle significant amounts of sensitive personal information seldom submit PIAs to our Office.

Similarly, some institutions may decide not to do a PIA in circumstances where, in our view, one is clearly needed or they may only complete one very late in rolling-out a new program. For example, in the 2013 case of the Canada Border Service Agency (CBSA) High Integrity Personnel Security Screening Standard, our Office was not consulted prior to implementation and a PIA was received upon the program's implementation. As a result, the new and more invasive screening measures began without our input and a related complaint under the *Privacy Act* followed. A legislative requirement to complete a PIA prior to implementation could have resulted in privacy risks being highlighted and mitigated early on.

Complaint investigations and court actions are time consuming and costly recourse mechanisms—which could be avoided if there was a legislative requirement to conduct PIAs on particularly risky programs before they are launched. Over the years, we continue to note how much more efficient and less expensive it is to identify and address privacy risks during the design of a program rather than having to modify one that is already up and running.

As a further step to identify privacy issues before they become privacy problems, we have recommended the Act also require government institutions to consult with our Office on draft legislation and regulations with

privacy implications before they are tabled; a requirement already in effect in a number of jurisdictions in Canada and elsewhere.

And, further, providing our Office with an explicit mandate to conduct education and research under the *Privacy Act*—a mandate that has been used to very good effect under PIPEDA—would enable us to better advance the purposes of the *Privacy Act*.

ENHANCING TRANSPARENCY

Currently, the Act's confidentiality provisions do not permit us to make public our investigation finding outside of annual and occasional special reports to Parliament. While we recognize that these provisions are reasonable in most cases, there should be some allowance made for limited exceptions, on grounds of public interest, as in PIPEDA. The primary goal of this discretion should be to inform Parliamentary debate and public discussions in a timely way.

In the past, our Office's ability to inform debate and discussion has been hampered by the existing confidentiality constraints in the *Privacy Act*. For example, in both the case of the CBSA's involvement with a television show (discussed in chapter six) and departments collecting personal information from a First Nation's advocate's personal social network page (outlined in our 2012-2013 annual report), we were withheld from publicly sharing our findings until reporting to Parliament several months later.

We see a particular need for greater transparency reporting in the context of **law enforcement**.

In the further interest of transparency, we have also recommended that departments be required to report on their administration of the *Privacy Act* in a more comprehensible way. These departmental reports typically comprise an elaborate array of statistics on the number of personal information requests received and processed in a year—with little or no explanation what the figures mean. If these reports are to be meaningful and useful in terms of transparency, they need to be intelligible.

We see a particular need for greater transparency reporting in the context of law enforcement. We have called on federal organizations to be open about the number, frequency and type of lawful access requests they make to internet service providers and other private sector organizations entrusted with customer information. The public, Parliamentarians and the privacy community in Canada have been advocating for more openness on this front for several years.

Maximize individuals' access to their personal information

Providing individuals with access to their personal information held by federal institutions is an important enabler of transparency and open government. We have recommended both extending rights of access to foreign nationals and maximizing disclosure, as appropriate, when individuals seek access to their own personal information.

This involves limiting the Act's exemptions to access to personal information requests, ensuring such exemptions are generally injury-based and discretionary as appropriate, and severing protected information wherever possible.

Privacy Act should apply to all federal institutions

We believe, as a matter of principle, individuals should be able to access their personal information and challenge its accuracy regardless of where it is within government.

This would be consistent with one of the fundamental purposes for which Agents of Parliament were created—as a window into the activities of the executive branch of government.

Expand Commissioner's authority to share information for enforcement

It is now truer than ever that personal information knows no borders, particularly in a world facing global security threats. Recent amendments to PIPEDA provided clear authority for our Office to share information with counterparts domestically and internationally to facilitate enforcement collaboration in the private sector. We have recommended providing the Office with a similar explicit ability to collaborate with other data protection authorities and review bodies both nationally and internationally on audits and investigations of shared concern in connection with *Privacy Act* issues.

In conclusion

Canadians have come to expect more openness and transparency about how their personal information will be used by government, with whom it will be shared, and how it will be protected. Domestic and international privacy laws have moved the yardstick considerably since the *Privacy Act* came into force in 1983. The protections of the Act as it stands are proving to be increasingly out of touch with Canadians and their engagement with a digital world.

We believe the modernization of the Act would provide Canadians with the protections and privacy rights they expect and that reflect current technological realities, thinking and experience, in Canada and internationally.

We look forward to further discussions with Parliament on bringing Canada's *Privacy Act* into the 21st century.

Chapter 2:

C-51 and surveillance

Canada is not alone in seeking the most effective ways of protecting its citizens from threats to national security. Governments around the world are collecting and sharing more and more personal information with a view to detecting and preventing threats, and new technologies are enabling the collection and analysis of previously unimaginable amounts of data. In our democratic society, finding the appropriate balance between the need for security and privacy is critical. Federal institutions with security mandates need to be able to protect Canadians, but their work must be done in ways that are consistent with the rule of law.

The ever-broader authority and capacity of government agencies to collect and share Canadians' personal information was raised time-and-again in our consultations with Canadians during our priority setting exercise.

Participants understood the value of surveillance in the protection of national security and crime prevention—but questioned how surveillance and risk profiling without their knowledge might infringe on basic rights and freedoms. The discussions also included calls for greater transparency.

The breadth of these types of concerns was underscored by the national debate following the introduction of Bill C-51 (the *Anti-Terrorism Act, 2015*) in January of 2015. This and other legislation granting government departments and agencies new and greater authority to collect and share information poses great challenges to our existing frameworks for protecting privacy.

We must consider whether privacy protections developed in the early 1980s are adequate in this new era. Under our Government Surveillance strategic privacy priority, our ultimate goal is to contribute to the adoption and implementation of laws and other measures that demonstrably protect both national security and privacy.

We must consider whether privacy protections **developed in the early 1980s** are adequate in this new era.

C-51: *the Anti-Terrorism Act, 2015*

Bill C-51 received Royal Assent in June 2015 as the *Anti-Terrorism Act, 2015*, and came into force in August 2015 The Act introduced the *Security of Canada Information Sharing Act* (SCISA), about which our Office expressed serious concerns in submissions to a number of Parliamentary committees studying the Bill, including the Senate Committee on National Defence and Security.

Since then, a new government has been elected. It has committed to consulting on changes to the law, and our Office would welcome an opportunity to share our views.

While our Office welcomed legislation to create a Parliamentary committee to oversee matters related to national security as a positive first step, we have also recommended expert or administrative independent review or oversight of institutions permitted to receive information for national security purposes.

While the question of oversight has, in part, been addressed, our concerns regarding thresholds remain. SCISA's current standard dictates that certain federal government institutions may share information amongst themselves so long as it is "relevant" to the identification of national security threats. In our view, that threshold is inadequate and could expose the personal information of law-abiding Canadians. A more reasonable threshold would be to allow sharing where "necessary."

In line with government surveillance as one of our strategic priorities, we set out a number of steps we would take in the short and medium term to reduce the privacy risks associated with SCISA. We also committed to examine and report on how national security legislation such as Bill C-51 is implemented to ensure compliance with the *Privacy Act* and inform the public debate.

We stated that we would report our findings to Parliamentarians and the public, and issue recommendations for potential improvements to policies or legislation, as warranted.

We are following through on this commitment, having recently completed a review of the first six months of SCISA—how the Act is being implemented and applied. We have identified a number of concerns, and offered recommendations.

REVIEW OF THE FIRST SIX MONTHS OF THE *SECURITY OF CANADA INFORMATION SHARING ACT*

1. The *Security of Canada Information Sharing Act* (SCISA) came into force on August 1, 2015. The stated purpose of the Act is to encourage and facilitate information sharing between Government of Canada institutions in order to protect against "activities that undermine the security of Canada". In introducing the SCISA, the government stated that effective, efficient and responsible sharing of information between the various institutions of government is increasingly essential to identify, understand and respond to threats to national security. Under the Act, information may be disclosed if it is relevant to the recipient institution's mandate or responsibilities in respect of activities that undermine the security of Canada, including in respect of the detection, identification, analysis, prevention, investigation or disruption of such activities. Protecting the security of Canadians is important, and we recognize that greater information sharing may assist in the identification and suppression of security threats.

2. The Act is broadly worded and leaves much discretion to federal entities to interpret and define "activities that undermine the

security of Canada", potentially resulting in an inconsistent approach in its application. Moreover, the scale of information sharing that could occur under this Act is unprecedented. While a preliminary review of the data suggests a limited use of SCISA during its first six months of implementation, the potential for sharing on a much larger scale combined with advances in technology allow for personal information to be analyzed algorithmically to spot trends, predict behaviour and potentially profile ordinary Canadians with a view to identifying security threats among them. Our intent in future reviews will be to examine whether law abiding citizens are indeed subject to these broad sharing powers, and if so, under what circumstances.

3. There is currently some level of review or oversight of certain federal entities responsible for national security. However, 14 of the 17 entities authorized to receive information for national security purposes under the SCISA are not subject to dedicated independent review or oversight. We note that the government has announced its intention to create a new Parliamentary Committee with responsibility for national security-related issues.

4. We initiated a review to inform stakeholders, including parliamentarians, on the extent of information sharing pursuant to the SCISA. A survey was issued to 128 Government of Canada institutions, specifically the 17 institutions which are authorized to both collect and disclose information under the SCISA and 111 federal institutions which may now disclose information to any of the 17 institutions. The survey covered the first six months that the SCISA was in force (August 1, 2015 to January 31, 2016).

5. Our survey found that during the first six months that the SCISA was in force, five institutions reported having either collected or disclosed information pursuant to the Act. The Canada Border Services Agency, the Canadian Security Intelligence Service, Immigration, Refugees and Citizenship Canada, and the Royal Canadian Mounted Police reported that collectively they received (i.e. collected), information under the SCISA on 52 occasions. The survey also revealed that collectively, the Canada Border Services Agency, Immigration, Refugees and Citizenship Canada and Global Affairs Canada made a total of 58 disclosures under the SCISA during the same time period. All of the other 111 federal institutions surveyed reported that they had not disclosed information under the SCISA. We also made general enquiries about the nature of the sharing activities. The enquiries were made to obtain an indication of the potential risk to law abiding citizens. We asked whether information shared

involved specific individuals as opposed to categories of individuals. As well, we wanted to know if the information shared included individuals not suspected of undermining the security of Canada at the time of disclosure. In responding to our survey, the entities reported that information shared under the SCISA was for named individuals suspected of undermining the security of Canada.

6. There are legal authorities that existed before the SCISA that permit the collection and disclosure of information for national security purposes. Some of these authorities are also very broad, including the common law powers vested in the police and others and the crown prerogative of defence. The survey found that 13 of the 17 entities used pre-existing authorities for such sharing activities. We did not enquire about the breadth of information shared. However, nine entities confirmed that the information sharing involved specific individuals.

7. Public Safety Canada (PS) is responsible for all matters relating to public safety and emergency management that have not been assigned to another institution of the Government of Canada. The department is also responsible for the coordination of the Public Safety Portfolio, including the Royal Canadian Mounted Police, the Canadian Security Intelligence Service and the Canada Border Services Agency. Although the Act does allow for the Governor in Council, on the recommendation of the Minister of Public Safety and Emergency Preparedness, to make regulations for implementing the SCISA—including regulations respecting disclosures, record keeping and retention requirements under the Act—it has not done so to date.

8. To support the implementation of the SCISA, PS prepared the DeskBook—a guidance document for employees in federal government institutions—and the publically available *Security of Canada Information Sharing Act*: *Public Framework*. These documents were examined as part of our review. Although they generally advocate responsible information sharing, the documents lack specificity and detail on how this should be achieved by departments and agencies in a manner that also respects privacy. Specifically, we found that the DeskBook lacks:

    - Guidance on the need for and core elements that should form part of information sharing agreements;
    - Sufficient explanation and examples, including case scenarios, that establish the thresholds for sharing and using information pursuant to the SCISA;
    - Guidance on the importance of preventing inadvertent disclosures of personal information during

discussions between disclosing and receiving institutions;

- Explanation of the factors that would mitigate against disclosure;
- Guidance on the content of records that should be kept, including a description of the information shared and the rationale for disclosure; and
- Guidance for destroying or returning information that cannot be lawfully collected.

9. The Treasury Board of Canada Secretariat (TBS) *Directive on Privacy Impact Assessmen*t (PIA) came into force in 2010. The Directive is designed to ensure privacy protection is a core consideration in the initial framing and subsequent administration of programs and activities involving personal information. This was partly in response to Canadians and parliamentarians who expressed concerns about the complex and sensitive privacy implications surrounding proactive anti-terrorism measures, the use of surveillance and privacy-intrusive technologies, the sharing of personal information across borders and the threats to privacy posed by security breaches.

10. We looked at whether the PS DeskBook provided clear guidance with regard to the requirement to complete PIAs, both in terms of the collection and disclosure of information pursuant to the SCISA. We note that the DeskBook indicates that "PIAs should not require amendments, unless normal triggers for amending PIAs are present". Although collection authorities may not change for institutions that receive information under the SCISA, it is clearly intended that more and different information may be received than was the case prior to the enactment of the Act. The disclosure of information for purposes other than that for which it was collected constitutes a substantial modification to a program or activity of the institution. According to the PIA Directive, such activities would trigger the need for a new or amended PIA. The PIA guidance provided in the PS DeskBook should align with the requirements and intent of the TBS directive.

11. Of the 17 entities authorized to collect information under the SCISA, 12 had undertaken some form of analysis to determine whether Privacy Impact Assessments (PIA) for their respective information sharing processes were necessary. Of these, two of the entities indicated that PIAs were deemed necessary and were under development.

12. As part of our survey, we asked institutions whether they developed policies and guidance documents to operationalize the Act. As reported above, five institutions collected and/or disclosed personal information

pursuant to the SCISA during the review period. Of these, three had developed such documents. We examined them and found that they lacked specificity and detail to provide meaningful assistance to employees to help them determine whether SCISA thresholds have been met. This small sample underscores the importance of having clear government-wide guidance to operationalize the SCISA.

13. **Recommendation**: Public Safety Canada should provide government institutions with sufficient guidance and direction to ensure that:

    - Information-sharing agreements are put in place and contain core privacy protection provisions;
    - The thresholds for using the SCISA—for collection and disclosure purposes—are understood;
    - Discussions between disclosing and receiving institutions do not result in an inadvertent disclosure of personal information;
    - Factors that would mitigate against disclosure are explained;
    - Appropriate record keeping practices are in place;
    - The privacy impacts of SCISA-related collection and disclosure activities are assessed; and
    - Information that cannot be lawfully collected is immediately destroyed or returned to the originating institution.

Departmental response: *Public Safety Canada agrees with the recommendation.*

The Department has provided guidance to institutions on the Security of Canada Information Sharing Act (SCISA), and Public Safety Canada will continue to do so in the future. For example, Public Safety Canada will provide further guidance on appropriate record-keeping practices, on the threshold for disclosure, and on the need to immediately destroy or return to the originating institution information that cannot be lawfully collected by a recipient, and on the other issues identified in the recommendation.

The Department of Public Safety and Emergency Preparedness Act provides the Minister of Public Safety and Emergency Preparedness and by extension, the Department the authority to "coordinate, implement or promote policies, programs, or projects relating to public safety and emergency preparedness" and "facilitate the sharing of information, where authorized, to promote public safety objectives." In keeping with this mandate, the guidance prepared by

Public Safety Canada on the SCISA and its disclosure authority is provided to institutions to help them in understanding the Act. Each Deputy Head is accountable for ensuring the proper implementation of the SCISA in their respective institution.

14. The next phase of our review will focus on verifying the details and nature of the personal information sharing activity pursuant to the SCISA, in part to confirm the information given to us by departments. It will also examine the exchange of personal information—for national security purposes—using legal authorities other than the SCISA. Our goal is to provide as clear a picture as we can of the use of SCISA and other authorities, to inform the public and parliamentary debate that will take place in the course of the review of Bill C-51 that was announced by the government. Our hope is that our work in this area will result in the adoption of measures to protect privacy effectively in relation to the collection and sharing of national security information.

