



Office of the  
Privacy Commissioner  
of Canada

## 2016–17 Annual Report to Parliament

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



## REAL FEARS, REAL SOLUTIONS

A plan for restoring confidence  
in Canada's privacy regime

2016-17 Annual Report to Parliament on the  
*Personal Information Protection and Electronic Documents Act* and the *Privacy Act*

**Real fears, real solutions: A plan for restoring confidence in Canada's privacy regime**

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

© Her Majesty the Queen of Canada for the Office of the Privacy Commissioner of Canada, 2017  
Cat. No.: IP51-1E-PDF  
ISSN: 1913-3367

Follow us on Twitter: @PrivacyPrivee  
Facebook: <https://www.facebook.com/PrivCanada/>

**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



The Honourable George J. Furey, Senator  
Speaker of the Senate  
The Senate  
Ottawa, Ontario  
K1A 0A4

September 2017

Dear Mr. Speaker:

I have the honour of submitting to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Personal Information Protection and Electronic Documents Act* and the *Privacy Act* for the period from April 1, 2016 to March 31, 2017.

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



---

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

September 2017

Dear Mr. Speaker:

I have the honour of submitting to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Personal Information Protection and Electronic Documents Act* and the *Privacy Act* for the period from April 1, 2016 to March 31, 2017.

Sincerely,  
*Original signed by*

Daniel Therrien  
Privacy Commissioner of Canada

---

# Table of Contents

Commissioner's message .....	1
Privacy by the numbers .....	9
<i>The Personal Information Protection and Electronic Documents Act</i>	
– A year in review .....	11
Report on consent .....	11
PIPEDA study .....	36
Proactive work in support of privacy: Helping Canadians exercise their rights and educating organizations about their obligations .....	39
Investigations under PIPEDA .....	44
PIPEDA in the courts .....	51
<i>The Privacy Act—a year in review</i> .....	53
Privacy Act reform .....	53
National security, public safety, borders and privacy .....	54
Investigations under the <i>Privacy Act</i> .....	68
Audits and Reviews .....	74
Privacy impact assessments .....	76
Public interest disclosures .....	79
Privacy Act related parliamentary appearances .....	80
Privacy Act cases in the courts .....	82
Appendix 1—Definitions .....	84
Appendix 2—Statistical tables .....	87
PIPEDA statistics .....	87
Statistical tables related to the <i>Privacy Act</i> .....	94
Appendix 3—Investigation processes .....	108
PIPEDA investigation process .....	108
Privacy Act investigation process .....	110
Appendix 4—Report of the Privacy Commissioner, Ad Hoc, for 2016–17 .....	112





## Commissioner's message

The digital revolution, which many have described as the 4<sup>th</sup> industrial revolution, has brought important benefits to individuals, from ease of communications to greater accessibility of information, products and services that make our lives better materially and intellectually. It is and will continue to be a major contributor of economic growth. However, it is also a cause of great concern. First among these concerns, undoubtedly, is the fear of losing our jobs. Another concern is the fear of losing our privacy, and consequently our inherent right to live and develop as autonomous human beings. Polls consistently show that an overwhelming majority of Canadians (more than 90%) are concerned about their privacy.

The development of technology, which overall is a positive thing, will not take place in a sustainable manner unless the fears of citizens are addressed with concrete and robust solutions. When we held consultations, Canadians told us that when it comes to privacy, they want better information to exercise individual control over their personal information, but they also expect better government protection, because they feel government has more knowledge and better tools to ensure privacy is protected.

I agree with Canadians. In my view, the solutions required to address their concerns should, of course, include better information to empower them to exercise

individual control and personal autonomy. But that is not enough. Individuals must be at the centre of privacy protection; however, stronger support mechanisms are also required. This includes among other things, independent regulators, such as my Office, with appropriate powers and resources giving them a real capacity to guide industry, hold it accountable, inform citizens and meaningfully sanction inappropriate conduct.

With that preface, it is my pleasure to present my Office's 2016-2017 Annual Report to Parliament. This report will cover both the *Privacy Act*, which applies to the personal information handling practices of government departments and agencies, and the *Personal Information Protection and Electronic Documents Act* (PIPEDA), Canada's federal private sector privacy law.

As was the case when I presented my last Annual Report, the swift evolution of technology—big data, the Internet of Things, biometrics and artificial intelligence, among other innovations—is continuing to have a tremendous impact

on personal privacy. It is becoming increasingly difficult for individuals to fully comprehend, let alone control, how and for what purposes organizations collect, use and disclose their personal information.

My Office has been carefully studying this phenomenon, and the need to modernize our privacy regime has never been more apparent or pressing.

Though technology neutral, Canada's laws were adopted in a much different era when routine, predictable, transparent one-on-one interactions between organizations and individuals were the norm. This is no longer the case in an age where computer algorithms and massive databases drive the economy and open the door to attractive new opportunities for federal institutions and private sector organizations. According to our latest public opinion poll released in January, 92 per cent of Canadians expressed concern about the protection of their privacy and a clear majority (57%) were very concerned.

This is certainly troubling. Something must change or we run the risk that Canadians will lose trust in the digital economy, thus hindering its growth and they may not enjoy all the benefits afforded by innovation. More fundamentally, it is quite unhealthy in a democracy when most citizens fear one of their basic rights is routinely not respected.

In the last year, we have taken a number of concrete steps to address this issue. We have put forward recommendations on *Privacy Act* reform, Canada's national security framework and, with this report, the role of consent under the federal private sector privacy law. This report details that work and more, and sets a new course for the future of privacy protection in Canada.

### **Consent consultation and PIPEDA reform**

Consent has long been considered a foundational element of PIPEDA. It is the chief mechanism by which individuals are able to express their autonomy and exercise control over their personal information. Legally, organizations must obtain consent to collect, use and disclose an individual's personal information, subject to a list of very specific exceptions. But obtaining meaningful consent has become increasingly challenging in the digital age where data has become ubiquitous, commodified and may be processed by multiple players totally unbeknownst to the individual to whom the data belongs.

For this reason, my Office published a discussion paper in May 2016 exploring the practicability of the current consent model under PIPEDA, whether it needs to change and who should be responsible for which changes—organizations, individuals, regulators or legislators.

We received more than 50 written submissions from businesses, civil society, academics, lawyers, regulators and individuals. We also held five stakeholder roundtables across Canada, as well as a series of focus groups with individual Canadians in four cities. After many months analyzing the feedback, we are pleased to unveil our conclusions as part of this year's annual report.

To begin, we heard how utterly powerless individuals feel in the digital marketplace when it comes to controlling how their personal information is collected and used by companies. Consumers are befuddled by incomprehensible privacy policies, yet feel compelled to consent if they are to obtain the goods or services they desire. Some group participants even said that with the information provided, they are “never” really able to give informed consent.

Still, there was also broad agreement that consent should continue to play a prominent role in privacy



protection. After much deliberation, we have presented a number of actions and recommendations intended to make consent more meaningful but also, because consent is not always sufficient as a privacy protection tool, to strengthen the roles of organizations and regulators. Where data-driven practices are likely to make consent impracticable, we have proposed alternatives.

For instance, to make consent more meaningful, we will update our guidance on online consent to specify four key elements that must be highlighted in privacy notices and explained in a user-friendly way. We will also inform individuals of existing consent tools and other privacy enhancing technologies that may assist them in having their preferences respected. We will further draft new guidance for businesses on no-go zones where the use of personal information, even with consent, should be prohibited as inappropriate.

We concluded individuals should not be expected to shoulder the heaviest burden when it comes to deconstructing complex data flows in order to make informed decisions on whether or not to provide consent.

Organizations must also be more transparent and accountable for their privacy practices. Because they know their business best, it is only right that we expect them to find effective ways, within their own specific context, to protect the privacy of their clients, notably by integrating approaches such as Privacy by Design. We will continue, in the course of investigations, to ask organizations to demonstrate how they comply with PIPEDA's accountability principle, and we will ask Parliament to augment our authority to enforce that principle proactively. We will also adapt our current accountability framework to the needs of small-and medium-sized businesses.