The next phase of review activities will commence in fiscal year 2016-2017.

Security agency metadata sharing leads to review and recommendations by our Office

In January 2016, the Minister of National Defence announced that, until further notice, the Communications Security Establishment (CSE) would no longer share certain metadata with its international security partners. The announcement followed the release of the 2014-15 Annual Report of the Office of the CSE Commissioner (the CSE's oversight authority), which reported that information revealing details about the communication activities of Canadians was, due to a filtering technique that became defective, not being properly minimized (for example, removed, altered, masked or otherwise rendered unidentifiable) before being shared with "Five Eyes" partners—the signals intelligence agencies of Australia, New Zealand, the United Kingdom and the United States.

WHAT IS METADATA?

The classic definition is that it is "data about data." It's not the content of an email or telephone conversation, but all the other information about the communication. Our email metadata, for example, would reveal who we sent emails to; when we sent them; our email and IP addresses; the recipients' email addresses; the email client login records with IP address; and the subject of the emails; and more. In the digital age, we generate metadata constantly, and when it is all combined and analyzed, it can reveal a great deal about who we are—not just our identity, but our habits and interests, the places we go and the people we associate with. To better understand and raise awareness of the potential impacts on privacy, our Office has conducted substantial research into metadata.

As noted in the CSE Commissioner's report, the CSE discovered in late 2013 that certain metadata was not being properly minimized. Although it was able to confirm that protections were in place in 2008, the CSE could not say for sure how long after that the problem arose, or how much metadata that was not minimized had been shared, before the 2013 discovery. It did however tell us that it shared large volumes of metadata with partners, some of which may have had a "Canadian privacy interest."

Given the potential impact on Canadians' privacy, our Office conducted a review of the circumstances that allowed this situation to arise. In April 2016, we shared our observations and recommendations with the CSE.

CSE'S ASSESSMENT OF THE BREACH

The CSE contended that the risk to privacy was minimal, because:

- The metadata did not constitute sensitive private information as it did not include names, contextual details related to individuals or contents of communications;
- Further analysis of the metadata would be required in order to identify specific individuals; and
- Five Eyes partners have all made commitments to carry out their operations while respecting the privacy of one another's citizens.

NEED FOR GREATER ASSURANCE

We questioned the CSE's contention that the risk was low for the following reasons:

- On the potential sensitivity of the data shared with partners, research by our Office and others, including a recent report from Stanford University, demonstrates that metadata can reveal very sensitive information about individuals' activities, associates, interests and lives.

- On the issue of partner's commitments not to spy on one another's populations, we have no reason to doubt this pledge but at the same time, such assurances cannot be construed as absolute guarantees. In fact, CSE officials told us words to the effect that 'states may do what they must to protect their national interest and security.'

- CSE acknowledged that the amount of metadata improperly shared with Five Eyes partners was large.

Following our review, we recommended that, going forward, before it resumes sharing metadata, the CSE should conduct a full Privacy Impact Assessment (PIA) on the program in accordance with the Treasury Board of Canada Secretariat's Directive on PIA. We also offered the expertise of our Office to assist in the process of clarifying the metadata Ministerial directive, and recommended that the *National Defence Act* be amended not only to clarify the CSE's powers—as suggested by the Office of the CSE Commissioner—but that those powers be accompanied with specific legal safeguards to protect the privacy of Canadians.

Warrantless access and the ongoing need for greater transparency

The legal controversy around "warrantless access" refers to the practice of law enforcement agencies seeking information about individuals from their telecommunications and Internet service providers without first obtaining court authorization.

In *R v. Spencer*, the Supreme Court stated that a warrant is needed in all circumstances except where: 1) there are exigent circumstances, such as where the information is required to prevent imminent bodily harm; 2) there is a reasonable law authorizing access; or 3) the information being sought does not raise a reasonable expectation of privacy.

Since this June 2014 ruling, many telecommunications companies and Internet service providers have required warrants or production orders when police officers seek confidential subscriber data.

Some law enforcement officials have said it has made their jobs impossible, arguing such a legal requirement is untenable in an era where more and more criminal activity has migrated online, where anonymity is often the norm.

However, an IP address can reveal a great deal about an individual. Access to basic subscriber information linked with Internet activity can unlock details of a person's interests based on websites visited, their organizational affiliations, where they have been and the online services for which they have registered.

Consequently, impartial oversight in the form of judicial authorization is critical before sensitive personal information may be turned over to the State. Courts are best placed to balance the interests of the police and of individuals. It is only in exceptional circumstances that warrantless access is and should be permitted.

PROGRESS ON TRANSPARENCY

Following the Supreme Court's landmark decision in *R. v. Spencer*, some telecommunications and other service providers began issuing their own, voluntary reports on requests from government authorities for information about their customers and clients. While we found these reports to be helpful, companies provided different information in varying forms, making it difficult to draw an accurate picture of the number and types of requests that were coming from government authorities, and how companies were responding to them.

In June of 2015, following consultation with our Office and various other stakeholders, Innovation, Science and Economic Development issued new transparency reporting guidelines for private sector organizations into which we provided input. While reporting remains voluntary, the guidelines seek to achieve more uniform reports, and better inform Canadians about how often, and in what circumstances businesses provide customer information to law enforcement and security agencies.

We hope companies will see the **value of transparency** and share relevant information with public.

Going forward, we hope companies follow the guidelines and that we begin to see more consistent reporting. For companies that have yet to produce such reports, we hope they will see the value of transparency and share relevant information with public. If not, we may resume our call for legislative changes in this area.

NEED FOR PUBLIC SECTOR ACTION

While a good first step, private sector reporting provides only part of the picture. Further transparency from the public sector is needed to shed light on how the use of powers to obtain personal information lines up with the associated privacy risks.

To match the momentum started within the private sector, we have asked federal institutions to issue their own transparency reports about requests they make to private sector organizations for customer information. This was part of our recommendations on *Privacy Act* reform, discussed in chapter one.

We have called on federal institutions to maintain accurate records and to report publicly on the nature, purpose and number of lawful access requests they make to telecommunications companies. Such an approach would give citizens and Parliament greater insight into how federal institutions are using their lawful access powers.

In conclusion

One point on which all voices in the debate around public safety and privacy would agree is that much has changed over the last two decades. National security threats are no longer beyond, but sometimes within, our borders and we recognize that the online environment poses new challenges for policing.

On the other hand, recent legislative changes have raised concerns about the possibility of intrusive monitoring and profiling of ordinary Canadians.

Canadians value security in the face of threats confronting the world today, but they also care deeply about their privacy. They want to ensure laws and procedures are in place that respect our values, and they want law enforcement and national security agencies to do their job lawfully.

When it comes to security and privacy, rather than wanting one over the other, Canadians rightly want both. Finding the right balance is absolutely critical because the repercussions can be so serious when that equilibrium shifts too far one way or the other.

In pursuit of a better balance, we have recommended, for example, changing SCISA's information sharing threshold from "relevance" to "necessity;" that private and public sector institutions follow through on transparency reporting; and amending the *National Defence Act* to add legal safeguards for protecting personal information collected and used by the CSE.

Chapter 3:

Consent and the economics of personal information

The fact that personal information has commercial value is well established. Over time, as marketing became more sophisticated, companies moved beyond collecting names and addresses and started asking for more and more of our personal information—before mailing in the little card to register a new product, for example, we might be asked to tick off boxes about our income, whether we owned or rented our home, and how we heard about the product we'd just purchased.

... we are constantly providing **personal information**—about our interests, our habits and our location.

Today, even that kind of one-on-one information transaction, in which we knew who was asking, had a reasonable chance of understanding why they were asking the question—and could choose to check the boxes or not—is a thing of the past. As we search, surf and shop on the Internet, expand our social media profiles or add a new app to our smart phone, we are constantly providing personal information—about our interests, our habits and our location.

It has become increasingly difficult to know what personal information is being collected from us and by whom—let alone understand the 21st century business models fuelled by personal information and the automated processes that make them work.

It is ironic that, while the commercial potential of our personal information has increased dramatically, the investment required to obtain, store and analyze it is often minimal—as much as we are in the age of Big Data, we are also in the age of cheap data. Thanks to technological advances and the increased willingness on the part of people to put information about themselves online, it is very easy and inexpensive to collect astronomical amounts of personal information and use it for commercial ends—web-crawling software that spammers use to collect email addresses is just one example.

The right to consent

To protect our privacy in this increasingly digital environment, we rely on the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

In many ways, consent is the cornerstone of this legislation. Organizations are required to obtain individuals' consent to lawfully collect, use and disclose personal information in the course of commercial activity. Without consent, the circumstances under which organizations are allowed to process personal information are limited.

However, while it was written to be technology neutral, this legislation predates smart phones, cloud computing, Facebook, the Internet of Things and so many other information-gathering technologies that are now part of the everyday. It is no longer entirely clear who is processing our data and for what purposes.

Is it fair then to saddle consumers with the responsibility of having to make sense of these complex data flows in order to make an informed choice about whether or not to provide consent? Technology and business models have changed so significantly since PIPEDA was drafted that many now describe the consent model, as originally conceived in the context of individual business transactions, to be no longer up to the task.

Among the stakeholders we consulted during our priority setting exercise, there were numerous questions about the efficacy and suitability of the PIPEDA consent model in the context of Big Data and the myriad and opaque ways our information can be collected. Many held the view that individuals are much less able to exert control and provide meaningful consent based on privacy policies that are often hard to understand, excessively long yet incomplete and/or ineffective. Canadians who participated in focus groups held as part of our priority setting exercise told us much the same thing, expressing concerns about not having enough control over their online information. They felt uninformed about what their personal information was being used for and by whom and felt online privacy policies were generally incomprehensible.

Consent in the 21st century

In May 2016, our Office released a discussion paper on consent and privacy. In it, we consider the role of individuals, organizations, regulators and legislators and what might be expected of each of these parties in the future. We look at how other countries have dealt with the matter and outline a number of potential solutions.

For example, we propose measures that would enhance consent by giving individuals better access to information or the ability to manage preferences across different services.

Possible solutions that serve as alternatives to the consent model are predicated on the notion that information flows have become too complex for the average person and that the ultimate solution is a relaxing of requirements for consent in certain circumstances. For example, the European Union allows data processing without consent if it is necessary for legitimate purposes and does not intrude on the rights of individuals.

A possible solution for Canada may be to broaden the permissible grounds for processing under PIPEDA to include legitimate business interests, either as flexible concept or by defining specific legitimate interests in law. We might also consider legislating "no-go" zones which outright prohibit the collection, use or disclosure of personal information in certain circumstances.

Governance solutions focus on the role organizations play and could involve things like industry codes of practice, privacy trust-marks or the creation of consumer ethics

boards to advise businesses on appropriate uses of data.

Such solutions, however, raise questions about the role of regulators and what authorities are required to effectively hold organizations to account. Order-making powers and fines, which our Office doesn't currently have, are some examples of enforcement measures that could influence an organization's practices and strengthen privacy protections for individuals. As well, currently our Office plays a more reactive role. We generally investigate complaints after a violation has occurred. Would it be reasonable to give our Office the authority to oversee compliance with privacy legislation more proactively, before problems arise? While many proposed solutions can be implemented within the current legal framework, others, such as the expansion of powers, may require legislative change.

Whether to legislate no-go zones, new legal grounds for processing where consent isn't practicable or "privacy by design"—which would require companies to integrate privacy protections into new products and services—are among other possible solutions that could fall to law-makers.

We have since invited written feedback to our consent paper and in the fall will be speaking directly with stakeholders—businesses, advocacy groups, academics, educators, IT specialists and everyday Internet users.

While it is unlikely that any one solution could serve as the proverbial "silver bullet," we believe a combination of solutions may help individuals achieve greater privacy protection, which is our ultimate goal.

THE INTERNET OF THINGS

The Internet of Things (IoT)—the term used to describe the growing number of physical objects that collect data using sensors and share it over telecommunications networks—presents unique challenges to consent-based privacy protection frameworks.

IoT provides individual and societal benefits through increased automation and monitoring of all aspects of the environment, potentially leading to better management of resources, increased efficiencies and added convenience. IoT applications can be used to lower home energy costs by running appliances when electricity is cheaper or managing traffic flow by monitoring the number of vehicles through road-embedded sensors.

As discussed in our February 2016 IoT research paper, the collection of IoT information is motivated by a desire to understand individuals' activities, movements and preferences, and inferences can be drawn about individuals from this information. For organizations, the value lies not in the revenue from selling devices but in the data that is generated and processed through big data algorithms.

Much of this data may be sensitive, or be rendered sensitive by combining data from different sources. For example, combining data generated by an individual carrying a smart phone, wearing a fitness tracker, and living in a home with a smart meter can yield a profile that can include physical location, associates, likes and interests, heart rate, and likely activity at any given time. If combined with other data collected in different ways—our

Internet activity, for example—the information becomes more sensitive and more valuable.

Data collection by IoT devices is often invisible to individuals. There is no interface between consumers and organizations where data is exchanged in a visible and transparent way. Instead, data collection and sharing occurs device to device, without human involvement, as a result of routine activities. This makes it increasingly challenging to relay meaningful information about privacy risks in order to inform the user's decision about whether or not to provide consent.

Key investigation findings involving consent issues

POSTING AN EMAIL ADDRESS ONLINE ISN'T PROVIDING CONSENT TO BE SPAMMED

Following the launch of the Canadian Radio-television and Telecommunications Commission (CRTC) Spam Reporting Centre, we noted hundreds of submissions from the public about the e-mail marketing activities of Compu-Finder, a Quebec-based corporate training provider. This led to our first-ever investigation under the address harvesting

FOLLOWING-UP ON BELL'S RELEVANT ADVERTISING PROGRAM

In October 2013, our Office received an unprecedented number of complaints following the introduction of Bell's "Relevant Advertising Program." This program involved tracking of customers' Internet browsing, app usage, telephone calling and television viewing activity—information Bell combined with demographic data from customer accounts to create detailed profiles to help third-party advertisers deliver targeted ads to Bell subscribers, for a fee.

Bell put the onus on customers unwilling to participate in the program to take steps to opt out. We concluded that customers should instead be asked to opt in—in other words, expressly choose to consent.

Following our investigation, Bell said it was cancelling the program and deleting all existing customer profiles related to the initiative. It later advised that it planned to launch a similar program using opt-in consent and asked for our views on the revised initiative.

Given the unprecedented number of complaints about the previous program and the potential privacy impacts of this type of targeted advertising on millions of individuals, we felt it was in the interest of Canadians to review and provide comments to Bell on the revamped program, and to that end, our Office had a number of discussions with the company.

While we are not in a position to say whether the new program meets the obligations set out under PIPEDA, we believe the new program is an improvement upon the one we investigated previously in that Bell is asking its customers whether they wish to participate on an opt-in basis. As we have previously stated, we see online behavioural advertising (OBA) as a legitimate activity if done correctly with the proper consent. We have provided suggestions for organizations in our Guidelines on online behavioural advertising.

provisions of PIPEDA introduced by Canada's anti-spam law (CASL).

During our investigation, the company reported that as of January 2014, it had some 475,000 e-mail addresses on file, about 170,000 of which it had collected using address harvesting software. While the company claimed it ceased collecting e-mail addresses using such software prior to CASL's July 2014 coming into force, we found it clearly continued to use some of these addresses for marketing purposes afterwards.

Compu-Finder said it collected addresses from websites of companies which it believed would be interested in its training and which, under Quebec law, had an obligation to provide such training. We found, however, that while its training sessions were offered almost exclusively in French at facilities in Montreal and Quebec City, the company was continually sending emails to recipients across Canada and even overseas.

Compu-Finder told us it thought email addresses posted on websites could be collected without consent under the "publicly available" exception in PIPEDA. In our view, this exception did not apply. Compu-Finder was using the addresses to sell services not always directly related to the purposes for which organizations had posted individuals' e-mail addresses on their websites—such as a computer science professor who received an email promoting a course for finance directors.

We also found that some of the sites from which the company collected addresses had clear statements that email addresses on the site were not to be used for solicitation. In any event, the publicly available exception in PIPEDA cannot be claimed if an address was collected with address-harvesting software.