Meanwhile regulators, such as my Office, are well positioned to play a strong role in terms of education and guidance. During our consultations, we were

consistently asked to provide more guidance to individuals on how to exercise their privacy rights and to organizations on how to respect their obligations.

This has prompted us to become more citizen-focused. We have already overhauled our website to make it easier to navigate, and are developing new tips sheets and guidance we hope are easier to digest and include concrete advice for people and organizations.

Going forward, we will continue to issue guidance on as many important privacy issues as possible, and will assist industry in developing codes of practice. We will begin by revising our guidance on online consent, but our goal is to provide information on approximately 30 topics within four years. We want to be assessed on how useful our guidance is for individuals and organizations.

In terms of public education, the most effective strategy may well be to teach children about privacy at an early age. We therefore urge provincial and territorial governments to integrate privacy education into school curricula.

We acknowledge that there is a need to encourage innovation and that personal information is an important part of a data-driven economy. In some instances, however, the complexity of the technology, and the uses of personal information and their consequences can pose a real challenge to meaningful consent. To address these realities, we will issue guidance on how to de-identify personal information in a privacy-protective manner. We also encourage Parliament to follow up on a recommendation from private sector stakeholders to address the definition of "publicly available information" for which consent is not required, and to consider whether new exceptions to obtaining consent may be appropriate where consent is simply not possible or practicable.

Search engine indexing websites and big data analytics are just two examples where the volume and

velocity of information collection and use may make consent impracticable. A few industry representatives recommended that Canada adopt the concept of “legitimate interests,” which is recognized in European law as a ground for data processing. While this is an option that Parliament may indeed consider, we think such an exception to consent would be very broad. If new exceptions to consent are to be adopted, we believe it would be preferable that they be defined in a more targeted way. We also think they should be subject to strict conditions and apply only in cases where the societal benefits—and not just the benefits to the organization—clearly outweigh the privacy incursions.

Lastly, the role of legislators will be critical to ensuring Canada’s privacy laws stay current and effective in protecting Canadians from risk of harm.

The time has come for Canada to change its privacy protection model to ensure that, as in the U.S., EU and elsewhere, regulatory bodies can effectively protect the privacy rights of citizens by having powers that are commensurate with the increasing risks that new disruptive technologies pose for privacy.

Canadians have told us they are worried. Focus group participants widely favour the notion of government policing businesses to ensure they respect privacy law. They agree that enforcement should be both proactive and reactive. Their views largely mirror the results of our last OPC public opinion poll in which seven in 10 respondents supported granting the Privacy Commissioner order-making power and the potential to impose substantial financial penalties on organizations that misuse their personal information.

Consequently, we are proposing a model that emphasizes proactive enforcement and is backed by order-making authorities and administrative monetary penalties. The model should also clarify the obligation for organizations to demonstrate respect for the principle of accountability.

While Canada’s largely reactive, complaints based model has had a measure of success in the past, it is facing formidable challenges in the digital age. A complaints-driven system does not give a complete picture of where privacy deficiencies may lie. People are unlikely to file a complaint about something they do not know is happening, and in the age of big data and the Internet of Things, it is very difficult to know and understand what is happening to our personal information. My Office, however, is better positioned to examine these often opaque data flows and to make determinations as to their appropriateness under PIPEDA.

A proactive compliance strategy would also allow us to perform voluntary or involuntary audits, as have been conducted for some time by some privacy regulators in other countries and by regulators in fields other than privacy in Canada. These are not extraordinary powers but rather authorities that have been exercised for a long time by other regulators.

That being said, complaint-based investigations will continue in the future, and I will make greater use of my existing power to initiate investigations where we see specific issues or chronic problems that are not being adequately addressed. But these powers are limited and do not authorize my Office to perform proactive audits simply to verify compliance, without grounds that a violation has occurred. These powers would be very useful, indeed necessary, in a field like privacy where business models and data flows are often complex and far from transparent.

In short, we are convinced the combination of proactive enforcement and demonstrable accountability is far more likely to achieve compliance

**We are proposing a model that emphasizes proactive enforcement and is backed by order-making authorities and administrative monetary penalties.**

with PIPEDA and respect for privacy rights than the current ombudsman model.

Along the same lines, my Office cannot issue binding orders or impose administrative monetary penalties under the current law. We can merely make non-binding recommendations organizations can take or leave as they wish.

This is not in keeping with the powers of many of our provincial counterparts who have order-making powers, nor of our international counterparts—such as the U.S. and many European countries—who are able to impose financial penalties, which serve as an important incentive for organizations to comply. Legislative changes are urgently needed to give my Office the same powers in order to ensure an effective respect for privacy rights.

I propose these changes knowing that many organizations seek to comply with PIPEDA and make significant efforts to that end. However, not all organizations do, and those who do not, cannot always be brought into compliance through non-binding recommendations and the fear of bad publicity. Penalties would be imposed to promote compliance, not to punish.

I am also unconvinced by the industry argument that changing the ombudsman model would make Canadian companies less competitive. U.S. companies face large penalties if found to engage in unfair privacy practices by the U.S. Federal Trade Commission, and they seem able to flourish in that environment.

I am pleased that the House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) has embarked on a comprehensive study of PIPEDA. While I made some preliminary remarks before the Committee in February, I very much look forward to returning to discuss our consent report.

## Privacy Act reform

This past year we also had an opportunity to present our recommendations for *Privacy Act* reform to ETHI as part of its statutory review of the legislation.

The [16 recommendations](#) we put forward dealt with technological change, enhancing transparency and legislative modernization. For more on our recommendations for reform of the *Privacy Act*, see page 53 of this report.

I'm pleased to say that the Committee agreed with all our recommendations in a report issued in December. While government officials understandably have their own objectives when it comes to reform, they too have responded positively to our call for modernization, acknowledging the *Privacy Act* is in need of a wholesale review.

I was especially pleased when Ministers promised to consider one of our key recommendations—that there be an explicit requirement in law that institutions only collect information that is *necessary* for the operation of a program or activity—and that pending legislative reform, they would reiterate to federal institutions the importance of complying with the necessity standard, in line with Treasury Board policy.

I look forward to working with the government in the year ahead so that we can breathe new life into the *Privacy Act*, which has not seen any substantive updates since it came into force in 1983.

That being said, our investigative function under the *Privacy Act* has kept us extremely busy this past year and we are pleased to unveil our findings in a number of important cases. For instance, our report of findings into a series of breaches involving the Government of Canada's Phoenix pay system can be found at page 72. Meanwhile, our conclusions following an investigation into the Privy Council Office's MyDemocracy.ca website aimed at engaging

Canadians on electoral reform can be found at page 69. The report also discusses an investigation related to the RCMP’s use of cell site simulators, sometimes referred to as “Stingray” devices or “IMSI catchers,” at page 65.

### **Public safety, national security and government surveillance**

In addition to the future of consent and legislative reform, matters related to national security, public safety and government surveillance have occupied a substantial portion of our time this past year.

In December we participated in the government’s National Security Green Paper consultation. Our submission, prepared jointly with our provincial and territorial counterparts, emphasized how important it is to consider the impact of surveillance measures on rights and addressed issues such as lawful access and the collection and use of metadata by law enforcement and national security agencies; encryption; information sharing by government and oversight.

Generally speaking, we agree that law enforcement and national security investigators must be able to work as effectively in the digital world as they do in the physical. However, that in no way means that legal thresholds and safeguards must be reduced.

To the contrary, safeguards that have long been part of our legal traditions must be maintained, albeit adapted to the realities of modern communication tools, which hold and transmit extremely sensitive personal information. We were pleased to hear Canadians echo our views in their responses to the government’s Green Paper.

In June, the government tabled new national security legislation. We expect to share our views on Bill C-59 with Parliament in due course.

A number of concerns south of the border are also raising difficult questions.