It was clear Compu-Finder was not aware of or did not respect its privacy obligations under PIPEDA. The company eventually agreed to implement all of our recommendations and enter into a compliance agreement marking our first use of this new tool made possible by changes to PIPEDA introduced by the *Digital Privacy Act*, which gained Royal Assent in June 2015.

Companies should read and understand PIPEDA's regulations carefully before determining if information is really "publicly available." In April 2015, we also posted a tip sheet and guide that describe best practices in email marketing and how to comply with the new address-harvesting provisions in PIPEDA.

CUSTOMER GETS SIGNED-UP FOR CREDIT CARD WITHOUT CONSENT

More and more often, we are asked to consent to the collection and use of our personal information by clicking an icon on a computer screen, a practice that creates risk. In this case, for example, the complainant told us that, while shopping at a retail store, he was approached by a salesperson and asked to join a loyalty program. The complainant stated that he agreed to join the loyalty program, but was surprised to receive a credit card from the retailer in the mail a few weeks later.

The complainant maintains he was never informed that he was applying for a credit card and, in fact, said he asked the salesperson directly if the application had anything to do with a credit card and was told it did not. In our investigation, we found much

of the information on the credit application submitted in his name—including his phone number, occupation, annual income and monthly rent—was, in fact, inaccurate.

The retailer stated that the complainant knowingly provided his personal information for the purpose of obtaining a credit card, and provided his express consent for a credit check by checking a box on the tablet computer the salesperson was using to record the information. However, the retailer was unable to prove that the complainant: ever saw the tablet screen; provided all the information included in the application; understood that it would be used to collect his credit information; or that he (and not the retailer's representative) actually clicked the requisite consent box.

Organizations must recognize that employees may not always follow procedures, so it is important that additional checks and balances are in place to ensure, for example, that consent can be verified. Our Privacy Toolkit: A Guide for Businesses and Organizations includes specific direction to organizations to "retain proof that consent has been obtained."

The retailer apologized to the complainant, cancelled the credit card and asked the credit reporting agency to remove the account and inquiry from the complainant's file.

In conclusion

New technologies and business models are raising important questions about how Canadians can meaningfully exercise their right to consent to the collection, use and disclosure of their personal information.

The time has also come to seriously think about the practicability of the current consent model under PIPEDA and how it might be better supported or enhanced.

With the release of our discussion paper, we hoped to launch a national, if not international, brainstorming session among business, advocacy groups, academics, educators, IT specialists and everyday Internet users.

In the end, we hope to be in a position to contribute real, concrete solutions and to identify what role individuals, organizations, regulators and legislators need to play if we are to truly help people exercise greater control over their personal information.

While many proposed solutions can be implemented using existing tools and within the current legal framework in Canada, others may require legislative change. This could include, if they are found desirable, potential changes to our Office's powers, the ability to be more proactive in our work, the establishment of no-go zones and even new legal grounds for processing where consent may not be practicable.

Chapter 4:

Reputation and privacy

Particularly since the advent of social media, much has been written about online reputation and how it can affect people's lives, both online and off. Internet technologies have caused a paradigm shift in the way reputations are formed. A more robust discussion is needed about the recourse available to people who object to the personal information that is posted about them online and the attendant roles of businesses, regulators, legislators and individuals.

In addressing the Reputation and Privacy strategic priority, our Office is focusing on the reputational risks stemming from the vast amount of personal information posted online. We are also considering existing and potential mechanisms for managing these risks and the options available to assure individuals can exert some control over their personal information.

... our Office is focusing on the **reputational risks** stemming from the vast amount of personal information posted online.

During our priority setting exercise, both stakeholders and individual Canadians told us they recognize the personal and professional benefits of participating in the online world. At the same time, they are increasingly concerned about their online reputation. In fact, the difficulty involved in controlling how our information is used online—let alone correcting or deleting it—was one of the most frequently expressed concerns throughout the exercise.

While we build our online reputation by posting profiles and photos or commenting on others' content, others can shape our reputation as well. Once our personal information is posted, it can be extremely challenging to keep others from using it in different contexts that could damage our reputation. And given the persistent nature of online content, once a reputation is tarnished, undoing the damage can be difficult.

The right to be forgotten

What others post about us, sometimes malevolently, or sometimes for well-intentioned purposes such as through open courts, journalism, open government, archives, for example—may be very difficult to forget or not be constantly reminded about. The whole world is grappling with the implications of the persistence of online personal information, and how this may impact human behavior and relationships over the long term.

The potential for reputational damage has been increased with the advance and commonality of search engine technology. This has rendered information once only traceable through great effort in archives

easily findable with a few keystrokes. In May 2014, the Court of Justice of the European Union ruled that search engines must offer all Europeans the opportunity to request the removal of search results that link to information about them that is "inaccurate, inadequate, irrelevant, or excessive."

The decision came as a result of a case involving a Spanish man who objected when a Google search on his name returned links to newspaper stories mentioning past financial debts he had long since repaid. He believed those details about his life were no longer relevant but were affecting his reputation.

The ruling is often referred to as the "right to be forgotten." The information at issue is not actually deleted—the ruling applies only to search engine results. Nonetheless, the ruling gives individuals some degree of control over access to their personal information by making it more difficult to find.

Opening a discussion

In January 2016, our Office issued a discussion paper that looked at the issue of online reputation in a Canadian context and set out the related privacy challenges faced by individuals online. By doing so, we hoped to stimulate the discussion about the scope of this emerging challenge and potential solutions.

Our aim in publishing the discussion paper was to draw attention to this emerging challenge in privacy protection with the intention of stimulating discussion about solutions. Ultimately, we intend to develop a position on remedies. To this end, we called on individuals, organizations, academics, advocacy groups, information technologists, educators and other interested parties to propose new and innovative ways to protect reputational privacy.

Specifically, we highlighted and sought views on potential gaps in protections between the online and offline worlds. We sought ideas on practical, technical, policy or legal solutions that should be considered to mitigate online reputational risks.

We received 26 submissions. The consultation's goal was to enrich the public debate and ensure that our Office is well positioned to inform Parliament on matters related to online reputation and to develop a policy position on this issue.

In addition to the discussion paper released in January, our Office dealt with the issue of reputation and privacy in work within the private and public sectors as well as the courts, outlined in the following examples.

Ashley Madison: A breach of intimate details

In today's online economy, many types of commercial websites of all sizes can hold substantial amounts of personal information extending beyond payment data. Under PIPEDA, the implications for individuals' reputations needs to be considered by organizations in determining the safeguards they must have, and other requirements such as those for consent.

In the summer of 2015, the servers of the Canadian company Avid Life Media (ALM) (recently rebranded as Ruby Corp.), that operates the Ashley Madison website—aimed at people looking to arrange a discreet

affair—were compromised by hackers, who subsequently published information from the accounts of approximately 36 million users in Canada and around the world.

Given users in some 50 countries were affected; we conducted a joint investigation with our counterpart agency in Australia through the Asia-Pacific Economic Cooperation Cross-border Privacy Enforcement Arrangement.

The investigation identified a number of contraventions of both PIPEDA and Australia's *Privacy Act*—and resulted in findings that offer important lessons for other organizations that hold personal information:

SECURITY

Safeguards put in place by ALM to protect personal information were not adequate. Considering the sensitivity of the information it held, the company's lack of a comprehensive information security plan was unacceptable. Specifically, the company's security framework was lacking a number of key elements, including: documented information security policies or practices, as a cornerstone of fostering a privacy and security aware culture; an explicit risk management process, including periodic and pro-active assessments of privacy threats, and evaluations of security practices; and adequate training to ensure all staff were aware of, and properly carried out, their privacy and security obligations.

In addition, specific weaknesses such as single factor authentication and poor key and password management practices also individually and collectively constituted failures to take reasonable steps to implement appropriate security safeguards of the personal information held by ALM.

CONSENT AND TRANSPARENCY

ALM did not obtain valid consent from users for the collection of their personal information in that they were not clear about some of their information handling practices up front, and because the consent was obtained at least in part through deception—the company displayed a fabricated "Trusted Security Award" on its home page, suggesting to would-be users that its information security practices had been reviewed and deemed high quality by an independent third party.

RETENTION

ALM's practice of indefinitely retaining users' personal information, unless they had paid for a "full delete," contravened PIPEDA's retention requirements which state that personal information shall be retained only as long as necessary for the fulfillment of the purposes for which it was collected.

EMAIL ACCURACY

ALM's practice of requiring email addresses from registrants, but not adequately ensuring the accuracy of those addresses, resulted in the email addresses of people who had never actually signed up for Ashley Madison being published online following the breach. This practice knowingly created reputational risks for non-users and contravened PIPEDA's accuracy requirements.

We were pleased that ALM, as a result of our joint-investigation, agreed to implement measures to address the concerns outlined

above. But, we will follow up to verify that they have met their commitments under a compliance agreement reached with the company at the end of the investigation.

In addition to illustrating the critical importance of considering the risk to reputation when ensuring appropriate safeguards are in place, this incident also demonstrates the care that must be taken when making statements to consumers about security and privacy to inform their consent.

This case also demonstrates that, in the face of ever decreasing costs of storing data, there are real costs and privacy risks to individuals and organizations of retaining personal information once it is no longer needed for the purpose for which it was collected.

The deficiencies found in this case, unfortunately, are not exceptional. There are lessons to be learned for all companies that manage large amounts of personal information, and, in 2016, there are many such companies.

Globe24h.com: A global risk to reputation

Once our personal information is uploaded online, even with the best of protections and intentions, it can be very difficult to control where it goes or how it is used after that—and, unlike the Internet, privacy protections at times do not easily cross international boundaries. There is a clear need for global cooperation in protecting reputation, illustrated by the case of a Romanian-based website, Globe24h.com, which republishes court and tribunal decisions, including those from Canada.

Recognizing that these decisions can contain sensitive personal information, Canadian courts do not allow these documents to be indexed by individuals' names—so that when a person's name is entered in a search engine, it would not return links to court proceedings in which they had been mentioned.

Globe24h.com removes this protection when it republishes the documents, allowing them to be searched by name. More than two dozen complaints about the site were filed with our Office. One of these, for example, was filed on behalf of the complainant's daughter, who was named and described as a "sex worker" in a case in which she had acted as a witness. This court document was the first result returned when searching her name online.

As documented in our PIPEDA annual report for 2014, our investigation found that, while Globe24h.com did offer people the opportunity to remove their personal information from the site, it demanded payment, sometimes in the hundreds of dollars—a business model that we found a reasonable person would not consider appropriate in the circumstances. Further, we also found the website had not obtained meaningful consent by affected individuals.

Beyond that, the website states that it is not subject to Canadian law, and refused our request to remove Canadian court and tribunal decisions from its servers and search engine caches.

One of the original complainants, looking to have our recommendations enforced, has filed an action against the website in the Federal Court of Canada. Our Office has been granted party status in the proceeding, which raises

a number of issues, including the extent to which PIPEDA applies to a foreign-based website.

In the meantime, our Office has had some success in asking some of the major search engines to voluntarily remove links to the Globe24h website, or otherwise reduce the company's prominence in search results.

In conclusion

Immense technological changes in a relatively short period of time have brought about new challenges to regulation, legislation, legal frameworks and individuals. Even if we exercise great care in what we post online about ourselves, we have little control over what others may post, or how our online activities—from what we buy to what we read—may be interpreted by various algorithms.

There are significant legal questions still to be answered, beginning with an examination of the effectiveness of existing privacy protections. PIPEDA is now more than 15 years old, and many of the online risks to reputation we see today had yet to emerge when the legislation was proclaimed. We must question how some of its founding principles—including ensuring accuracy of personal information held by organizations; limiting collection, use and disclosure to only appropriate purposes; and providing meaningful opportunity for individuals to withdraw consent—can be applied effectively in a world increasingly marked by the automated analysis of persistent online data.

Chapter 5:

The body as information

The rise of digital health technologies, or collecting, using and disclosing biometric data for commercial, recreational, and forensic purposes represents the increased use of the most personal of our information – that of our bodies.

A whole global industry has arisen that capitalizes on information about the body—from blood analysis to genetic testing. More and more devices that collect this information, from fitness trackers to bathroom scales, are connected to the Internet of Things, enabling the collection, analysis and sharing of unprecedented amounts of the most intimately personal information.

How this information is used or disclosed could affect our lives in a variety of ways, from our future insurability or employability to our personal relationships. In the case of genetic testing, our families could be affected as well.

In short, the **risk** to our most intimate personal information has been transformed by technology.

In short, the risk to our most intimate personal information has been transformed by technology. And neither the tools nor the general awareness that would enable individuals to control this highly personal information have kept pace.

Potential benefits, potential risks, real concerns

During our priority setting exercise, stakeholders and focus group participants alike agreed that, because of its sensitivity, body-related information requires our special attention.

As new technologies and practices implicating the body emerge, participants recognized the many potential benefits offered to society through biomedical advances and other avenues of technological progress that involve the body. At the same time, participants emphasized the importance of ensuring the anonymity of this information, and the need for a proactive approach to identify and address the impacts on privacy. Many stakeholders expressed particular concern over the application of Big Data analytics to health, genetic and biometric information, pointing to the potential risk of harmful secondary uses ranging from marketing to insurance applications to potential uses yet to be even imagined. Some saw the need for clear restrictions in this area.

Others saw a need for enhanced transparency to provide individuals with a better awareness of what information was being collected, by whom, and for what purposes. The privacy of vulnerable groups, such as those who are dependent on medical

devices, was seen as being most at risk. Security was also viewed as a significant concern due to the sensitivity of the information and its attractiveness to criminals and vulnerability to hacking.

These are issues that are of broad concern to Canadians. In our 2014 survey of individuals on privacy matters, for example, more than 80 percent of respondents stated they were concerned about the results of genetic testing being used for non-health related purposes, and 70 percent stated some degree of concern about wearable computers that collect personal information from the wearer.

Understanding the issues

Wearable computers and other connected devices, such as smart scales, sleep monitors and other health-related products are capable of not only capturing, but sharing some of our most intimate data—fitness trackers, for example, that connect to a user's smart phone, and link in turn to a cloud application which evaluates the data; offers advice to the user; and gives the user an ability to share the results with his or her community.

Given the sensitivity of the information, it is imperative that the companies behind such devices are transparent about what information they collect, how the information will be used and with whom the data will be shared. In keeping with our Body as Information strategic priority—to promote respect for the privacy and integrity of the human body as the vessel of our most intimate personal information—our Office plans to complete an environmental scan of new health applications and digital health technologies being offered on the market, and to examine their privacy implications.

Based on our analysis of the results of the scan, GPEN Sweep results and further lab research, our Office plans to develop and provide guidance to the designers of these devices and associated applications—with a particular focus on small- and medium-sized enterprises and app developers—on how to build privacy protections into their new products and services. This work will also help to inform our education and outreach efforts to raise Canadians' awareness of the privacy risks associated with wearable devices.

Global Privacy Sweep: Our Office focuses on health technologies

It's estimated that some 170 million wearable sports and wireless health monitoring devices alone will be in use by 2017. This growth and the privacy concerns surrounding it prompted the Global Privacy Enforcement Network to focus on the Internet of Things during the Global Privacy Sweep which took place in April 2016. This year's theme dovetails with other initiatives by the Office in this emerging area.

The sweep involved a number of data protection authorities from around the world, including our Office along with our Alberta, British Columbia, Nova Scotia and Ontario counterparts. As part of this year's initiative, authorities gave special attention to the question of accountability, examining the privacy communications and practices related to Internet connected devices.

Participating authorities had the flexibility to choose a different category of products and

a preferred approach—some opted to sweep wearables or appliances; others looked at very specific items like smart meters, connected cars or smart TVs. Our Office focused on health devices, building on and complementing other initiatives already undertaken or planned related to our Body as Information strategic priority, and helping to promote compliance amongst developers and privacy awareness to users of these devices.

In addition to focusing on different types of devices, the various data and privacy authorities participating in the exercise approached the sweep from different angles. Some purchased products and assessed privacy communications right out of the box, even putting the products to use to get a first-hand look at what personal information is being collected and whether that coincided with what manufacturers or retailers said was being collected in their privacy communications. Others chose to examine the privacy information available through the manufacturer's website. In some instances, authorities could contact the manufacturer, retailer or data controller directly with specific privacy questions. In its examination of health devices, our Office used all three methodologies.

The goal of the Sweep was to increase public and business awareness of privacy rights and responsibilities, encourage compliance with privacy legislation, identify concerns that may be addressed through targeted education or enforcement and enhance cooperation among privacy enforcement authorities.

As of this report's writing, the Sweep findings were being compiled with the goal of being made public in the fall of 2016. As in years past, concerns identified may result in follow-up work such as outreach to organizations and/or enforcement action.

International and domestic dialogue on genetics

Privacy and data protection authorities around the world are wrestling with these and other privacy risks related to genetic testing. In October of 2015, for example, participants in the International Conference of Data Protection and Privacy Commissioners—including our Office—discussed the challenges arising from society's increasing ability to collect, analyze and use genetic information.

The conference recognized that while there are clearly many benefits that do and will continue to stem from genetic information, the collection and use of such information could lead to a variety of risks including discrimination or the denial of services on the basis of genetic predispositions. The conference concluded with a call for strong privacy safeguards, stating that it is crucial that individuals remain in control of their data, receive appropriate information about the options available to them and have their choices respected. This was regarded as particularly important in the case of genetic test results that can reveal highly sensitive information about individuals and their families.

The Association of Francophone Data Protection Authorities, of which our Office is a member, made a similar call for new safeguards to address these issues in June 2015, endorsing a Resolution on Genetic and Health Data.

Through its participation in international fora of this kind, its research, Parliamentary

activities and other outreach, our Office continues to identify and draw attention to the current and potential privacy challenges associated with genetic testing, as well as work with our counterpart agencies in Canada and elsewhere to propose ways to mitigate these risks—none of which were foreseen when existing privacy legislation was drafted. In the next fiscal year, we will be issuing a fact sheet on direct-to-consumer genetic testing in collaboration with our provincial colleagues, to inform individuals of the potential risks to their privacy, and provide guidance with regard to options for protecting themselves.

During 2015-2016, our Office continued its active involvement as an ex officio member of the National DNA Databank Advisory Committee. Much of the Committee's work this year involved the planned implementation of new indices relating to DNA profiles of human remains, victims, volunteers, missing persons and their relatives.

Proposed legislation on genetic discrimination

In February, the Commissioner appeared before the Standing Senate Committee on Human Rights as part of its examination of Bill S-201, an *Act to Prohibit and Prevent Genetic Discrimination*.

The Bill would impose a general prohibition on the collection of genetic test results as a requirement for providing goods or services—such as an insurance policy—or entering into a contract, and require written consent from individuals who wish to provide such information by choice.

Following the Commissioner's submission, Bill S-201 was amended to reflect our recommendation to ensure an individual's written consent would also be required for any proposed disclosure of their genetic test results. The Committee also accepted our recommendation against adding information derived from genetic testing to the definition of personal information in the *Privacy Act* and PIPEDA on the basis that such information is already encompassed.

The Bill passed the Senate on April 14, 2016 and was sent for debate in the House of Commons.

In conclusion

These are only some of the many challenges to be addressed if we are to protect the privacy and intimacy, of our bodies and minds from the growing risks posed by evolving technologies—such as wearables, biometrics, genomics, robotics and artificial intelligence—that enable the collection and use of our personal information in new and subtle ways.

Much like the issues of consent discussed in Chapter three, in this fast-changing environment, we must find answers to the questions posed by this new reality and determine what new tools are needed and how existing ones should be improved to help people reap the benefits of exciting new technologies while effectively managing their privacy risks.

Chapter 6:

The Year in Review

Throughout the year, this Office continued to carry out a wide range of other activities to protect and promote the privacy rights of individuals.

The work highlighted in the preceding chapters highlights issues and efforts directly related to our four strategic privacy priorities as well as the need to bring the *Privacy Act* into the 21st century. But there was a lot of other important work we undertook throughout 2015-2016. This chapter provides a summary and sampling of these other key activities.

Public education and outreach

Improving public education is critical to informing organizations about their privacy obligations and individuals about protecting their privacy rights and maintaining trust in the digital economy.

Over this past year, we have increased certain outreach initiatives within our existing resources. In particular, we have developed strategies aimed at youth, seniors and small businesses – groups which were identified during our priorities-setting exercise as those that would benefit from receiving more information about privacy issues.

Our awareness efforts through communications, public education and outreach involve a wide range of activities, including meetings with stakeholders, speaking engagements, exhibiting, and the development and dissemination of resource materials, often via our website.

In 2015-2016, for example:

- We delivered more than 100 speeches and presentations across Canada, engaging a wide variety of audiences and stakeholders—ranging from the University of Alberta Access and Privacy Conference, to the Countermeasure 2015 conference for information technology security professionals and the Digital Youth Summit.

- We also exhibited at some 40 other events to reach audiences identified through our priority setting exercise and engage with stakeholders.

- Our Toronto office – a regional presence that recognizes the significant number of businesses subject to PIPEDA headquartered there – continued to play a key role in stakeholder relations and outreach activities. Since January 2015, the team conducted 128 outreach and stakeholder relations activities and also generated new information products such as Ten Tips for Addressing Employee Snooping and Ten Tips for Services Aimed at Children and Youth.

Another important area of work for us was to bring significant enhancements to our website's content and usability to ensure Canadians and organizations can access clear, comprehensible and relevant information about privacy issues. Individuals and businesses have told us that when they need help with privacy issues, their very first source is the Internet and continuous improvement of our website will remain an ongoing priority.

In addition to web visits, Canadians and organizations contact us for privacy advice to the tune of some 9,000 inquiries per year. In 2015-2016, we created two new tools to help individuals reach our Office to raise questions and privacy concerns. A "smart" online form was launched for those who prefer to submit questions electronically. As well, we have a new privacy comment form that allows people to share concerns about privacy issues in order to help us to identify trends and to inform possible action.

As discussed above, we also began implementing multi-year communications and outreach strategies to better connect with and raise awareness among three key target audiences.

SMALL BUSINESS OUTREACH

Understanding that, in general, the smaller the business, the less likely it has in-house resources to advise on privacy matters, our Office is reaching out to smaller businesses across Canada to help raise awareness of their privacy obligations and provide related guidance and information.

To better understand small business information needs, we conducted focus groups with small business owners and employees in three Canadian cities, using the insights gained through that exercise to fine-tune our outreach work.

Members of our staff spoke with various small business audiences, reaching some 14,000 people during the past year. These presentations included a number of events organized with local chambers of commerce in cities throughout the country.

In addition to broad-based initiatives, our small business strategy also takes a sectoral approach, targeting sectors that have generated higher numbers of calls and complaints to our Office. For example, this work has involved efforts to build relationships and explore collaboration with key associations in the accommodations and retail sectors.

REACHING OUT TO YOUTH

Among our youth outreach activities, we developed an interactive online tool called "House Rules," to help parents learn more about their children's online activities and discuss ways to protect their privacy online.

We also created and distributed a classroom activity, inspired by the Sweeps discussed in this report, to schools across Canada to help teachers familiarize students with privacy policies and issues related to the collection of personal information online.

Global Privacy Sweep – focus on kids

The Office joined privacy authorities from close to two dozen other countries in conducting the third annual Global Privacy Enforcement Network (GPEN) Privacy Sweep in May of 2015, focused on

apps and websites that are targeted at or popular with children.

While there were some innovative examples of protective controls such as the use of pre-set usernames and avatars to prevent children from using their real names or photos, too many developers were found to be collecting particularly sensitive personal information from children—including photos, videos and location—and often allowing it to be posted publicly or shared with third parties, raising serious questions about the potential for harm to both reputation and well-being.

A number of specific examples illustrating the observations can be found in a blog post on our Office's website. In all, our Office Sweep team—which included several children—looked at 172 websites and apps. The young sweepers, who were accompanied by parents, shared their observations in a separate blog post.

CONNECTING WITH SENIORS

Our outreach strategy for seniors focuses on developing and sharing information and guidance to address issues of specific concern to this group, including for example identity theft, phishing and other online scams, as well as privacy issues related to social networking and the use of mobile devices.

Over the last year, we conducted two radio campaigns on privacy protection and identity theft; distributed our "Identity Theft and You" publication to libraries across Canada; and made presentations at a number of events for seniors, reaching some 45,000 people at events in various cities. Efforts to reach this important vulnerable group are ongoing.

Parliamentary activities

The Office provided input on a number of items of proposed legislation and other issues with potential impacts on privacy during the reporting period. We provided our views through a total of 20 written submissions to and/or appearances before committees of both the House of Commons and Senate. Among others, including Bills C-51, S-201 and *Privacy Act* reform, which are referenced in other chapters of this report, the Office provided comments on:

Bill C-26, the Tougher Penalties for Child Predators Act

In an appearance before the Senate Standing Committee on Legal and Constitutional Affairs in June 2015, we focused specifically on the general efficacy of the *Sex Offender Information Registration Act* (SOIRA) and the value of creating a High Risk Child Sex Offender Database that could be accessed by the public. The legislation was passed without amendments and received royal assent on June 18, 2015.

Bill C-377, An Act to Amend the Income Tax Act

Under this Bill, labour unions would be required to disclose their financial payments, names and salaries of staff, and political activities on a Canada Revenue Agency website. We noted a number of concerns in an appearance before the Senate Committee on Legal and Constitutional Affairs in May

2015. Among others, we found a provision to publicly associate the names of specific individuals with their political activities especially troubling from a privacy perspective. The Bill was enacted but, as of this writing, was in the process of being rescinded by the current Parliament.

Bill C-59, Economic Action Plan 2015, No. 1

In June 2015, at the invitation of the Senate Committee on National Finance, the Office submitted its views on parts of Bill C-59 that had a number of implications for privacy, including allowing the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) to disclose information to provincial bodies that administer securities legislation for investigative purposes, and expanding the collection of biometric information through the visa and immigration process. Our submission also addressed a clause in the Bill that would exempt Long-gun Registry records from the *Privacy Act*.

Audits

Under the *Privacy Act*, the Commissioner has the discretion to review the privacy practices of federal government institutions and recommend remedial actions when needed.

AUDITING PRIVACY IN THE OLD AGE SECURITY PROGRAM

Administering the Old Age Security (OAS) program involves the collection of significant amounts of sensitive personal information, from Social Insurance Numbers to financial information. In February 2015, our Office began an audit of the personal information handling practices of Employment and Social Development Canada (ESDC) for the OAS program. We also reviewed the role of Shared Services Canada (SSC) in safeguarding the information technology (IT) infrastructure on which OAS information resides.

In general, as detailed in the full audit report, while we found that ESDC has many elements of an effective privacy management regime, we identified a number of gaps and weaknesses in the implementation of some of its privacy and security policies and practices, including:

- The existing business arrangement between ESDC and SSC, which describes in general terms their ongoing business relationship, does not define the roles and responsibilities of the two departments with regard to the protection of OAS client information—which Treasury Board of Canada Secretariat (TBS) regards as an "essential element" of such agreements. Without a clear agreement defining how personal information will be protected, there is a risk that this information could be accessed, used or disclosed improperly. We recommended ESDC work with SSC to develop an agreement that includes the appropriate security and privacy provisions.

- We looked at a number of information sharing agreements (ISAs) ESDC has with its partners and found that some agreements were missing key privacy and security clauses. In this regard, we recommended that ESDC update its information sharing agreements using their newer ISA template, which contains clauses that would address those that were missing in our review.

- Neither the OAS systems managed by ESDC, nor the infrastructure where these systems reside has been certified or accredited as required—thus, potential privacy and IT security risks have not been fully assessed and mitigated. We recommended that ESDC assess the privacy and security risks of these systems through the certification and accreditation process, as required under TBS policy. We also recommended that ESDC work with SSC to ensure that the infrastructure undergoes the required assessments.

- ESDC has procedures to ensure only staff with a legitimate need to know can access personal information. We found that these were not followed consistently, nor was there proactive monitoring of when and by whom personal information was accessed within IT systems. In addition to adhering to its own procedures, we recommended ESDC review the audit trails produced by the IT systems of users' activities in the OAS systems on a regular basis.

- Hard copy versions of closed OAS client files were being retained beyond the six-year time limit set by ESDC policy. Electronic files are currently retained indefinitely, although the Department is implementing a retention and disposal schedule to allow the department to destroy these files. We recommended ESDC develop a plan for disposing records that have been retained beyond the six year time limit.

- Physical security controls at the facilities we visited were adequate for the storage of paper documents and ESDC is now tracking Threat and Risk Assessments (TRAs) to better manage the results from those assessments. The frequency of TRAs is not consistent at ESDC and there is also no centralized oversight in the Department to ensure physical security risks are assessed and mitigated in the same way across the country. We recommended that ESDC update its existing security policy to include how often TRAs should be conducted and that the Department develop a centralized oversight function.

ESDC has responded to our audit findings and agrees with all our recommendations. The Department has committed to specific actions and timelines to address our Office's findings. The full details of ESDC's response can be found in the audit report. While the focus of this audit was on ESDC's personal information management practices, during the audit, we also reviewed the gaps identified that relate to SSC.

The Office has no authority to enforce its recommendations, but we do follow up after two years to see what actions have been taken to address them.

Follow-up on past work

We followed up on our 2013 audit of the Canada Revenue Agency (CRA) to determine what actions the Agency has done to implement our recommendations and ensure that taxpayer information is as secure as it can be from inappropriate internal access, use or disclosure.

The CRA indicated that it has substantially or fully implemented all measures that we

recommended. The Agency reports that it has made several important improvements to its management of personal information, including introducing new policies, increasing corporate oversight and ensuring more timely assessment of privacy and security risks.

The Agency appointed a Chief Privacy Officer (CPO) in 2013 who is a member of the Agency Management Committee and has a broad mandate for privacy oversight and promotion. The CPO's role includes overseeing decisions related to privacy, including privacy impact assessments; championing personal privacy rights, including the management of privacy breaches; and overseeing privacy awareness, including communications and training activities for all Agency employees.

The Agency has also enhanced its information technology (IT) controls over taxpayer systems, including improved internal access rights management and monitoring. It also expects in 2017 to fully implement the monitoring controls recommended in our audit. To date the CRA has invested approximately $10.5 million and is planning a further significant investment to enhance its identity and access management controls. Finally, the CRA has improved its privacy breach procedures to support timelier reporting of incidents.

Privacy Impact Assessments

TBS directs federal government institutions to conduct Privacy Impact Assessments (PIAs) for new or substantially modified programs or activities that involve the use of personal information for decision-making purposes which affect individuals. Institutions provide copies of their PIAs to our Office. We review these submissions and, when warranted, advise the institution on privacy risks and ways to improve personal information-handling practices. While our recommendations are not binding, in most cases institutions do accept and implement our advice.

Some examples:

Royal Canadian Mounted Police – Body Worn Video

The RCMP is currently evaluating whether or not to implement a national program to have all members wear video cameras on their uniforms in the future. At present, body worn video cameras are being used on an occasional basis—usually at sites of protests and demonstrations where there are RCMP concerns about potential violence.

We continue to consult with the organization on this issue and have made recommendations encouraging the RCMP to be transparent in its use of body worn video technology, and to ensure its use is necessary and proportionate before being deployed in any particular situation. We expect to be kept fully apprised of developments in this program, including any contemplated use of facial recognition software or other video analytics.

Canada Revenue Agency information sharing with U.S. Internal Revenue Service

We raised a number of concerns with the Canada Revenue Agency (CRA) following our review of their PIA for the administration of the intergovernmental agreement (IGA) under the U.S.-based *Foreign Account Tax Compliance Act* (FATCA). The IGA covers the collection of personal information from Canadian financial institutions by the CRA related to reportable

accounts belonging to U.S. persons or entities and sending it to the U.S. Internal Revenue Service (IRS).

In our initial review, we noted the potential over-collection of personal information, concerns about the lack of clarity regarding the threshold for reporting accounts holding $50,000 or more, and what appeared to be an unnecessarily long 11-year retention period.