Canadians have reportedly faced deeply personal interrogations when travelling to the U.S. and have been forced to turn over passwords to laptops and mobile phones. We have cautioned people to limit what they bring when travelling, or to remove sensitive information on devices that could be searched.

When U.S. President Donald Trump issued an Executive Order excluding non U.S. citizens and lawful permanent residents from the protections of the U.S. *Privacy Act* regarding personally identifiable information, we received numerous requests to consider the implications for Canada.

We concluded that while Canadians have some privacy protection in the U.S., that protection is fragile because it relies primarily on administrative agreements that do not have the force of law.

We’ve urged Canadian government officials to ask their U.S. counterparts to strengthen privacy protections for Canadians—namely to ask that we be added to a list of designated countries under the *Judicial Redress Act*. This would extend certain judicial recourse rights established under the U.S. *Privacy Act* to Canadians.

**Generally speaking, we agree that law enforcement and national security investigators must be able to work as effectively in the digital world as they do in the physical. However, that in no way means that legal thresholds and safeguards must be reduced.**

We have also asked the government to confirm whether administrative agreements previously reached between Canada and the United States will continue to offer privacy protection to Canadians in the United States. Once we receive a response from the government on this matter, we will provide additional guidance to Canadians to ensure they are well-informed about their rights and how to protect their personal information in the context of international travel.

Our work in the area of national security, public safety, borders and privacy is discussed in further detail in this report at page 54. We expect our work in this area to continue in the months ahead.

### ***A final word***

---

Privacy need not be a barrier to innovation, government efficiency or national security, but the pursuit of these objectives is no reason to maintain deficient privacy laws or, more generally, to stick to old ways of doing things.

This is why we want to shift our approach towards proactive enforcement and why we have put forward concrete solutions to the problems related to consent. With adequate funding and resources, we can implement these solutions within our existing authorities.

We have reached a point, however, where this is not enough. If Canada is to remain a global leader on privacy, we must have laws that reflect the realities of the 21st Century.

In June, the government tabled legislation aimed at reforming Canada's Access to Information law (Bill C-58) and national security oversight regime (Bill C-59). These are two areas that directly implicate privacy and I look forward to sharing our views on these important matters with Parliamentarians.

The government must now address the shortcomings in Canada's privacy regime. I am encouraged by expressions of interest by Parliamentary committees and cabinet ministers to explore legislative reform as it pertains to both the *Privacy Act* and PIPEDA.

It is not enough for the government to say that privacy is important while taking no systemic measures to protect it. An overwhelming majority of Canadians are concerned about how the digital revolution is infringing on their right to privacy. They do not feel protected by laws that have no teeth and organizations that are held to no more than non-binding recommendations.

While they expect to derive benefits from innovation, they also expect their privacy to be respected.

Now is the time to instill confidence in Canadians that new technologies will be implemented in their best interest and not be a threat to their rights. Now is the time to reform Canada's critically outdated privacy laws.



# Privacy by the numbers

<b>325</b>	PIPEDA complaints accepted*
<b>205</b>	PIPEDA complaints closed through early resolution*
<b>89</b>	PIPEDA complaints closed through standard investigation*
<b>95</b>	PIPEDA data breach reports
<b>1357</b>	Privacy Act complaints accepted*
<b>423</b>	Privacy Act complaints closed through early resolution*
<b>660</b>	Privacy Act complaints closed through standard investigation*
<b>147</b>	Privacy Act data breach reports
<b>95</b>	Privacy Impact Assessments (PIAs) received
<b>49</b>	Advice provided to public sector organizations following PIA review or consultation
<b>3</b>	Public sector reviews concluded
<b>376</b>	Public interest disclosures by federal organizations
<b>27</b>	Bills and legislation reviewed for privacy implications
<b>13</b>	Parliamentary committee appearances on private and public sector matters
<b>16</b>	Formal briefs submitted to Parliament on private and public sector matters
<b>4</b>	Other interactions with parliamentarians or staff (for example, correspondence with MPs' or Senators' offices)
<b>9,091</b>	Information requests
<b>123</b>	Speeches and presentations
<b>2,012,900</b>	Visits to website
<b>245,583</b>	Blog visits
<b>417</b>	Tweets sent
<b>12,709</b>	Twitter followers as March 31, 2017
<b>57,428</b>	Publications distributed
<b>50</b>	News releases and announcements

\* includes one representative complaint for each series of related complaints, see Appendix—2 Statistical tables for more details





# The Personal Information Protection and Electronic Documents Act

## A year in review

### REPORT ON CONSENT

---

Widely known as the cornerstone of Canada's federal private sector privacy law, consent is the tool that affords individuals the opportunity to stake their autonomy and exercise control over their personal information. Organizations that wish to collect, use or disclose that data must, by law, seek and obtain consent. But technological innovations such as big data, the Internet of Things, artificial intelligence and robotics have created serious challenges for those on both sides of this transaction. Organizations say that they cannot always pinpoint or predict every reason for which personal information may be used or disclosed in today's rapidly changing, data-driven marketplace. In this environment, where efforts to explain privacy practices tend to take the form of long, legalistic and often incomprehensible policies and terms of use agreements that are constantly evolving, it is unfair to expect individuals to be able to exert any real control over their personal information or to always make meaningful decisions about consent. Herein lies the dilemma and it's one that is only expected to get more complicated, not less. The time to act is now.

In May 2016, the OPC published a [discussion paper](#) on consent under the [Personal Information Protection and Electronic Documents Act](#) (PIPEDA) to identify improvements to the current consent

model and bring clearer definition to the roles and responsibilities of the various players who could implement them.

We received 51 [written submissions](#) in response to the paper, with roughly half coming from businesses or associations representing businesses. The balance of submissions came from civil society, academics, the legal community, regulators and individuals. We held five stakeholder roundtables across the country to have in-depth discussions about consent challenges and ways to address them. We also solicited the views of individual Canadians through focus groups held in four Canadian cities. We would like to thank everyone who participated in this effort for their time and their valuable contribution.

In this chapter, we lay out what we heard during our consultation and put forward our recommendations for enhancing consent to ensure PIPEDA can effectively protect Canadians in the 21<sup>st</sup> century. Our May 2016 discussion paper provides useful background for the concepts discussed below.

## What we heard

Many we heard from agreed that the increasingly complex digital environment poses challenges for the protection of privacy and the consent model. There was recognition that consent may be a poor fit in certain circumstances, for example, where consumers do not have a relationship with the organization using their data; and where uses of personal information are not known at the time of collection, or too complex to explain to individuals. While we heard a broad range of opinions on how these challenges should be addressed, most felt nonetheless that consent should continue to have a prominent role in privacy protection.

Business largely emphasized the technology-neutral and flexible nature of PIPEDA, suggesting the current legislative framework is adequate and that there are ways to address consent-related challenges largely without resorting to legislative amendments. Respondents from the advocacy community,

including some academics, were more inclined to challenge the status quo and recommended a broader range of solutions to address the perceived shortcomings of PIPEDA and the consent model, including stronger enforcement powers generally.

Focus group participants were dismayed about a perceived lack of control over how their personal information is collected and used by

companies. They felt that they had no choice but to consent to practices they did not know much about. They felt unable to inform themselves because they find the information provided by organizations to be vague, complex and nearly impossible to understand. They were particularly concerned about disclosure to third parties and expected very clear language on this point before giving consent. They wanted better information to exercise individual control but also expected better government protection, because government has more knowledge and better tools to ensure privacy is respected.

Below are specific comments and suggestions that we heard, followed by the OPC's response in terms of action plans and recommendations.

### Enhanced consent

Many participants expressed views about the importance of consent and the role alternatives to consent might play in the future. Those who believed most strongly in consent viewed privacy as protecting individuals' right to decide for themselves what happens to their personal information, and consent as the means to exercise autonomy. Some felt that challenges to consent stem not from the notion of consent itself, but how it is put into practice. We also heard that consent should be an ongoing process, rather than a one-time, all or nothing choice. It was noted, however, that consent may place too much responsibility on individuals in some situations, such as big data algorithmic processing which can be far too complex for non-experts to understand and where future uses of information may not immediately be known.

### Form of consent

We heard much discussion about the form of consent required. It was suggested that the OPC provide further clarification as to when express consent is required and when implied consent may be acceptable. Some proposed that purposes that are not immediately obvious should require opt-in.



**Focus group participants told us they think about privacy and the protection of their personal information at least to some extent. When it comes to acceptable uses of their personal information by companies, selling or passing this information to a third-party crossed the line.**

Conversely, some suggested that consent for the collection of personal information directly required for the good or service could be implied, with limited exceptions. We also heard that the types of notices and choices provided should be directly linked to the sensitivity of information or the risk of harm of a data processing activity. Some suggested that the OPC should widen the scope of implied consent while at the same time placing greater accountability on organizations for their handling of personal information.

### *Simplified privacy policies*

Although a few written submissions recommended the use of shorter and/or standardized privacy policies, overall we heard little support for generic policies or templates. It was generally felt that privacy practices must be described in the specific context of the service being provided in order to be useful. It was noted that even within an industry sector, it would be challenging to identify generic privacy practices. We heard that organizations should strive to highlight up front the core information individuals will look for when being asked for consent. This would include what information is being collected, and what it will be used for, who it will be shared with and for what purposes. Particular prominence should be given to unexpected risks or potentially harmful practices. It was suggested that the OPC could clarify best practices through guidance or codes of practice.

Many participants liked shortened or layered privacy policies. One common suggestion was to allow organizations to highlight only those practices that deviate from the norm while filtering out standard regulatory requirements common across the industry and/or lengthy explanations of practices that would or should be obvious to users in light of the service provided. Others were in favour of real-time consent notices and using infographics, videos, and bots to supplement the information provided through privacy policies. Some called for more research into innovative mechanisms for conveying privacy information.

There was some criticism of privacy policies in general, which were likened to contracts of adhesion due to their “take-it-or-leave-it” nature. We heard that it is important to seek consent at the right time in the process in order for it to be meaningful. Focus group participants generally bemoaned the fact that accepting the terms and conditions is the cost of doing business with companies. In their view, consent is rarely if ever informed. It is an all or nothing scenario over which they have no control.

### *Technological solutions*

Technological solutions to enhancing consent were generally viewed with optimism, though some felt that these were still relatively nascent in a fast-changing digital environment.

Among the solutions presented in written submissions was “tagging” data as a mechanism for restricting its collection, use, disclosure, and retention. Another concept referenced was the use of “consent receipts” to exert control over future choices. There were also recommendations for dashboard/portals to control and adjust privacy settings. One submission suggested that technical measures could be adopted to mask or conceal certain data elements, thereby protecting only that data which needs to be protected, and allowing other data elements to be freely used.

We heard that technology could help manage complexity and that metrics could be adopted to measure consistency on a company’s data management practices with individuals’ consent preferences. It was suggested that the OPC identify the best existing solutions among different approaches such as privacy signaling tools, choice dashboards, infrastructure, database structure and transparency tools. We also heard that the OPC should strongly encourage the tech giants to bake consent-enhancing solutions into their operating systems.

### De-identification

Many participants appeared to view de-identification as beneficial to privacy but not without significant risks. On the one hand, the process of de-identification can be used to strike a balance between protecting personal information and the organizations' desire to use personal information in new and innovative ways. On the other hand, there were concerns that it may simply not be possible to render personal information fully non-identifiable without any residual risk of re-identification.

A number of participants from industry and the legal community argued that de-identified information is not personal information, it falls outside PIPEDA's framework, and consent is therefore not required for its collection, use and disclosure. Others, including representatives from academia and civil society, felt that PIPEDA should continue to apply even to de-identified information, given the real and growing risks of re-identification and the need to ensure organizations remain accountable for their use of de-identified data, including responsible purposes and appropriate safeguards. Some participants saw de-identification and contractual backstops against re-identification as useful strategies for minimizing the risks of unauthorized collection, use, and disclosure of personal information but not necessarily as an alternative to consent.

Industry representatives called for guidance from the OPC on issues such as methods of de-identification and assessing the risk of re-identification, to supplement existing guidance from other data protection authorities. This would help organizations lower the risk of re-identification and achieve better balance between privacy protection and commercial purposes.

### Privacy by design and privacy by default

Generally, stakeholders expressed support for Privacy by Design (PbD) and felt it should be encouraged. However, they cautioned against an overly prescriptive approach as this could risk hampering innovation and competitiveness. Industry held the view that although a sound guiding principle, PbD does not need formal integration in law as it is already recognized as a best practice.

Privacy by default on the other hand was less universally accepted. Some felt that privacy by default would maximize user control while others felt it would be cumbersome and interfere with the practical and seamless use of a product or service. Many felt that privacy controls were dependent on the type of service being provided and should reflect the personal preferences of individuals, who have various levels of comfort with sharing their personal information.

### No-go zones

Generally speaking, there was little support for specifically legislated no-go zones. The concept of no-go zones is based on the belief, recognized in section 5(3) of PIPEDA, that the collection, use and disclosure of personal information should be prohibited outright in certain circumstances regardless of whether consent is obtained. Generally, section 5(3) of PIPEDA was viewed as robust and flexible enough to address "no-go" type situations without having to prescribe them in law. Some cautioned against imposing too much regulation in a fast-changing environment or resorting to top-down protections rather than empowering individuals, though it was recognized that certain practices, such as unauthorized listening through connected devices, were particularly objectionable and inappropriate.

Some civil society groups favoured no-go zones and even suggested examples of prohibited uses to consider, including i) recording sound from a user's microphone or camera, except in cases where a user is using the microphone or camera as part

of obtaining services from the site; ii) publishing personal information for the purpose of incentivizing individuals to pay for the removal of their information; and, iii) attempting to re-identify a user in anonymized data.

### Legitimate interests

There was limited support for legitimate interests as a new ground for processing while recognizing that in some situations, the boundaries of consent are being stretched beyond their limits. For example, it was noted that intermediaries like search engines cannot possibly seek consent as a condition for returning billions of search results each day that may or may not contain individuals' personal information. Also, in a big data context, opportunities are constantly emerging to analyze huge volumes of data originally obtained for one purpose, combined with a variety of other data sources in search of new, innovative possibilities; yet such possibilities cannot always be anticipated at the time of original collection, nor is it always practicable or even possible to recontact each individual in order to obtain fresh consent, as is required under PIPEDA.

Many civil society groups and academics were concerned that a legitimate interest approach would significantly reduce individual control as it is too open-ended. They were skeptical of the idea of importing into PIPEDA a European concept that is rooted in an entirely different legal framework. They commented on the European context that contains much stronger complementary protections currently lacking in PIPEDA.

For their part, industry did not strongly support the concept either. We heard that a better option might be to stretch implied consent because consent can be withdrawn, whereas legitimate interest cannot be revoked. There were also arguments in favour of a broad description of purposes (such as "improving customer service") which would authorize organizations to use the information for purposes not

known at the time of collection. Others felt the time has come to recognize the limits of consent and that a new concept might be required to balance industry needs and privacy protection.

Some were not opposed to the concept of legitimate interests but were concerned that if organizations alone were to define it, profit-making might prevail to the detriment of individual and public interests. A possible solution might be to require that the rationale for a legitimate interests decision be disclosed to the regulator and/or vetted by some third party.

### Ethics

While a few submissions supported ethical assessments and frameworks, including the creation of independent third-party ethics boards, participants at stakeholder meetings—whether from industry or civil society or other regulators—were generally skeptical of the idea.

Some participants thought this approach was potentially paternalistic by allowing ethics board members to speak on behalf of individuals. Others were concerned about the operational feasibility of ethics boards, either because they would be too onerous for small business or would create needless red tape. While some large companies have already begun instituting internal ethics advisory boards, some thought it unlikely that organizations would agree to disclose confidential commercial information to outside third parties or be bound by external advice. Others suggested that there are other ways to address unethical uses of data, for example through subsection 5(3) of PIPEDA or through enhanced enforcement.