In response, the CRA agreed to shorten the retention period to seven years (in line with its retention of individual tax returns) and implementing a web form to ensure that financial institutions submit only the required information, to mitigate the risk of over-collection. The CRA also clarified provisions relating to the $50,000 threshold. The Agency specified that the *Income Tax Act* allows financial institutions to decide to apply the threshold, whereas the IGA allows institution to choose not to apply it. In short, this means that while institutions are technically required to report on all accounts, they may opt to apply the threshold in certain circumstances.

The CRA further informed us that while it performs validations of received records for completeness and consistency on a risk assessment basis, it does not have the required information to verify whether reportable accounts were appropriately identified. To facilitate individuals' access to their information and allow them to challenge when it may have been erroneously transferred, our Office has recommended that the CRA consider notifying impacted individuals upon their data being provided to the IRS.

Canadian Food Inspection Agency Mental Health Peer Support Program

In June 2015, the Canadian Food Inspection Agency (CFIA) launched a voluntary program connecting employees dealing with mental health challenges with colleagues who had successfully overcome similar challenges. While well-intentioned, the initiative raises a number of privacy issues and questions.

It was not clear from the PIA how peer supporters would protect participants' personal information and anonymity, or how the inappropriate disclosure of information would be prevented in practice. We recommended that the CFIA update its PIA to include, among other things, an assessment of whether the program's policies and procedures provide sufficient guidance to ensure compliance with the *Privacy Act*, and an assessment of technical safeguards and security controls to mitigate privacy risks.

The CFIA responded to our letter of recommendation and agreed to address most of our recommendations. However, the Agency continues to limit the PIA's scope to an examination of risks to the personal information of the peer supporters and not the participants. We continue to recommend that CFIA revise the PIA to include a more comprehensive analysis of the risks to the sensitive information shared by participants.

Complaints and investigations

PIPEDA INVESTIGATIONS

Over the last five years under PIPEDA, the number of complaints has risen with more cases being resolved through early resolution while treatment times have been lowered significantly.

Under the Act, from January 1, 2015 to March 31, 2016, we accepted 391 complaints. As noted in the Commissioner's Message, a 2015 legislative amendment changed PIPEDA's reporting period interval from calendar year to fiscal year. For the purposes of a comparison, in calendar year 2015, we accepted 309 complaints, an increase of 49% from five years ago, in 2010, when we accepted 207.

In 2015, we closed 171 files through early resolution, more than double the 80 concluded this way in 2010. Meanwhile, 133 were closed by standard investigation, less than half the 249 closed this way in 2010. Meanwhile, the average treatment time for files closed through early resolution has been brought down from three months in 2010 to 2.7 in 2015, while that for standard investigation dropped substantially from 19.2 months in 2010 to 12.2 in 2015.

While the preceding chapters featured key investigations, under PIPEDA, we are able to share details of cases outside of reports to Parliament, and frequently add new ones to our website throughout the year at: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/

PRIVACY ACT INVESTIGATIONS

The volume of complaints received under the *Privacy Act* over the last five years has grown, amidst new technology and the integration of government programs that generate a higher level of sharing of Canadians' information increasing the complexity of investigations. The Office has increased its use of early resolution and implemented strategies to deal with the receipt of multiple complaints as a result of single incidents, and single individuals submitting multiple complaints. These have led to greater efficiencies enabling redress for thousands of Canadians each year. However, we are getting to a point in which we are unable to keep pace with demand.

In 2015-2016, we accepted 1,768 complaints under the *Privacy Act*, compared with 3,977 recorded a year earlier. But when we exclude complaints made by individuals who submitted multiple complaints (which under our multiple complaints strategy are held in abeyance, enabling us to more equitably serve the needs of a broader range of complainants), the number—which is more representative of our work-load—actually rose from 1,040 to 1,389 complaints. Compared to five years ago, in 2010-2011, *Privacy Act* complaints have increased by 96%.

Our use of early resolution has increased significantly over the past five years. In 2015-2016, our Office closed 1,226 files under the *Privacy Act*, including 460 through early resolution. These totals represent major increases from 2010-2011, when 648 files were closed (up 89% over five years) with only 78 by early resolution (up 489% over five years). The average treatment time for files closed by early resolution has also been reduced over the past five years, from 3.6 to 2.2 months.

However, when it comes to cases closed by standard investigation, partly owing to a steadily increasing inventory of more complex files, the average treatment time has risen from eight to just over 10 months.

As noted in Chapter 1, our Office is unable to share details of investigations under the *Privacy Act* outside of reports to Parliament. Summaries of examples from the past year follow. The full versions of these and other investigation reports may be found here on the OPC website.

TV show raises numerous questions of consent

Since 2012, the Canada Border Services Agency (CBSA) was featured in a weekly TV program called, "*Border Security: Canada's Front Line.*" The program followed the work of CBSA officers, most often as they interviewed travelers taken aside for secondary screening. Before filming would begin, individuals were asked by a CBSA officer for permission to be filmed. When filming finished—assuming individuals had provided verbal consent—the production company then asked them to sign a consent form, giving permission for the footage to be used on the show and waiving their rights under the *Privacy Act*. Those who did not sign had their faces blurred.

Our investigation examined both the filming of a complainant who was detained during a CBSA raid of a Vancouver-area construction site in 2012, as well as issues affecting the show more broadly. In concluding our investigation, we identified a number of privacy concerns—the most serious of which related to consent:

- As the CBSA permitted the production company to access customs controlled areas to film operational activities, there was a real-time disclosure of personal information by the Agency to the production company. For such a disclosure to respect the *Privacy Act,* the CBSA needed to obtain valid and meaningful consent from individuals.

- We were unsatisfied that the CBSA was obtaining such consent. There are many factors, including duress, impacting the validity of consent, which must be given freely, on a voluntary basis and with an appreciation of the related consequences. Due to the coercive nature of being detained, individuals may not have had a clear frame of mind to provide truly voluntary consent.

- In reviewing the raw footage involving the complainant—and contrary to the CBSA's submission—we found that filming began before any effort to obtain consent was made. The complainant was asked several questions by the CBSA officer before being advised of the filming's purpose.

- While the complainant later signed a consent form, we found no evidence that he or others were made fully aware of the significance of waiving their *Privacy Act* rights, or given an opportunity to seek independent legal advice prior to signing.

- We also raised concerns with the blurring techniques used to conceal individuals' identities. The treatment level most often used was weak and there was usually an abundance of secondary information, providing a serious possibility that individuals could be identified.

In concluding our investigation, we reminded the CBSA that privacy protection must be a core consideration in the initial development and administration of these types of initiatives. In response to our findings and recommendations, the CBSA ended its involvement in the program. The Agency also noted our recommendation that it conduct a Privacy Impact Assessment before pursuing a television show in the future.

Canada Revenue Agency takes adequate measures to ensure personal information not moved to U.S.

Once our personal information leaves Canada—whether it's been moved by a federal institution, a private organization, or even if we've transferred it ourselves—the laws of the country in which the information resides will then apply. Those laws will determine who can obtain access to that personal information. In some cases, foreign laws may allow access to our personal information in situations or for uses that many of us might find objectionable in comparison with Canadian privacy law.

The complainant in this case was concerned that the Canada Revenue Agency (CRA) outsourced storage of Canadians' tax records to a company he believed was based in the U.S. If that were the case, U.S. authorities could gain access to the personal information of Canadian taxpayers under the USA PATRIOT Act.

In May 2013, CRA awarded a contract for storage and management of Canadians' tax records to "Mobilshred Inc., operating as Recall." In discussions with the CRA and with Mobilshred corporate officers, we determined that Mobilshred Inc. is 100% owned by Recall Canada Holdings, a Canadian entity, which is in turn 100% owned by Recall's parent company, Recall Holdings Limited, which is based in Australia. We noted that Mobilshred Inc. does not have any facilities located in the U.S.

Based on our investigation, we are of the view that the CRA took appropriate steps to guard against potential disclosure of Canadians' tax information to U.S. authorities. Among others, its contract with Mobilshred includes a requirement that all information transferred to the company—all in paper format—remain in Canada at all times.

We also note that, prior to awarding the contract, to ensure issues of privacy and security were fully considered and effectively addressed—including the implications of the USA PATRIOT Act—the CRA consulted its Access to Information and Privacy Directorate, as well as our Office and the Department of Justice.

Canada Post collection of online signatures for mail tracking draws complaint

Canada Post routinely collects electronic signatures from people when they accept an item for which the sender has requested proof of delivery. As long as the recipient does not object, his or her signature is posted on the Canada Post website, where the sender of the package can view it by typing in the tracking number of the item in question.

In this case, the complainant alleged that Canada Post was not doing enough to ensure recipients of a package understood they could refuse to have their signature posted online (in which case the sender could request a paper copy). The electronic signature devices used by

Canada Post have a label that says, "I agree my signature may be viewed online."

Following our review, we found that the disclosure of the signature for the purpose of parcel tracking is consistent with the purpose for which it was collected by Canada Post. Consequently, there is no requirement for Canada Post to obtain consent to disclose the signature – even on the online tracking website. While we raised concerns that the wording of the label on the signature devices may not be sufficiently clear, Canada Post was of the view that the procedure for customers to opt-out of having their signature displayed online is upfront and understood, and did not agree to modify the wording of the label in this case. This did not, in our view, render Canada Post in contravention of the Act.

However, our investigation also examined Canada Post's online tracking tool. Following our review of the security and privacy controls implemented to protect the digitized signatures displayed online, we were not satisfied that Canada Post had adequately considered the risks in the current functionality and design of the site to adequately safeguard addressees' signatures.

As a result, Canada Post committed to strengthening its online tracking website, including implementing the more secure HTTPS protocol to mitigate the overall risk to privacy. We found this aspect of our investigation to be conditionally-resolved. Canada Post will keep our Office informed of its progress in the implementation of the controls identified.

Mishandling employees' personal information

Each year, the Office receives a number of complaints about federal institutions that have allowed employees' personal information to be accessed or disclosed improperly. Some examples:

- A failure by the Parole Board of Canada (PBC) to examine documents carefully led to the personal medical information of an employee being disclosed to a number of people who were to participate in a hearing on a staffing issue. We noted that, in its request for background on the appointment process, the Public Service Staffing Tribunal (now amalgamated within the Public Service Labour Relations and Employment Board) advised the PBC that personal information, including "medical/health information" was to be removed from any documents before they were sent to the Tribunal.

- An employee at what was then known as Public Works and Government Services Canada complained that a manager against whom she had filed a harassment complaint had shared this fact in a staff meeting with individuals who had no need to know this information. In sharing this news, the manager was disclosing her own personal information, but also disclosing sensitive personal information belonging to the employee. A reminder that individuals involved in recourse proceedings must be advised that these matters should be treated with utmost discretion.

- During an RCMP data entry training exercise, employees were given a variety of information to enter into a system that tracks complaints of harassment in the workplace. The information included the names, ranks, addresses and contact information of the complainants, a description of the alleged harassment, and the names of others involved. One of the trainees realized that the information was not generic, as she expected, but were actual cases. Our investigation found that, in order to help ease a backlog of information that needed to be entered into the system, the RCMP Superintendent in charge of the training session decided to use real data for the training—in the process, disclosing the sensitive personal information of dozens of employees.

Data breaches

DATA BREACH REPORTING UNDER THE *PRIVACY ACT*: ANOTHER RISE IN REPORTS

Breach reports to our Office are growing year over year, particularly since 2014 when government reporting of material breaches was deemed mandatory under Treasury Board policy. Unfortunately, with no corresponding rise in funding for these activities, our ability to effectively deal with breaches has been limited. At this time, we are only able to cursorily review, advise and follow up on all but a few of the breach reports we receive.

In 2015-2016, breach reports rose 16 per cent to 298 from 256 in the previous reporting period. As in years before, "accidental disclosure" was the most common cause cited for breaches, highlighting the need for institutions to ensure proper procedures are in place to protect Canadians' personal information.

Without question, the change to mandatory reporting through administrative directive has led to improvement. But there are still some institutions not submitting breach reports. Of the breaches reported last year, most were reported by a handful of organizations. As shown in Appendix 2, several of those with vast amounts of personal information holdings reported very few.

Further questions were raised about the consistency of breach reporting among federal institutions in April 2016 by information tabled in the House of Commons in response to a question from a Member of Parliament. The response showed there were more than 5,800 breaches recorded in 2015-2016, with just over 5% of those reported to our Office.

In responding to questions on the matter, we noted that many of the breaches did not necessarily involve personal information or would not likely include such sensitive data as to be considered "material" breaches. As such, in those circumstances, the incidents would therefore not need to be reported under Treasury Board policy.

As discussed in Chapter one, placing a specific legal obligation for reporting "material" privacy breaches would however provide our Office with a clearer picture of the situation across federal institutions, and better position us to work with organizations to help mitigate the risks and impacts.

DATA BREACH REPORTING UNDER PIPEDA AND IMPLEMENTING THE *DIGITAL PRIVACY ACT*

The past year saw a sharp increase in voluntary data breach reports submitted to our Office by organizations covered by PIPEDA. For calendar year 2015, we received 98, more than double the 44 received in 2014.

The increased reporting may be a sign that companies are preparing for a new reality. In the near future, the reporting—to Canadians and our Office—of breaches posing a real risk of significant harm to individuals will be mandatory.

This change stems from the passage of the *Digital Privacy Act* (Bill S-4) in June 2015. While the mandatory breach reporting regime will not come into effect until regulations are drafted by Innovation, Science and Economic Development Canada, other changes came into force immediately. All changes are outlined in a fact sheet we published in 2015.

International and domestic cooperation

Our Office continued its long tradition of promoting privacy rights and knowledge internationally with ongoing participation in a variety of fora and with counterpart agencies around the world. Specific activities this past year included contributions to working papers published by the International Working Group on Data Protection in Telecommunications, including the Working Paper on Transparency Reporting and the Working Paper on Wearable Computing Devices, both of which were published in April of 2015.

INTERNATIONAL CONFERENCE OF DATA PROTECTION COMMISSIONERS – RESOLUTION ON TRANSPARENCY

During the International Conference of Data Protection Commissioners (ICDPC) held in Amsterdam in October 2015, our international counterparts supported a resolution on the subject of transparency (co-sponsored with our New Zealand counterpart) on the part of telecommunication service providers on requests they receive for personal information from government institutions.

The resolution urges private organizations to publish transparency reports on the number of requests they receive, the nature of their responses, and the legal basis on which government institutions request access to personal information of their customers and employees. It also calls on governments to maintain accurate records and to report publicly on the nature, purpose and number of lawful access requests they make and to remove hurdles to transparency reporting.

In addition to the transparency reporting resolution, the Conference led to resolutions: pledging cooperation with the United Nations' Special Rapporteur on the Right to Privacy; and supporting necessary analysis and guidance with regard to privacy and international humanitarian action, such as efforts to assist persons displaced by situations of violence and natural disasters.

LEADERSHIP AND PARTICIPATION IN INTERNATIONAL FORA

Throughout the year, our Office continued in our role as a new member of the Executive Committee of the International Data

Protection and Privacy Commissioners' Conference.

We also continued to co-chair the Common Thread Network, which in a November 2015 statement, urged privacy to be given greater priority by the Commonwealth Heads of Government, recognizing this group's potential to supplement global value in the field of privacy and data protection. The Heads of Government, in their communiqué following their meeting later that month, "recognised the need to adopt legal frameworks that promote privacy rights" and "resolved to encourage the development of practical networks that facilitate the sharing of information and building of capacity" in privacy and data protection.

Our Office also participated in the Asia Pacific Privacy Authorities (APPA) group, which in June 2015 held its 43rd forum in Hong Kong and in December 2015 held its 44th forum in Macao; along with *l'Association Francophone des autorités de protection des données personnelles* (AFAPDP), which adopted resolutions on mass surveillance and, as noted in chapter five, the ethical use of health and genetic data.

"BRING YOUR OWN DEVICE" GUIDANCE

We also work closely with our provincial and territorial partners, engaging in regular and ongoing consultation. This past year for example, we collaborated with the Alberta and British Columbia Information and Privacy Commissioners to develop and publish guidelines for organizations considering whether to join the growing trend toward "Bring Your Own Device"—BYOD.