### Enforcement

Stakeholder groups had diverging opinions on the need for stronger enforcement powers for the OPC. Organizations largely felt that there is no need to increase OPC powers. Some felt that the threat of public interest naming is already effective in

bringing organizations into compliance because of the reputational harm this can cause to organizations. It was noted that increased powers would increase organizations' compliance costs significantly and enforcement should be done in the most cost-effective way possible to avoid suppressing innovation. Some felt that stronger enforcement is not the solution because Canadian organizations tend to have a desire to comply with PIPEDA; and cautioned that stronger powers might cause organizations to resist innovating out of fear of non-compliance. Others felt that more outreach to organizations to increase

a reversal of the burden of proof under a proactive audit system.

Some suggested that the OPC provide preliminary opinions on a company's proposed practice upon request. A civil society organization recommended that the Commissioner should be empowered to issue "comfort letters", at a business's expense, providing its preliminary opinion as to whether a proposed practice would comply with PIPEDA.

### Education

Focus group participants expressed a widespread desire for educational materials on privacy-related matters. Information considered most helpful included: what to look for in a privacy policy, what data not to share with businesses, what the government does to protect personal information, and individuals' rights and obligations.

Stakeholders also supported public education efforts, although some cautioned that education should not be used to offload privacy responsibilities onto individuals.

Many stakeholders commented on the value of OPC guidance and recommended that the OPC issue additional guidance. Topics of interest included de-identification, forms of consent, and practical tools aimed at small and medium businesses. There was also a strong call for OPC guidance to clarify OPC expectations for compliance in specific areas, such as smart cars.



does not work. Some thought enforcement is the most effective tool for influencing privacy-compliant behavior and yet, there is too little enforcement. It was noted that CEOs inevitably pay more attention and invest more compliance resources in areas where they risk facing enforcement by domestic or international regulators who have stronger authority to make orders and impose fines.

Consumers clearly expect stronger enforcement in all forms, including orders, fines and audits. We heard that in some situations, complaints are unlikely to be filed and therefore the regulator needs to be more proactive in monitoring compliance. There were calls for a lowering of thresholds for audits. Self-auditing by companies was also suggested. However, some organizations objected to what they viewed as

**Focus group participants expressed a widespread desire for information government could provide by way of outreach/public education on privacy-related matters, including what to look for in a privacy policy and what information not to share.**





We heard that both the OPC and organizations have a responsibility to identify norms that would be acceptable to most individuals. It was suggested that good practice be rewarded in order to offset the perception that privacy impedes innovation and adds complexity.

Codes of practice were discussed as a way of providing clarity to organizations on their legislative responsibilities and reassurance to individuals that organizations adhering to the codes are meeting their privacy obligations. Stakeholders were divided about the value of codes of practice. From business we heard that “one-size-fits-all” sectoral codes of practice do not reflect the diversity of practices and needs of businesses in the digital economy. However, there was support for activity-based codes developed with input from the target stakeholders.

We heard that organizations should be responsible for leading code of practice initiatives as they know their business best but may need some encouragement to do so. Codes of practice can be used by good businesses to nudge bad actors into compliance and towards a higher standard. This could also encourage a culture of respect for privacy, which is good for organizations’ reputations and building consumer trust.

### **Our view**

Consent remains central to personal autonomy, but in order to protect privacy more effectively, it needs to be supported by other mechanisms, including independent regulators that inform citizens, guide industry, hold it accountable, and sanction inappropriate conduct. Alternative privacy protection tools must also be considered in exceptional and justifiable circumstances where consent is simply not possible or practicable.

Consent is a foundational element of PIPEDA. Legally, organizations must obtain meaningful

consent to collect, use and disclose an individual’s personal information, subject to a list of specific exceptions. When PIPEDA was adopted, interactions with businesses were generally predictable, transparent and bidirectional. Consumers understood why the company they were dealing with needed certain personal information. There were clearly defined moments when information collection took place and consent was obtained. But obtaining meaningful consent has become increasingly challenging in the digital environment.

In the consent discussion paper, we described the many challenges new technologies and business models are bringing to PIPEDA’s consent model. Reliance on opaque privacy policies as the basis for consent, complex information flows, and business processes involving a multitude of third-party intermediaries, such as search engines, platforms and advertising companies, have put a strain on the consent model. In this age of big data, the Internet of Things, artificial intelligence and robotics, it is no longer entirely clear to consumers who is processing their data and for what purposes. For individuals, the cost of engaging with modern digital services means accepting, at some level that their personal information will inevitably be required to be collected and used by companies in exchange for a product or service.

As such, the practicability of the current consent model has been called into question. Nonetheless, we are of the view that there remains an important role for consent in protecting the right to privacy, where

**Consent remains central to personal autonomy, but in order to protect privacy more effectively, it needs to be supported by other mechanisms, including independent regulators that inform citizens, guide industry, hold it accountable, and sanction inappropriate conduct.**

it can be meaningfully given with better information. We've heard a broad range of suggestions from stakeholders and focus groups on how consent can work better.

Situations in which consent may be simply impracticable are likely very specific, for example, intermediaries where there is no relationship between an individual and the organization collecting and using personal information, such as search engines. Meaningful consent may also be impracticable (or at the very least challenging) in the case of big data initiatives or Internet of Things devices that individuals have no choice but to use. It is conceivable that technology may function in such a way as to defy understanding of how personal information is being processed or what the consequences may be, undermining the meaningfulness and validity of informed consent.

Where consent may not be practicable, the challenge then centres on what can be done to maintain effective privacy protections in the face of ever-changing pressures from technology, business and society, and to identify improvements required to the way consent functions currently.

Technological changes bring important benefits to individuals. They greatly facilitate communication, make available a wealth of information, and give access to products and services from all areas of the world. However, technologies also create privacy risks. Effective privacy protection is essential to maintaining consumer trust and enabling a robust and innovative digital economy in which individuals feel they may participate with confidence. New technologies also hold the promise of important benefits for society, and future economic growth will come in large part from the digital economy. For instance, Canada is well placed to become a world leader in artificial intelligence, which depends on the collection and use of massive amounts of data. The federal government has already invested heavily in this area based on the great potential for return on investment. At the same time, Canada has signed the [2016 OECD Ministerial](#)

[Declaration on the Digital Economy](#) committing among other things, to an international effort to protect privacy, recognizing its importance for economic and social prosperity.

Yet, according to the OPC's 2016 [Survey of Canadians on Privacy](#), the

vast majority of Canadians are worried that they are losing control of their personal information, with 92% of Canadians expressing concern, and 57% being very concerned, about a loss of privacy. Without significant improvements to the ways in which their privacy is protected, Canadians will not have the trust required

for the digital economy to flourish and will not be able to reap all the benefits made possible through innovation. One of the OPC's strategic goals is to *enhance the privacy protection and trust of individuals so that they may confidently participate in an innovative digital economy*, hence our focus on consent.

The absence of strong privacy protections will likely have societal consequences as well. Internet users want to express themselves, explore others' views and search sensitive issues like health without fear that these activities will embarrass them, be turned against them or shared with others with adverse interests. Privacy and informed consent help support our democratic system where individuals have agency to exercise their right to autonomy, including the right to make choices and express preferences. We need to critically examine any situations that threaten to subvert our autonomy and work to 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*<sup>1</sup>.

**An overwhelming majority of Canadians is concerned. They have real fears. Now is the time to give them confidence that new technologies will serve them and not be a threat to their rights.**

<sup>1</sup> This is also one of the goals of the OPC's strategic privacy priorities.



In attempting to identify solutions that would serve to enhance privacy protections today and going forward, we were faced with the central dilemma of how the responsibility for protecting privacy should be apportioned among the various actors—individuals, organizations, regulators and legislators. We heard a compelling opinion from one stakeholder that individuals have to remain at the centre of privacy protection but they need trusted third parties such as regulators to play a more proactive role in further protecting their interests.