While expanding, the practice of having employees use their own devices blurs the lines between professional and personal lives. Employees are becoming concerned that their privacy is at risk, not to mention issues associated with the collection and use of consumers' personal information that may end up residing on employees' personal mobile phones and other devices.

Contributions program

Created in 2004 to support independent, non-profit research on privacy, further privacy policy development, and promote the protection of personal information in Canada, the Contributions Program is considered one of the foremost privacy research funding programs in the world.

The Office issues an annual call for proposals and in some years an additional special call for Pathways to Privacy knowledge translation projects based on previously completed research. The program, recently renewed by the Government of Canada for another five years, has an annual budget of $500,000. A maximum of $50,000 can be awarded to any single project.

The Program has contributed to the advancement of our strategic priorities by continuing to move towards innovative solutions to new and emerging privacy issues. Projects selected for funding and other Contributions Program announcements are posted on our website. This year saw the successful completion of nine projects directly related to our Office's strategic privacy priorities and the selection of 10 applications for the 2016-2017 funding year. As well, a

number of recent projects were detailed in the latest edition of our Real Results publication.

In the Courts

In the past year our Office appeared on interventions or applications in a number of cases:

Fontaine et al v. Canada
Our Office was granted leave to intervene by the Ontario Court of Appeal last year and appeared in court in appeals and cross-appeals related to the protection, archiving and eventual disposal of records created as part of the Independent Assessment Process (IAP) under the Indian Residential Schools Settlement Agreement (IRSSA). Without taking a formal position on the merits, our Office questioned whether the level of privacy protection offered by federal privacy and access legislation was compatible with the near to absolute confidentiality negotiated by the parties under the Agreement. Our Office also offered submissions concerning the relevant considerations for assessing whether the IAP records are under government control and underlined the importance of survivors of residential schools retaining control over their individual stories.

A majority of the Court held that the IAP records are not under government control and therefore not subject to the *Privacy Act*, the *Access to Information Act*, or the *Library and Archives of Canada Act*. The majority also upheld as reasonable the order that the documents be destroyed after a 15-year retention period and clarified that during this period; the documents are subject to the confidentiality provisions of the IRSSA but are not subject to federal privacy and access legislation.

This has important implications in view of past and potential complaints to our Office about the treatment of IAP records by the IAP Secretariat. An application for leave to appeal this decision has now been filed with the Supreme Court of Canada (SCC).

The Information and Privacy Commissioner of Alberta v. The Board of Governors of the University of Calgary
Our Office, with the Office of the Information Commissioner and several other provincial and territorial information and privacy commissioners intervened jointly in a case heard before the SCC on April 1, 2016. The case concerns the Alberta Privacy Commissioner's ability to obtain records, over which a public body— in this case, a university—claims solicitor-client privilege under Alberta's *Freedom of Information and Protection of Privacy Act*.

At issue was what kind of language is required to allow an officer, such as the Privacy Commissioner, to override solicitor-client privilege for the purposes of reviewing a claim. The language in question is very similar to that employed in the *Privacy Act*, which says, in part, "Notwithstanding any other Act of Parliament or any privilege under the law of evidence, the Privacy Commissioner may, during the investigation of any complaint under this Act, examine any information recorded in any form under the control of a government institution, other than a confidence of the Queen's Privy Council for Canada."

At the time of this report's writing no decision had yet been released

Royal Bank of Canada v. X et al

While not a party to the matter, our Office participated in a hearing before the Ontario Court of Appeal as a "friend of the Court," and was then asked to participate in the same role in a subsequent appeal to the SCC. At issue in the appeal, (that was heard in April 2016), is whether PIPEDA prevents a creditor from obtaining a mortgage pay-out statement from a third-party lender to the debtor to pursue a legal remedy to enforce a judgment. The majority of the Ontario Court of Appeal held that PIPEDA prevents the disclosure in such circumstances without consent and that implied consent was not sufficient.

X v. Canada (CANADIAN TRANSPORTATION AGENCY) ET AL.

In June 2015, the Federal Court of Appeal released a decision in a case relating to the open court principle as it applies to an administrative tribunal and the concept of "publicly available" personal information under the *Privacy Act*. Our Office had status as an intervenor.

The Court found that the open court principle applies to the Canadian Transportation Agency (CTA) in its function as a quasi-judicial tribunal and that its regulations clearly stipulated that the CTA "shall place on its public record any document filed with it in respect of any proceeding," unless a request for confidentiality had been made. The Court held that the materials the Applicant had requested had been placed on the CTA's public record as required by its rules and that all of those documents were therefore "publicly available" within the meaning of the *Privacy Act*. As such, the CTA was ordered to disclose the unredacted documents as requested by the Applicant.

While this decision applied to the CTA, our Office continues to encourage administrative tribunals, each with their different rules, powers and responsibilities, to adopt policies that, while respecting the open court principle and the specificities of their enabling legislation, also respect their privacy obligations under the *Privacy Act*.

X v Attorney General of Canada

The Office was granted leave to intervene last year in an Application to the Federal Court for judicial review of a report of findings issued by our Office in a complaint against the Canada Revenue Agency (CRA). The Applicant is challenging both the fairness of our investigation as well as the conclusions reached in the report.

X v. Privacy Commissioner of Canada

The Federal Court was asked for a judicial review of our findings related to a complaint filed against a federal department under the *Privacy Act*. The Applicant argued that our report of findings contained errors and that our Office did not provide her with sufficient opportunity to present her case, did not conduct a thorough investigation, and was biased in investigating her complaint.

The Court dismissed the application, noting that our investigation was thorough and fair. The ruling confirmed that our Office "should have broad latitude in determining how to run its own investigation," that its investigations and reasons provided for its findings "need not be perfect, but rather must be reasonable."

X and GLOBE24H.com

This is an application brought pursuant to section 14 of PIPEDA against the website Globe24h.com following the release of the OPC's report of findings (featured in our 2014 PIPEDA annual report) concerning the site. The applicant is one of the 27 complainants whose complaints the OPC investigated. This applicant is seeking broad relief against Globe24h.com including damages and an order for the site to delete all court and tribunal decisions on its servers and take steps to remove them from search engine caches.

In March 2016, the Federal Court permitted our Office to participate in the proceedings to inform on the application of PIPEDA. This proceeding raises issues including the extent to which PIPEDA applies to a foreign-based website; the meaning of "publicly available" information as defined in the Act, the interpretation of the "journalistic purpose" exemption, and the restriction in s.5(3) of the Act regarding appropriate purposes.

Appendix 1 – Definitions

Complaint Types

Access: The institution/organization is alleged to have denied one or more individuals access to their personal information as requested through a formal access request.

Correction/Notation (access): The institution/organization 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: In a request under the *Privacy Act,* personal information is alleged to have not been provided in the Official Language of choice.

Fee: The institution/organization is alleged to have inappropriately requested fees in an access to personal information request.

Index: *Info Source* (a federal government directory that describes each institution and the information banks – 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.

Accuracy: The institution/organization is alleged to have failed to take all reasonable steps to ensure that personal information that is used is accurate, up-to-date and complete.

Collection: The institution/organization is alleged to have collected personal information that is not necessary, or has collected it by unfair or unlawful means.

Retention (and disposal): The institution/organization is alleged to have failed to keep personal information in accordance with the relevant retention period: either destroyed too soon or kept too long.

Use and disclosure: The institution/organization is alleged to have used or disclosed personal information without the consent of the individual or outside permissible uses and disclosures allowed in legislation.

Time limits: Under the *Privacy Act*, the institution is alleged to have not responded within the statutory limits.

Extension notice: Under the *Privacy Act*, 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 limit): Under the *Privacy Act*, 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.

Accountability: Under PIPEDA, an organization has failed to exercise responsibility for personal information in its possession or custody, or has failed to identify an individual responsible for overseeing its compliance with the *Act.*

Challenging compliance: Under PIPEDA, an organization has failed to put procedures or policies in place that allow an individual to challenge its compliance with the *Act,* or has failed to follow its own procedures and policies.

Consent: Under PIPEDA, an organization has collected, used or disclosed personal information without valid consent, or has made the provisions of a good or service conditional on individuals consenting to an unreasonable collection, use, or disclosure.

Openness: Under PIPEDA, an organization has failed to make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Safeguards: Under PIPEDA, an organization has failed to protect personal information with appropriate security safeguard.

Identifying purposes: Under PIPEDA, an organization has failed to identify the purposes for which personal information is collected at or before the time the information is collected.

Dispositions

Well-founded: The institution/organization contravened a provision(s) of the privacy legislation.

Well-founded, resolved: The institution/organization contravened a provision of the privacy legislation but has since taken corrective measures to resolve the issue to the satisfaction of the OPC.

Well-founded and conditionally resolved: The institution/organization contravened a provision of the privacy legislation. The institution/organization committed to implementing satisfactory corrective actions as agreed to by the OPC.

Not well-founded: There was no or insufficient evidence to conclude the institution/organization contravened the privacy legislation.

Resolved: Under the *Privacy Act,* the investigation revealed that the complaint is essentially a result of a miscommunication, misunderstanding, etc., between parties; and/or the institution agreed to take measures to rectify the problem to the satisfaction of OPC.

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

Discontinued:

> **Under the *Privacy Act*:** The investigation was terminated before all the allegations were fully investigated. A case may be discontinued for various reasons, but not at the OPC's behest. 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.
>
> **Under PIPEDA:** The investigation was discontinued without issuing a finding. An investigation may be discontinued at the Commissioner's discretion for the reasons set out in subsection 12.2(1) of PIPEDA.

No jurisdiction: It was determined that federal privacy legislation did not apply to the institution/organization, or to the complaint's subject matter. As a result, no report is issued.

Early Resolved: Applied to situations in which the issue is resolved to the satisfaction of the complainant early in the investigation process and the Office did not issue a finding.

Declined to investigate: Under PIPEDA, the Commissioner declined to commence an investigation in respect of a complaint because the Commissioner was of the view that the complainant ought first to exhaust grievance or review procedures otherwise reasonably available; the complaint could be more appropriately dealt with by means of another procedure provided for under the laws of Canada or of a province; or, the complaint was not filed within a reasonable period after the day on which the subject matter of the complaint arose, as set out in subsection 12(1) of *PIPEDA.*

Withdrawn: Under PIPEDA, the complainant voluntarily withdrew the complaint or could no longer be practicably reached. The Commissioner does not issue a report.

Appendix 2 – Statistical Tables

PIPEDA (January 1, 2015 – March 31, 2016) complaints accepted by industry sector

Sector	Number	Proportion of all complaints accepted
Accommodations	15	4%
Entertainment	4	1%
Financial	57	15%
Government	11	3%
Insurance	32	8%
Internet	83	22%
Not for profit	1	0%
Other sectors	34	9%
Professionals	6	2%
Sales/retail	28	7%
Services	38	10%
Telecommunications	46	12%
Transportation	26	7%
Total	381	100%

PIPEDA (January 1, 2015 – March 31, 2016) complaints accepted by complaint type

Complaint type	Number	Proportion of all complaints accepted
Access	79	21%
Accountability	4	1%
Accuracy	7	2%
Appropriate purposes	9	2%
Collection	20	5%
Consent	124	33%
Correction/notation	9	2%
Openness	2	1%
Retention	5	1%
Safeguards	39	10%
Use and disclosure	83	22%
Grand total	381	100%

PIPEDA (January 1, 2015 – March 31, 2016) investigations closed by industry sector and disposition

Sector category	Early resolution (ER)	Dispositions (not ER)									Subtotal of dispositions not ER	Total early resolution and other dispositions
		Declined	Discontinued (under 12.2)	No Jurisdiction	Withdrawn	Settled	Not well-founded	Well-founded	Well-founded resolved	Well-founded conditionally resolved		
Financial	28		1		5		10		10	4	30	58
Government	7					1					1	8
Not for profit	1										0	1
Transportation	12	1			1	1	2		5	2	12	24
Telecommunications	41				2		2	1	4	1	10	51
Services	19	1			1				1	1	4	23
Internet	34		3		4	1		2	2		12	46
Other sectors	36	2	3		2	1	1		3		12	48
Insurance	12	1	4	4	3	1	2		1	2	18	30
Sales/retail	22		1		3	2		2	4	2	14	36
Accommodations	9			1	1		1		1		4	13
Professionals	6							1	2		3	9
Entertainment	3								1		1	4
Total	230	5	12	5	22	7	18	6	34	12	121	351

PIPEDA (January 1, 2015 – March 31, 2016) - investigations closed by complaint type and disposition

Complaint type	Early resolution	Discontinued (under 12.2)	Declined	No Jurisdiction	Withdrawn	Settled	Not well-founded	Well-founded	Well-founded resolved	Well-founded conditionally resolved	Total
Access	45	3	2	1	5	1	2	1	11	2	73
Use and Disclosure	53	6		2	1		3	4	10	6	85
Collection	19		1	2	4	2	2		3	1	34
Appropriate purposes	3	1			2		1				7
Safeguards	27		2		4	1	2		2	2	40
Consent	66	2			6	1	7	1	8	1	92
Accuracy	3						1				4
Retention	5										5
Accountability	1					2					3
Correction/notation	6										6
Openness	2										2
Fees											0
Total	230	12	5	5	22	7	18	6	34	12	351

PIPEDA (January 1, 2015 – March 31, 2016) investigations average treatment times by disposition

Disposition	Number	Average treatment time in months
ER-resolved	230	2.9
Settled	7	5.4
Discontinued (under 12.2)	12	9.6
Withdrawn	22	15.3
No jurisdiction	5	2.1
Not well-founded	18	14.0
Well-founded conditionally resolved	12	23.0
Well-founded resolved	34	16.1
Well-founded	6	14.8
Declined to investigate	5	4.2
Total cases	351	
Overall weighted average		**6.7**

PIPEDA (January 1, 2015 – March 31, 2016) investigations average treatment times by complaint and resolution types

	Early resolution		All other resolutions (not ER)		All investigations	
Complaint Type	Number of cases	Average treatment time in months	Number of cases	Average treatment time in months	Number of cases	Average treatment time in months
Access	45	3.0	28	11.2	73	6.1
Accountability	1	5.3	2	4.3	3	4.6
Accuracy	3	2.8	1	19.3	4	6.9
Appropriate purposes	3	2.4	4	10.6	7	7.1
Collection	19	3.2	15	13.8	34	7.9
Consent	66	2.8	26	14.6	92	6.1
Correction/notation	6	1.1			6	1.1
Openness	2	2.8			2	2.8
Retention	5	3.4			5	3.4
Safeguards	27	2.9	13	10.2	40	5.3
Use and disclosure	53	3.0	32	13.2	85	6.8
Grand total	**230**	**2.9**	**121**	**12.6**	**351**	**6.7**

PIPEDA (January 1, 2015 – March 31, 2016) voluntary breach notifications - by industry sector and type of incident

	Incident type				
Sector	Accidental disclosure	Loss	Theft and unauthorized access	**Total incidents per sector**	**% of total incidents**
Accommodation			2	2	2%
Entertainment	1		1	2	2%
Financial	17	1	13	31	27%
Health	6		2	8	7%
Government			1	1	1%
Insurance	1		4	5	4%
Internet			3	3	3%
Not for profit organizations	3		4	7	6%
Other sectors	1		10	11	10%
Sales/retail	2	1	16	19	17%
Services	4	2	8	14	12%
Telecommunications	7		2	9	8%
Transportation	1		2	3	3%
Grand Total	**43**	**4**	**68**	**115**	100%