Indeed, in the current digital ecosystem, it is no longer fair to ask consumers to shoulder all of the responsibility of having to deconstruct complex data flows in order to make an informed choice about whether or not to provide consent. Autonomy is very important but, given the complexity of the environment, there is a strong role for regulators who have the expertise to enhance privacy protection through education and proactive enforcement. Organizations too must be transparent about their practices and respectful of individuals' right to make privacy choices. And legislators need also to step in when laws are no longer meeting the very objective they set out to achieve and are no longer effective in protecting Canadians from risk of harm.

In other words, everyone—individuals, organizations, regulators and legislators—needs to play their part for privacy to be protected effectively. As stated in the consent discussion paper, the burden of understanding and consenting to complicated practices should not rest solely on individuals without having the appropriate support mechanisms in place to facilitate the consent process. Accordingly, we propose the following solutions for consideration by all the relevant players.

## ***Making consent more meaningful***

---

### ***Privacy notices***

To tackle the situations where obtaining consent is challenging, it is important to first address where and how existing consent mechanisms can be improved. Many situations, including those involving emerging technologies and business models, will continue to require an individual's consent. In order for consent to be valid, individuals must be able to understand the nature, purpose and consequences of the collection, use and disclosure of their personal information. Even though privacy policies are not mentioned in PIPEDA, most companies have chosen to use the privacy policy or terms of use as the primary vehicle for obtaining informed consent, as well as satisfying various other legal and regulatory requirements. This was a questionable choice from the beginning and these documents continued to grow longer and more complex over time. The problem was compounded as companies moved online and largely failed to adapt their privacy notices to a digital environment. Instead they have simply transferred a static, point-in-time, analog document into electronic form.

During the consultations, privacy policies were heavily criticized for obfuscating data practices by being overly lengthy, using complex and ambiguous language, and generally failing to provide individuals with a clear description of how their personal information is to be managed. Individuals talked about the complexity, lack of clarity, and all-or-nothing approach of consent mechanisms. Based on what we heard, in the mind of the average person, privacy policies are broken. Many of our focus group participants had no clear or definite idea of what it means when a company has a privacy policy and most admitted to not reading them.

Much time was devoted to discussing how to fix privacy policies. Suggestions put forward ranged from highlighting unexpected uses of personal information to multimedia and interactive policies. We agree that

privacy policies have been ineffective from a consent perspective, but nevertheless they serve a range of important legal purposes. They are the foundation for the current contractual notice-and-consent model. In addition, regulators and others need to refer to privacy policies in order to hold organizations to account for their personal information management practices and other legal obligations.

While we did hear calls for the OPC to develop templates for privacy policies specific to different sectors, we do not believe that should be the role of a regulator. Rather, it is best left to organizations to find innovative and creative solutions to the consent process in a manner that respects the nature of their relationship with consumers. However, in so doing, we encourage organizations to be guided by the following principles:

1. Information provided about the collection, use and disclosure of individuals' personal information must still be readily available in complete form, although, to avoid information overload and facilitate understanding by individuals, certain elements warrant greater emphasis or attention in order to obtain meaningful consent (see elements below).
2. Information must be provided to individuals in manageable and easily-accessible layers, and individuals should be able to control how much more detail they wish to obtain and when.
3. Individuals must be provided with easy "yes" or "no" options when it comes to collections, uses or disclosures that are not integral to the product or service they are seeking.
4. Organizations should design and/or adopt innovative consent processes that can be implemented just in time, are specific to the context and appropriate to the type of interface used.

5. Consent processes must take into account the consumer's perspective to ensure that they are user-friendly and that the information provided is generally understandable from the point of view of the organizations' target audience(s).
6. Organizations, when asked, should be in a position to demonstrate the steps they have taken to test whether their consent processes are indeed user-friendly and understandable from the general perspective of their target audience.
7. Informed consent is an ongoing process that changes as circumstances change; organizations should not rely on a static moment in time but rather treat consent as a dynamic and interactive process.

As stated in the [2014 joint guidelines for online consent](#), the consent obtained by organizations must be based on complete and understandable information and therefore that information must be readily available. However, we believe that certain elements in particular should be given more prominence in order to obtain meaningful consent. These are:

- what personal information is being collected;
- who it is being shared with, including an enumeration of third parties;
- for what purposes is information collected, used, or shared, including an explanation of purposes that are not integral to the service; and,
- what is the risk of harm to the individual, if any.

Organizations should deliver the right information to individuals when they most need it. This includes using meaningful language and going beyond vague descriptions of purposes such as "improving the customer experience." We recognize the difficulties

**We will update our guidance on online consent to specify four key elements that must be highlighted in privacy notices and explained in a user-friendly way.**

of finding the sweet spot between delivering information required for users to make informed decisions and not disrupting the flow of their experience or causing consent fatigue. Nonetheless, it is only when the right information is brought to individuals' attention at the right

time and in a digestible format that they can exercise meaningful control.

In the course of our compliance activities, we will continue to require organizations to provide complete information, but we will also expect that additional emphasis be given to the above-mentioned four elements. We have updated the online consent guidance to provide more clarity around these expectations, and are welcoming comments on this proposed change.

### **Forms of consent**

Stakeholders also had questions about what form of consent should be required in a given situation. We heard from stakeholders that consent should be explicit for proposed practices that are not core or integral to the service, or that are unexpected or out of context. At the same time, individuals do not want to be asked too often for express consent. Again, we recognize that consent fatigue is against everyone's interest, individuals and businesses alike. The courts have affirmed that in determining the form of consent to use, organizations need to take into account the sensitivity of the information, and the reasonable expectations of the individual, both of which will depend on the context.<sup>2</sup> We will consider how best to flesh out the concept of reasonable expectations of individuals in different contexts. This may mean

working with organizations and individuals to examine what personal information they view as integrally linked to their services, and we will expect organizations to be very transparent about when personal information is core or integral to the service and when it is not.

We also agree with stakeholders that the form of consent should depend on the sensitivity of the information and the risk of harm of a data processing activity. PIPEDA refers to sensitivity, but it does not refer specifically to risk of harm. Yet we see risk of harm as an important and related factor to consider when assessing the sensitive nature of personal information in a given context. We will therefore amend our consent guidelines accordingly, and we will ask Parliament to make risk of harm an explicit factor to consider when determining the appropriate form of consent.

### **Children and youth**

During the consent consultations, some stakeholders asked for guidance in applying PIPEDA's consent requirement to children. We believe that a child's ability to provide meaningful consent is a function of individual maturity which we recognize is an evolving process of cognitive and social development. While a child's capacity to consent can vary from individual to individual, we believe that there is nonetheless a threshold age below which young children are not likely to fully understand the consequences of their privacy choices, particularly in this age of complex data-flows. As such, we are taking the position that, in all but exceptional cases, consent for the collection, use and disclosure of personal information of children under the age of 13, must be obtained from their parents or guardians. As for youth aged 13 to 18, their consent can only be considered meaningful if organizations have taken into account their level of maturity in developing their consent processes and adapted them accordingly. Our draft online consent guidelines will propose guidance on this issue.

<sup>2</sup> Royal Bank of Canada v. Trang, 2016 SCC 50

### *Encouraging consent technologies*

Technology has a role to play when traditional attempts at providing meaningful consent have failed. It has the potential of facilitating the consent process and making it more practical and meaningful. The OPC's consent stakeholder sessions and submissions discussed a number of technical solutions that could enhance the consent process. We believe that there is no shortage of technologies or good ideas for facilitating the consent process, but there does seem to be a lack of deployment and adoption in the business community. The current economic and regulatory environments provide little incentive for deploying promising consent technologies, so further development of technology alone is not likely to lead to significant changes.

To raise awareness of available consent technologies and encourage their use by individuals, the OPC will publish education material identifying various consent technologies available on the market today. We will also find ways to fund research and knowledge translation activities to promote development and adoption of consent technologies by industry through the OPC's Contributions Program. The OPC also plans to explore opportunities to take an active role in standard-setting bodies and industry groups.