***Privacy Act* dispositions of access and privacy complaints by institution**

Respondent	Well-founded	Well-founded resolved	Not well-founded	Resolved	Discontinued	ER-resolved	Settled	Total
Bank of Canada						1		1
Canada Border Services Agency		2	11	1	3	32		49
Canada Post Corporation			5		4	12		21
Canada Revenue Agency	11	5	9	1	57	12		95
Canada School of Public Service				2		1		3
Canadian Air Transport Security Authority							1	1
Canadian Broadcasting Corporation			9			3		12
Canadian Cultural Property Export Review Board		1						1
Canadian Food Inspection Agency			1			2		3
Canadian Heritage						1		1
Canadian Human Rights Commission			1					1
Canadian Institutes of Health Research						1		1
Canadian Nuclear Safety Commission	1							1
Canadian Radio-television and Telecommunications Commission						2		2
Canadian Security Intelligence Service			16			6	3	25
Canadian Transportation Agency						1		1
Communications Security Establishment			1	1				2
Correctional Service Canada	9	12	14	3	13	87	3	141
Department of National Defence			19	1	5	18	1	44
Elections Canada			1		1	8		10
Employment and Social Development Canada	2		6	1		24	1	34
Environment and Climate Change Canada			1			4		5
Fisheries and Oceans Canada	1				1	2		4
Global Affairs Canada			1			7		8
Health Canada		2	22	1	2	13		40
Immigration and Refugee Board			1			3		4
Immigration, Refugees and Citizenship Canada	1	1	5		2	20		29
Indigenous and Northern Affairs Canada	1							1
Infrastructure Canada		1						1
Innovation, Science and Economic Development Canada			3			4		7
Justice Canada	1	3	4		7	10		25

***Privacy Act* dispositions of access and privacy complaints by institution (cont.)**

Respondent	Well-founded	Well-founded resolved	Not well-founded	Resolved	Discontinued	ER-resolved	Settled	Total
National Battlefields Commission								0
National Research Council of Canada			1					1
Natural Resources Canada						2		2
Office of the Commissioner of Lobbying of Canada						1		1
Office of the Commissioner of Official Languages						2		2
Office of the Information Commissioner of Canada			1					1
Office of the Privacy Commissioner of Canada			1					1
Office of the Procurement Ombudsman			1					1
Parole Board of Canada	1		4		1	6		12
Passport Canada	1		1			1		3
Privy Council Office						10		10
Public Health Agency of Canada						3		3
Public Prosecution Service		1	2			1		4
Public Safety Canada						2		2
Public Sector Integrity Commissioner of Canada	1		4					5
Public Service Commission of Canada	1	4	1		2			8
Public Services and Procurement Canada	1	1			1	8	1	12
Royal Canadian Mounted Police	6	6	19	1	16	58	1	107
Security Intelligence Review Committee						2		2
Service Canada					1	4		5
Statistics Canada				1	1	2		4
Sustainable Development Technology Canada						1		1
Transport Canada		2				7		9
Treasury Board of Canada Secretariat						8		8
Veterans Affairs Canada		2	1			6		9
VIA Rail Canada					1			1
Grand total	**38**	**43**	**166**	**13**	**118**	**398**	**11**	**787**

***Privacy Act* treatment times - early resolution cases by complaint type**

Complaint type	Count	Average treatment time (months)
Access		
Access	255	2.38
Correction – notation	2	3.87
Language	1	1.49
Time Limits		
Time limits	61	1.10
Correction – time limits		
Extension notice	1	0.40
Privacy		
Use and disclosure	113	2.45
Collection	16	1.86
Retention and disposal	7	1.56
Accuracy	4	3.75
Grand total	**460**	**2.21**

***Privacy Act* treatment times - standard investigations by complaint type**

Complaint type	Count	Average treatment time (months)
Access		
Access*	160	18.74
Correction-notation	1	17.27
Time limits		
Time limits	323	4.82
Correction - TL	2	2.78
Extension notice	52	3.15
Privacy		
Use and disclosure*	71	17.78
Collection	10	16.54
Retention and disposal	7	14.96
Accuracy	2	12.25
Grand total	**628**	**10.03**

* Includes 1 representative complaint for each of several series of related complaints; excluded complaints total 138.

***Privacy Act* treatment times - all closed files by disposition**

Complaint type	Count	Average treatment time (months)
Standard complaints*		
Well-founded*	319	5.98
Not well-founded	176	13.07
Discontinued	69	9.15
Well-founded resolved	41	24.32
Settled	9	25.67
Resolved	14	15.21
ER-resolved	460	2.21
Grand total	**1088**	**6.70**

* Includes 1 representative complaint for each of several series of related complaints; excluded complaints total 138.

***Privacy Act* breaches by institution**

Respondent	Incident
Canada Border Services Agency	1
Canada Revenue Agency	21
Canadian Air Transport Security Authority	1
Canadian Environmental Assessment Agency	1
Canadian Human Rights Commission	1
Canadian Museum of History	1
Canadian Security Intelligence Service	1
Communications Security Establishment	2
Correctional Service Canada	50
Elections Canada	3
Employment and Social Development Canada	17
Environment and Climate Change Canada	1
Fisheries and Oceans Canada	4
Global Affairs Canada	7
Health Canada	2
Immigration, Refugees and Citizenship Canada	47
Indigenous and Northern Affairs Canada	9
Justice Canada	3
Military Grievances External Review Committee	1
Department of National Defence	1
Office of the Information Commissioner of Canada	1
Public Prosecution Service of Canada	5
Public Service Commission Canada	10
Public Services and Procurement Canada	4
Royal Canadian Mounted Police	12
Statistics Canada	4
Transport Canada	3
Veterans Affairs Canada	84
VIA Rail Canada	1
Grand total	**298**

***Privacy Act* complaints**

Category	Total
Accepted	
Access	418
Time limits	478
Privacy	493
Total accepted and active	**1389**
Total accepted and in abeyance	379
Closed through early resolution	
Access	258
Time limits	62
Privacy	140
Total	**460**
Closed through standard investigation	
Access	210
Time limits	377
Privacy	179
Total	**766**
Total closed	**1226**
Breaches received	
Accidental disclosure	242
Theft	5
Loss	29
Unauthorized access	22
Total received	**298**

Privacy Act* complaints accepted by complaint type

Complaint type	Early resolution		Investigation		Total count	Total percentage
	Count	Percentage	Count	Percentage		
Access						
Access	299	55%	104	12%	403	29%
Correction - notation	5	1%	1	0%	6	0%
Language	9	2%	0	0%	9	1%
Time limits						
Time limits	55	10%	352	42%	407	29%
Extension	1	0%	66	8%	67	5%
Correction - time limits	0	0%	4	0%	4	0%
Privacy						
Use and disclosure	132	24%	97	11%	229	17%
Collection	25	5%	220	26%	245	18%
Retention and disposal	10	2%	5	1%	15	1%
Accuracy	4	1%	0	0%	4	0%
Grand total	540	100%	849	100%	1389	100%

* Does not include complaints in abeyance (379)

Privacy Act top 10 institutions by complaint accepted

Respondent	Access		Time limits		Privacy		Grand total
	Early resolution	Investigation	Early resolution	Investigation	Early resolution	Investigation	
Correctional Services Canada	94	12	34	178	21	208	547
Royal Canadian mounted Police	48	9	4	34	15	10	120
Canada Border Services Agency	34	12	3	29	7	3	88
Canada Revenue Agency	9	8	0	15	10	43	85
National Defence	11	12	3	40	6	5	77
Public Service Commission	0	5	0	60	0	9	74
Immigration, Refugees and Citizenship	13	4	0	11	10	6	44
Employment and Social Development Canada	14	1	4	5	15	3	42
Canadian Security Intelligence Service	8	16	4	0	0	3	31
Environment and Climate Change	11	0	0	10	1	0	22
Treasury Board of Canada Secretariat	7	1	0	9	0	5	22
Grand total	**249**	**80**	**52**	**391**	**85**	**295**	**1152**

Privacy Act top 10 institutions by complaints accepted and fiscal year

Organization	2012-13	2013-14	2014-15	2015-16
Correctional Service Canada	284	514	314	547
Royal Canadian Mounted Police	182	265	140	120
Canada Border Services Agency	88	56	66	88
Canada Revenue Agency	76	61	106	85
Department of National Defence	90	84	68	77
Public Service Commission of Canada	3	6	2	74
Immigration, Refugees and Citizenship Canada	17	53	42	44
Employment and Social Development Canada	1030	78	35	42
Canadian Security Intelligence Service	19	17	21	31
Environment and Climate Change Canada	2	1	7	22
Treasury Board of Canada Secretariat	2	1	3	22
Grand total	**1793**	**1136**	**804**	**1152**

***Privacy Act* complaints accepted by institution**

Respondent	Early resolution	Investigation	Grand total
Bank of Canada	1	0	1
Canada Border Services Agency	44	44	88
Canada Post Corporation	11	6	17
Canada Revenue Agency	19	66	85
Canada School of Public Service	0	2	2
Canadian Broadcasting Corporation	3	1	4
Canadian Food Inspection Agency	2	1	3
Canadian Heritage	1	0	1
Canadian Human Rights Tribunal	0	1	1
Canadian Institutes of Health Research	2	0	2
Canadian Radio-television and Telecommunications Commission	1	1	2
Canadian Security Intelligence Service	12	19	31
Canadian Transportation Agency	1	0	1
Correctional Service Canada	150	397	547
Department of National Defence	20	57	77
Elections Canada	8	2	10
Employment and Social Development Canada	33	9	42
Environment and Climate Change Canada	12	10	22
Finance Canada	0	1	1
Fisheries and Oceans Canada	3	2	5
Freshwater Fish Marketing Corporation	0	1	1
Global Affairs Canada	8	4	12
Health Canada	13	0	13
Immigration and Refugee Board	5	0	5
Immigration, Refugees and Citizenship Canada	23	21	44
Indigenous and Northern Affairs Canada	0	10	10
Innovation, Science and Economic Development Canada	3	0	3
Justice Canada	8	9	17
Library and Archives Canada	2	0	2
National Battlefields Commission	0	1	1

***Privacy Act* complaints accepted by institution (cont.)**

Respondent	Early resolution	Investigation	Grand total
Natural Resources Canada	2	10	12
Office of the Commissioner of Official Languages	1	0	1
Office of the Privacy Commissioner of Canada	0	1	1
Office of the Superintendent of Financial Institutions	1	0	1
Parks Canada	3	0	3
Parole Board of Canada	11	7	18
Passport Canada	1	0	1
Privy Council Office	2	9	11
Public Health Agency of Canada	5	0	5
Public Prosecution Service of Canada	0	3	3
Public Safety Canada	2	1	3
Public Sector Integrity Commissioner of Canada	0	1	1
Public Service Commission of Canada	1	73	74
Public Services and Procurement Canada	9	3	12
Royal Canadian Mounted Police	67	53	120
Security Intelligence Review Committee	4	0	4
Service Canada	8	3	11
Shared Services Canada	0	1	1
Social Sciences and Humanities Research Council	0	1	1
Standards Council of Canada	1	0	1
Statistics Canada	4	1	5
Sustainable Development Technology Canada	1	1	2
Transport Canada	10	4	14
Treasury Board of Canada Secretariat	7	15	22
Veterans Affairs Canada	8	4	12
Grand total	533	856	1389

***Privacy Act* complaints accepted by province/territory**

Province/territory	Early resolution		Investigation		Total count	Total percentage
	Count	Percentage	Count	Percentage		
Alberta	49	3.53%	24	1.73%	73	5.26%
British Columbia	100	7.20%	89	6.41%	189	13.61%
Manitoba	10	0.72%	20	1.44%	30	2.16%
New Brunswick	21	1.51%	29	2.09%	50	3.60%
Newfoundland and Labrador	2	0.14%	5	0.36%	7	0.50%
Northwest Territories	0	0.00%	0	0.00%	0	0.00%
Not specified	7	0.50%	1	0.07%	8	0.58%
Nova Scotia	9	0.65%	21	1.51%	30	2.16%
Nunavut	1	0.07%	0	0.00%	1	0.07%
Ontario	193	13.89%	456	32.83%	649	46.72%
Other (not US)	5	0.36%	2	0.14%	7	0.50%
Prince Edward Island	1	0.07%	1	0.07%	2	0.14%
Quebec	121	8.71%	165	11.88%	286	20.59%
Saskatchewan	15	1.08%	31	2.23%	46	3.31%
United States	5	0.36%	1	0.07%	6	0.43%
Yukon	0	0.00%	1	0.07%	1	0.07%
Blank	1	0.07%	3	0.22%	4	0.29%
Grand total	540	38.88%	849	61.12%	1389	100.00%

***Privacy Act* dispositions by complaint type**

Complaint type	Well-founded	Well-founded resolved	Not well-founded	Resolved	Discontinued	ER-resolved	Settled	Grand total
Access								
Access	6	43	101	12	39	255	8	464
Correction - notation				1		2		3
Language						1		1
Time limits								
Time limits	280		29	2	12	61		384
Extension	10		31		11	1		53
Correction - time limits	2							2
Privacy								
Use and disclosure	32		55		70	113	2	272
Collection			5		5	16	1	27
Retention and disposal	1		5		1	7		14
Accuracy					2	4		6
Grand total	**331**	**43**	**226**	**15**	**140**	**460**	**11**	**1226**

***Privacy Act* dispositions of time limits by institution**

Respondent	Well-founded	Well-founded resolved	Not well-founded	Resolved	Discontinued	ER-resolved	Grand total
Canada Border Services Agency	17		1			3	21
Canada Post Corporation	1						1
Canada Revenue Agency	8		1				9
Canadian Heritage						1	1
Canadian Institutes of Health Research						1	1
Canadian Security Intelligence Service						4	4
Correctional Service Canada	168		2	1	3	38	212
Department of National Defence	29		2		2	3	36
Employment and Social Development Canada	4					4	8
Environment and Climate Change Canada	3		6				9
Fisheries and Oceans Canada	2		2		2		6
Global Affairs Canada	2				1		3
Immigration, Refugees and Citizenship Canada	9		1	1	1		12
Justice Canada	1		1				2
National Battlefields Commission	1						1
Natural Resources Canada	7		1				8
Parole Board of Canada	2		2			2	6
Privy Council Office			1				1
Public Prosecution Service			1				1
Public Sector Integrity Commissioner of Canada	1						1
Public Service Commission of Canada	3		36		13		52
Public Services and Procurement Canada	3						3
Royal Canadian Mounted Police	24		1			6	31
Transport Canada	2						2
Treasury Board of Canada Secretariat	5		1				6
Veterans Affairs Canada	1		1				2
Grand total	293		60	2	22	62	439

Appendix 3 – Investigation Processes

Privacy Act Investigation Process

Intake

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

Complaint?

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

Yes:
An investigator is assigned to the case.

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

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

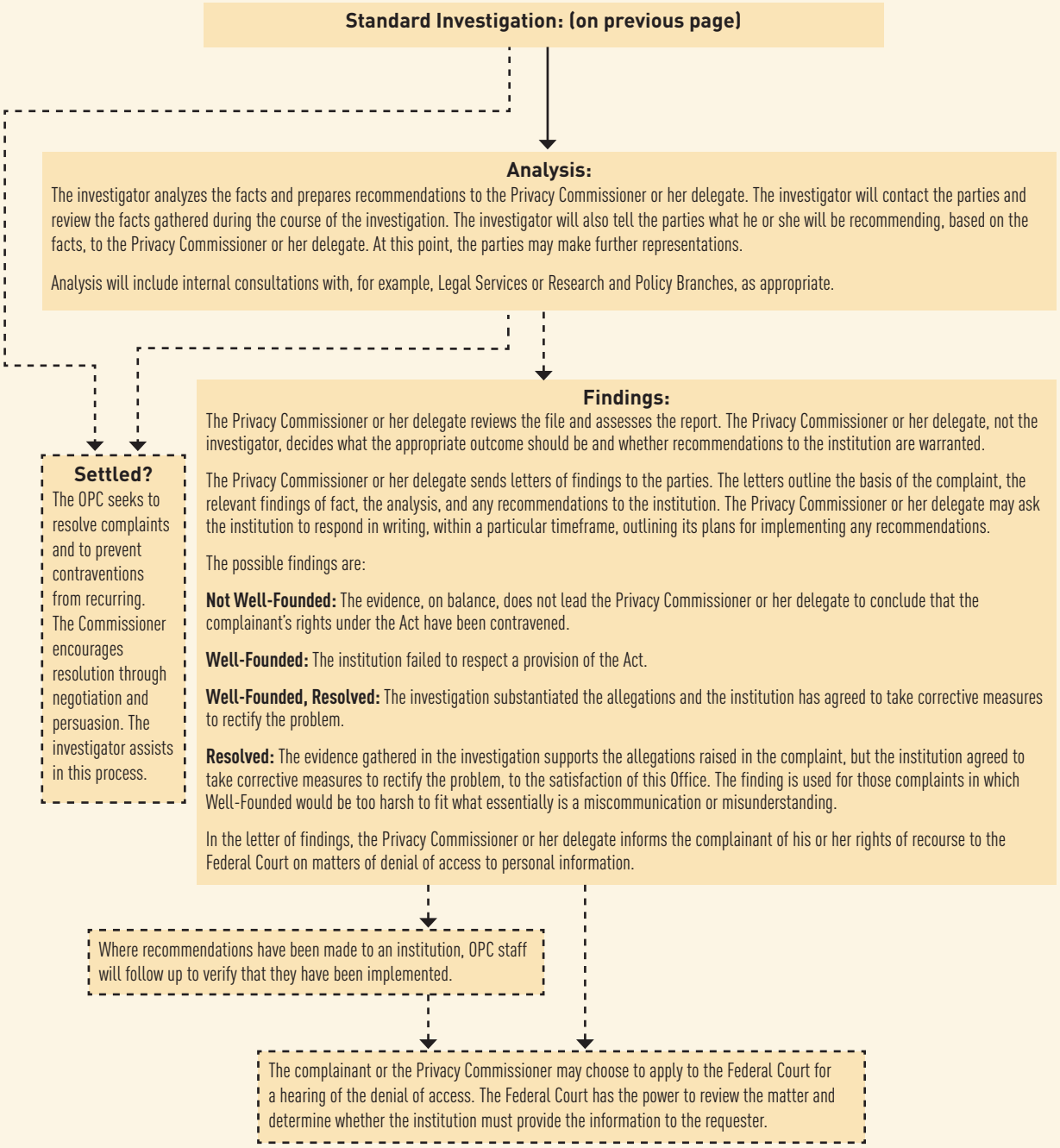
The investigator writes to the institution, outlining the substance of the complaint. The investigator gathers the facts related to the complaint through representations from both parties and through independent inquiry, interviews of witnesses, and review of documentation. Through the Privacy Commissioner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

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

Analysis (on next page)

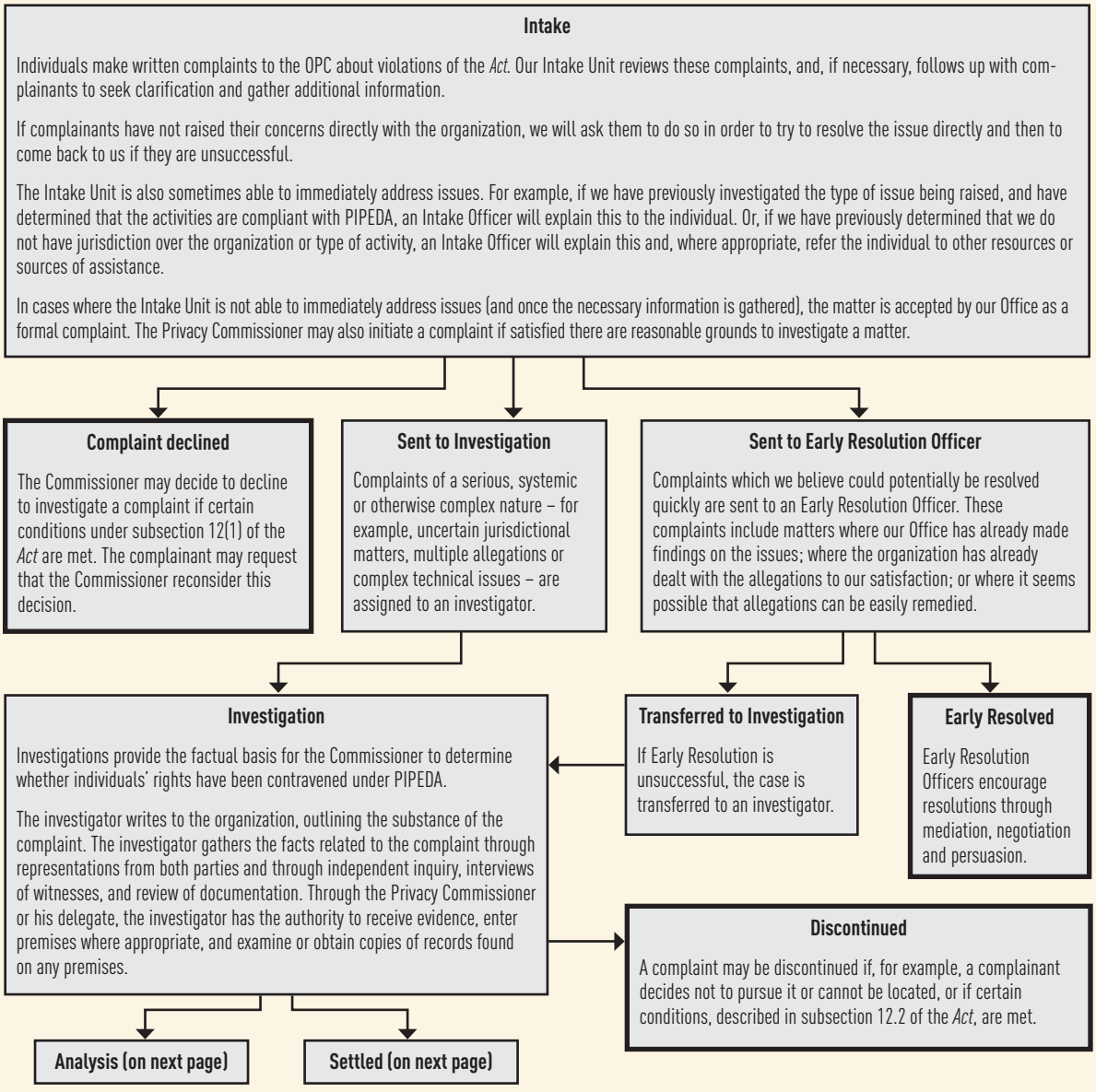
Settled? (on next page)

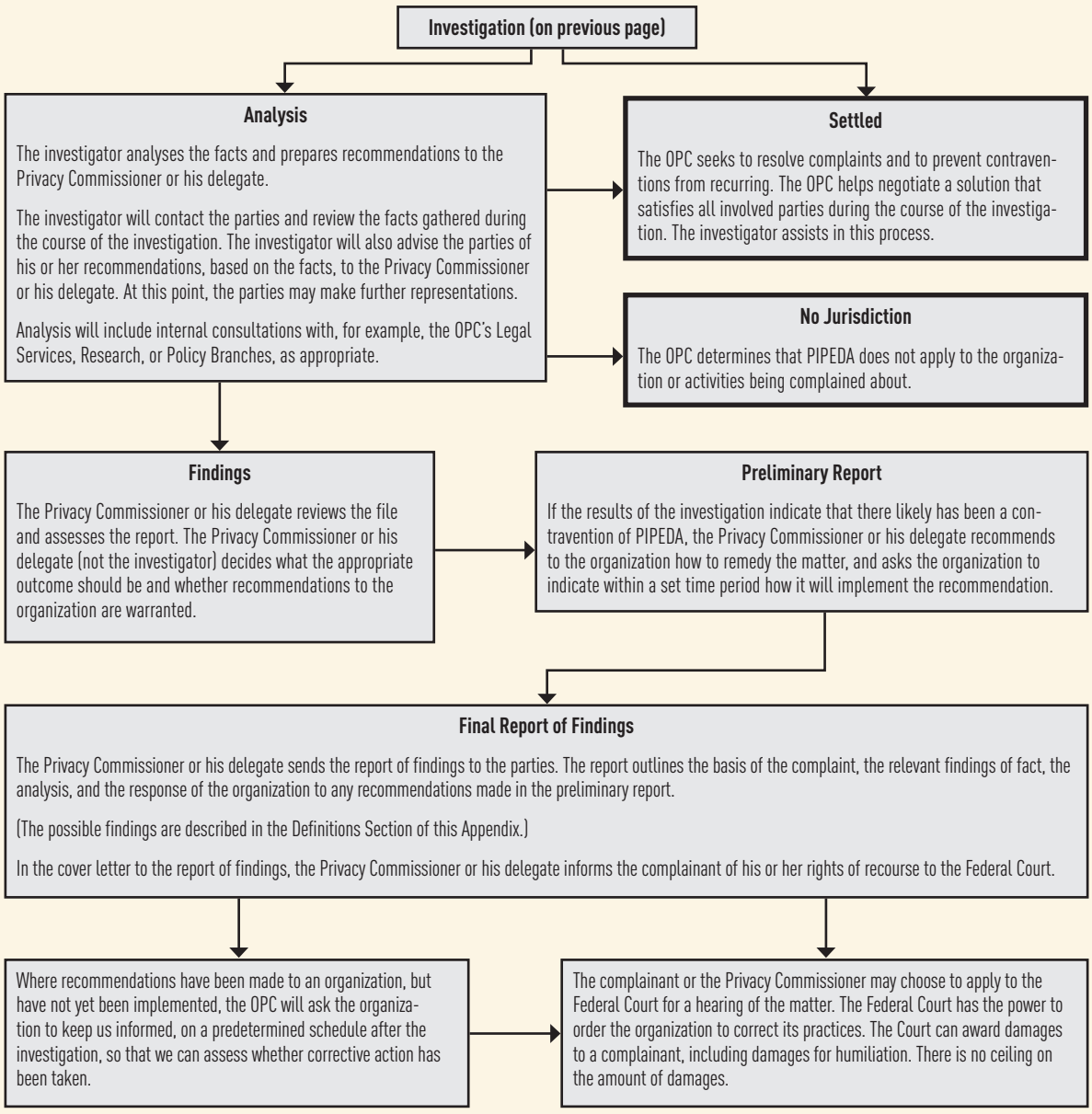
Note: a broken line (- - - -) indicates a *possible* outcome.



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

PIPEDA Investigation Process




Investigation (on previous page)
Analysis
The investigator analyses the facts and prepares recommendations to the Privacy Commissioner or his delegate.
The investigator will contact the parties and review the facts gathered during the course of the investigation. The investigator will also advise the parties of his or her recommendations, based on the facts, to the Privacy Commissioner or his delegate. At this point, the parties may make further representations.
Analysis will include internal consultations with, for example, the OPC's Legal Services, Research, or Policy Branches, as appropriate.
Settled
The OPC seeks to resolve complaints and to prevent contraventions from recurring. The OPC helps negotiate a solution that satisfies all involved parties during the course of the investigation. The investigator assists in this process.
No Jurisdiction
The OPC determines that PIPEDA does not apply to the organization or activities being complained about.
Findings
The Privacy Commissioner or his delegate reviews the file and assesses the report. The Privacy Commissioner or his delegate (not the investigator) decides what the appropriate outcome should be and whether recommendations to the organization are warranted.
Preliminary Report
If the results of the investigation indicate that there likely has been a contravention of PIPEDA, the Privacy Commissioner or his delegate recommends to the organization how to remedy the matter, and asks the organization to indicate within a set time period how it will implement the recommendation.
Final Report of Findings
The Privacy Commissioner or his delegate sends the report of findings to the parties. The report outlines the basis of the complaint, the relevant findings of fact, the analysis, and the response of the organization to any recommendations made in the preliminary report.
(The possible findings are described in the Definitions Section of this Appendix.)
In the cover letter to the report of findings, the Privacy Commissioner or his delegate informs the complainant of his or her rights of recourse to the Federal Court.
Where recommendations have been made to an organization, but have not yet been implemented, the OPC will ask the organization to keep us informed, on a predetermined schedule after the investigation, so that we can assess whether corrective action has been taken.
The complainant or the Privacy Commissioner may choose to apply to the Federal Court for a hearing of the matter. The Federal Court has the power to order the organization to correct its practices. The Court can award damages to a complainant, including damages for humiliation. There is no ceiling on the amount of damages.

Appendix 4

– Report of the Privacy Commissioner, Ad Hoc

Report of the Privacy Commissioner, Ad Hoc, for 2015-16

It is my pleasure to report here on the activities of the Office of the Privacy Commissioner, Ad Hoc. On April 1, 2007, the Office of the Privacy Commissioner (OPC) became subject to the *Privacy Act* (Act). This means that a privacy request can be made to the OPC as an institution to which the right of access to personal information applies.

The law that brought this about did not, however, create a mechanism separate from the OPC, which oversees government compliance with privacy requests, to investigate any complaints that privacy requests to the OPC have not been handled as the Act requires. Since it is a fundamental principle of the privacy law that decisions on the disclosure of government information should be reviewed independently, the office of an independent Privacy Commissioner, Ad Hoc was created and given the authority to investigate any such complaints about the OPC as an institution under the Act.

The Privacy Commissioner has for this reason delegated the majority of his powers, duties and functions to me as set out in sections 29 through 35 and section 42 of the Act in order to enable me to investigate complaints lodged against the OPC under the Act.

OUTSTANDING COMPLAINTS FROM PREVIOUS YEAR

Our office had two outstanding complaints from the previous year. These two complaints had been made as a result of the loss of a portable hard drive in 2014 by the OPC during its move to its new office in Gatineau. The first complaint revolved around the retention period of the personal information contained on the lost hard drive and the second revolved around the failure to protect the personal information under the control of the OPC. The first complaint was not well-founded and the second was well-founded. These complaints were the subject of a report by my predecessor as Privacy Commissioner, Ad Hoc, John Sims QC. That report was made public during this reporting year. It is further discussed later in this report.

NEW COMPLAINTS THIS YEAR

Twenty-six complaints were received this year. Twenty-five were investigated and disposed of by the end of fiscal year, while the remaining one will be dealt with this year.

The central issue in the twenty-six complaints, as well as in another complaint mentioned, concerned the proper application of paragraph 22.1(1) of the Act. This paragraph exempts from disclosure information obtained or created in the course of an investigation by the OPC. Once the investigation and all related proceedings are finally concluded, however, the exemption is partially lifted. At that point, the exemption no longer applies to documents created during the investigation.

In each case, our investigation revealed that the disputed documents had been obtained during the course of the OPC's own investigations. I therefore found that the OPC properly applied the mandatory exemption in refusing to disclose the requested documents. In addition, in some of these cases, the OPC had also applied exemptions pursuant to section 26 (personal information) and section 27 (solicitor-client privilege).

Most of these complaints were found to be not well-founded, and one complaint was abandoned by the complainant. In one case where section 26 was applied, the OPC agreed to release additional information and this case was closed as resolved.

In addition to these twenty-six complaints, my Office also received two letters from an individual who was dissatisfied with how the RCMP was handling the individual's requests for access to information. This office does not have jurisdiction to investigate concerns about how the RCMP handles such requests. I therefore invited the individual to write to the OPC about these complaints against the RCMP.

SPECIAL REPORT INTO THE LOST HARD DRIVE BY THE OPC

My predecessor, John Sims QC, investigated the OPC's loss of a hard drive. During the OPC's move to its new office in Gatineau in 2014, a portable hard drive containing personal information about the staff of both the OPC and of the Office of the Information Commissioner (OIC) was lost. This occurred sometime between February 13, 2014 and March 20, 2014.

The portable hard drive served to back up the financial system used by the OPC and OIC to manage and forecast employee salaries. It therefore contained financial information of current and former OPC and OIC staff from 2002 until February 13, 2014. Approximately 800 people were potentially affected by the loss.

Amongst his findings, Mr. Sims concluded that the portable hard drive had not been properly recorded and tracked as an asset, the information on the portable hard drive was retained longer than recommended, and certain OPC and Treasury Board policies were not followed. There was no evidence that any of the personal information contained on the missing hard had been disclosed or used improperly. Mr. Sims made a number of recommendations to the OPC, which were accepted. Some of his recommendations had already been implemented before the conclusion of the investigation.

CONCLUSION

The existence of an independent Commissioner, Ad Hoc helps to ensure the integrity of the OPC's handling of access requests made to it, as an institution, and therefore contributes to the health of the overall system of access to personal information at the federal level. My Office looks forward to continuing to play this part in access to personal information.

June 1, 2016

David Loukidelis QC
Privacy Commissioner, Ad Hoc for the
Office of the Privacy Commissioner of Canada