We believe that companies should assist individuals in making privacy choices. We are particularly concerned by reports that companies may be complicit in establishing an environment that disregards or counteracts individuals' use of consent technologies. For example, certain types of tracking used in online behavioural advertising cannot be stopped or controlled without taking extraordinary measures (and some cannot be stopped or controlled at all). These include so-called zombie cookies, super cookies, and device fingerprinting. To that end, we would encourage individuals to advise us of any such problems they encounter when they attempt to make use of these new consent technologies but see their choices being overridden nonetheless. We will pursue issues reported to us where we find reason

to believe that individuals' privacy choices are not being respected or are being reversed against their wishes. More broadly, there is an opportunity for government involvement in this area. As part of its strategy to promote the development and adoption of innovative technologies, like artificial intelligence or superclusters, we encourage government to fund technologies on the condition that they build in privacy protections. In our view, there is an opportunity for the government to leverage innovation and better privacy protections across the board.

### *No-go zones even with consent*

One of the questions we put to stakeholders is whether they see a need to amend PIPEDA (or other legislation) to introduce clear and specific prohibitions on the use of personal information even with consent (so called "no-go zones"). PIPEDA already prohibits inappropriate uses under subsection 5(3), which cannot be overridden by consent, but these are broad and subject to interpretation.

We agree with stakeholders that legislating specific no-go zones would not be ideal, given the fast pace of change and innovation. However, we do intend to issue guidance under subsection 5(3) to provide greater clarity to organizations on what we consider inappropriate uses from "the reasonable person standpoint," which we believe would also be useful to consumers. We will be releasing a draft version of this guidance and seeking input before finalizing it. Our draft is informed by comments we heard during the consultations, as well as our experience investigating privacy practices and listening to Canadians' concerns over the past 15 years. Some examples of what we consider to be purposes that a reasonable person would not consider appropriate are: collection, use or disclosure that is otherwise unlawful; profiling or categorization that leads to unfair, unethical or discriminatory treatment; publishing personal information with the intended purpose of charging individuals to pay for its removal; and situations that are known or likely to cause significant harm to

the individual. By “significant harm,” we mean both material and reputational harm as is contemplated in the new subsection 10.1(7) of PIPEDA, which has been adopted but is not yet in force.

Although privacy, as an inherent right, can be infringed without harm, some stakeholders made mention of the important role of harm in privacy protection. We agree that mitigating the risk of harm is one of the aims of privacy legislation and, as noted earlier, we think that it should be made explicit under the law. Specifically, where collection, use or disclosure of personal information is known or likely to cause significant harm to individuals, it should be prohibited. On the other hand, where risk of harm is lower and reasonable in return for a benefit, the choice to accept or not should be left to the individual. In order to inform these trade-off decisions, risks must be fully disclosed, and individuals’ acceptance of those risks must be expressed explicitly.

### *Guidance for individuals and organizations*

Privacy protection starts with knowledge. For individuals this means being able to identify privacy risks, having the skills to mitigate them, and knowing how to exercise their privacy rights. For their part, organizations need to know their privacy obligations, and understand what is expected of them with some sense of consistency and predictability in order to comply with the law.

During the consent consultations, stakeholders overwhelmingly called on the OPC to provide more education and guidance for individuals and organizations and we agree that this is an integral part of addressing not only the consent challenge but ensuring effective privacy protection as a whole. We heard that businesses look to the OPC to develop and promote good privacy practices and provide clarity around PIPEDA requirements. Guidance is particularly useful to small- and medium-sized businesses that typically have a lower awareness of

PIPEDA and lack the resources to address privacy effectively.

Focus groups expressed a widespread desire for information on privacy-related matters. This includes what to look for in a privacy policy and how to address the risks associated with sharing personal information with companies. As part of the OPC’s public education mandate, we have a strong commitment to helping raise awareness of privacy issues and to providing individuals with information to help exercise their privacy rights and reduce privacy risks. Public education also has the added benefit of empowering consumers themselves to play a challenge function and hold companies to account through questions and complaints.

However, it is important to recognize that privacy education does not just benefit consumers. All Canadians, regardless of their role in the economy, need to become digitally literate so as to exercise their privacy rights and have control over their personal information. Children in particular need to be educated about privacy and its value to individuals and our society in order to make informed decisions.

The OPC’s particular focus in education materials has been on helping equip children and young people with the skills to evaluate and mitigate privacy risks and to make informed privacy choices. To that end, we have developed resources for parents, educators and librarians, such as lesson plans, fact sheets and a graphic novel to help bring privacy education to kids. Internationally, we helped develop the [2016 Marrakech Resolution](#) calling for the adoption of a [competency framework for privacy education](#) in schools. Currently we are participating, through the International Working Group on Digital Education, in efforts to further the inclusion of privacy and data protection skills in the education of students around the world.

While we are proud of our work to date in this area, as a federal body we face jurisdictional limits to our ability to influence education. We note that our provincial and territorial counterparts have expressed similar concerns about the need to improve digital education. Together, we are asking that privacy education should be made an official part of the curriculum starting as early as possible. Kindergarten to grade 12 education reaches nearly all Canadians and while some provincial curricula may touch on privacy skills to some degree, the need to promote privacy literacy in a holistic and consistent manner should not be ignored. We are ready to support our provincial and territorial colleagues to help institutionalize privacy education so that children are empowered to protect their privacy from a young age and stand ready to participate fully in the digital world with knowledge of the value of privacy and the skills to exercise their privacy rights.

Beyond school curricula, privacy education and guidance for individuals figures prominently in our action plan for improving Canadians' control over their privacy, across the age spectrum, including seniors. To that end, we have identified a series of topics where we think Canadians would benefit from privacy information. We intend to issue guidance and fact sheets in as many areas as possible in order to help Canadians have a better understanding of privacy implications and have more agency in exercising their privacy choices. We have also identified topics where we intend to issue guidance or update existing materials aimed at businesses to help provide clarity and certainty around particular issues or practices:

1. Consent (including forms of consent)
2. Subsection 5(3) no-go zones
3. De-identification
4. Big data, artificial intelligence & robotics
5. Genetic information
6. Internet of Things
7. Connected cars
8. Smart homes
9. Privacy enhancing technologies
10. Surveillance technologies

11. Privacy at the border (smart borders)
12. Necessity and proportionality in the public sector
13. Online reputation
14. Privacy and social media
15. Educational apps/platforms
16. Biometrics & facial recognition
17. Cookie-less tracking
18. Blockchain
19. Digital health technologies
20. End-to-end encryption
21. Social engineering
22. Trans-border data flows & cloud
23. Open government
24. Accountability maturity model
25. Breach notification
26. Data brokers
27. Fintech
28. Sharing economy
29. In-store tracking
30. Behavioral economics

While we cannot promise to fulfil this wish list as quickly as we would like, we will undertake to complete as much as we can by 2021, taking into account our workload and resources. Recognizing that we cannot do it all in the near future, we will begin in the next two years with those areas where we see the greatest need directly related to the issue raised in this chapter: online consent, subsection 5(3) no-go zones, de-identification and privacy enhancing technologies, genetic information and breach notification, in addition to our parallel work on online reputation, biometrics and the border. We will also publish research on artificial intelligence.

Moreover, we will encourage industry to help us by developing codes of practice in some key areas. To start, we are funding two research projects through our [Contributions Program](#) that will seek to develop codes of practice on the connected car and legal apps, and we hope to expand on this in the foreseeable future. Codes of practice are a useful and effective tool for enhancing compliance.



### OPC Actions

- The OPC will issue updated guidance on online consent that will set the following expectations:
  - While organizations must continue to make readily available to individuals complete and understandable information, the following elements must, in order to obtain informed consent, be given particular prominence and be brought to the individual's attention in a user-friendly format and at an appropriate time:
    - what personal information is being collected;
    - who it is being shared with;
    - for what purposes is information collected, used, or shared, including an explanation of purposes that are not integral to the service; and
    - what is the risk of harm to the individual, if any.
  - In determining the form of consent, organizations must consider the reasonable expectations of the individual, the sensitivity of the information and the risk of harm.
- The OPC will also amend its accountability guidelines to clarify that organizations give prominence to a few key pieces of information and that they be able to demonstrate that they have a process in place to verify that their consent mechanism works.
- The OPC will draft and consult on new guidance that will explicitly describe those instances of collection, use or disclosure of personal information which we believe would be considered inappropriate from the reasonable person standpoint under subsection 5(3) of PIPEDA (no-go zones).
- The OPC will better flesh out the concept of reasonable expectations of individuals in different contexts, including for the purpose of informing the form of consent.
- The OPC will inform individuals of available technological tools designed to implement consumers' consent choices, and will pursue reports made to us that individuals' privacy choices have been obstructed.
- The OPC will fund research and knowledge translation activities to promote development and adoption of new consent technologies through our Contributions Program.
- The OPC will explore opportunities to take an active role in standard-setting bodies and industry groups to promote consent technologies.
- The OPC will issue fact sheets (information documents) in as many areas as possible in order to help Canadians have a better understanding of privacy implications and exercise their privacy rights. Similarly, we will issue guidance to organizations in as many areas as possible on how to comply with their privacy obligations.
- The OPC will encourage industry to develop codes of practice, starting with one on the connected car and another on legal applications.

### OPC Recommendations

- Parliament should consider making risk of harm explicit in PIPEDA, for instance for the purpose of informing the form of consent (implied vs explicit).
- The government is encouraged to fund emerging technologies that build in privacy protections in order to help create incentives for their adoption.
- Provincial and territorial governments are urged to integrate privacy education in school curricula.

## Alternatives to consent

No matter the measures taken to facilitate and enhance the ability of individuals to provide informed consent and of organizations to obtain it, the fact remains that in some circumstances consent may simply not work. Such circumstances are likely exceptional, though they may expand as technology evolves. As outlined in our consent discussion paper and noted earlier, business models, facilitated by new technologies, have moved far beyond the traditional transactional, usually bilateral relationships that PIPEDA envisaged. Where in the past companies could be described in terms of their dominant business lines—retail, telecommunication, entertainment—today many have become omnichannel data companies powered by personal information. In some cases, technology has become so complex, and algorithms so complicated, so as to defy understanding of how personal information is being managed or what the consequences may be, undermining the meaningfulness and validity of informed consent. Innovations like artificial intelligence and robotics will no doubt layer on further complexity in the future. Below we outline three potential solutions for enhancing privacy protections in such circumstances.

### De-identification

De-identification was discussed with much interest at the stakeholder roundtables, particularly by industry which views de-identification as a way of mitigating potential privacy risks and addressing some of the consent challenges under PIPEDA. Yet, we also heard much concern about the risk of re-identification and the corresponding need to be careful in establishing at what point PIPEDA requirements would no longer apply to the information.

Given the vast amounts of personal information being processed in the digital environment, de-identification may seem like a promising measure for enhancing privacy protection. At the same time, we acknowledge

concerns that re-identification is a real risk not only because of the availability of data sets that can be used to re-identify personal information, but also because of the lack of rigour in de-identification methods. Nonetheless, we are guardedly optimistic that de-identification can be a viable solution provided it is managed appropriately.

To that end, we intend to issue guidance on de-identification that will, among other things, aim to help organizations quantify what is meant by a “serious risk of re-identification.” Currently, the law sets as the legal standard the serious possibility of identifying an individual based on data either alone or in combination with other data, and we propose to set out factors we consider integral to evaluating this threshold, both qualitatively and quantitatively. The guidance will help organizations assess and reduce risk of re-identification to a sufficiently low level where it may reasonably be used without consent.

We also find value in the idea of a spectrum of identifiability that can attract more or less rigorous privacy requirements commensurate with the level of privacy risk. For example, the EU *General Data Protection Regulation* (GDPR) recognizes pseudonymization as a safeguard and allows organizations greater flexibility when processing pseudonymized information while still considering this information to be personal for the purposes of the law.

The idea that different categories of data beyond the existing black or white concepts, merit different levels of protection, more or less stringent depending on risk of re-identification is also being explored by leading privacy and legal experts. For example, a paper presented at the 2016 Brussels Privacy Symposium, by El Emam *et al* build upon existing research to propose a framework for classifying states of data between non-identifiable and personal information, taking into account risk of identifiability and proposing



methods for mitigating privacy risk.<sup>3</sup> We encourage Parliament to examine this emerging issue, which has the potential to provide the flexibility needed to achieve a better balance between privacy protection and economic value of data.

### Publicly available information

In the interests of promoting more relaxed consent requirements, a number of industry stakeholders suggested changes to PIPEDA's [Regulations Specifying Publicly Available Personal Information](#) (the Regulations). They argued that the categories of publicly available information need to better reflect today's environment where personal information can be readily accessed in "open spaces" such as the Internet.

We find the Regulations to be a 'snapshot in time' of what the legislators considered to be generally accepted forms of publicly available information at the turn of the century, and agree that updating is required. However, we caution against the common misconception that simply because personal information happens to be generally accessible online, there is no privacy interest attached to it.

The issue of deciding how to protect the privacy interest of people whose information is accessible to the public is extremely complex, and will have to take into account many considerations including the purposes of those posting their own information and deciding how to treat personal information posted by third parties. This issue also raises fundamental questions of freedom of expression and the right to access information in the public interest. We are currently examining these issues in the context of our Reputation Project and may have more to say later this year. Ultimately, however, given the importance of this issue, it would not suffice to merely tweak the

existing Regulations by the Governor-in-Council. Rather, the matter merits the further attention of and deliberation by Parliament as these issues will require a careful reflection and balancing of fundamental individual and societal rights.

### New consent exceptions

The concepts of de-identification and publicly available information address the consent issue to a certain extent. However, some situations still remain where consent is simply not possible or practicable, and privacy protection needs to be otherwise ensured. Some have argued that PIPEDA was never intended to apply to certain activities which do not involve any relationship at all between an individual and the organization collecting and using personal information. Yet these situations raise privacy issues that need addressing.

There are also situations where, even though a relationship may exist between an individual and a company, consent may still not always be practicable, for instance in the big data context considering the continuous collection of massive volumes of data, the numerous new purposes for which data may be used and the complexity of algorithms that are difficult to explain in any understandable way to consumers. Seeking consent for new purposes may be possible in some circumstances, and in such cases it should be sought. However, we also believe it is likely that fresh consent may sometimes be not only difficult but also impracticable to obtain.

To deal with these challenges, we propose that Parliament consider amending PIPEDA to introduce new exceptions to consent under section 7 of PIPEDA to allow for socially beneficial activities that the original PIPEDA drafters did not envisage. While recommending exceptions to consent may seem contrary to our mission as a privacy regulator, in fact we have come to the conclusion that acknowledging this reality with appropriate protections is preferable

3 Khaled El Emam, Eloise Gratton, Jules Polonetsky and Luk Arbuckle. "The Seven States of Data: When is Pseudonymous Data Not Personal Information?" Presented at the 2016 Brussels Privacy Symposium.

to otherwise stretching or distorting the concept of implied consent so as to become meaningless.

Such exceptions would need to be limited to circumstances where the societal benefits clearly outweigh the privacy incursions and where several prior conditions must be met before information can be used for such purposes. We would recommend that Parliament consider the circumstances where such exceptions might be warranted from a broader societal perspective. In our view, situations where consent is likely not always practicable include: search engines indexing web sites and presenting search results to Internet users where appropriate; geolocation mapping services that society has become increasingly reliant upon; or certain data processes, such as big data analytics, Internet of Things, artificial intelligence or robotics applications where commercial and societal interests align.

As for prescribed prior conditions, these could include an organization having to demonstrate, on request, that:

- it is necessary to use personal information;
- it is impracticable to obtain consent;
- pseudonymized data will be used to the extent possible;
- societal benefits clearly outweigh any privacy incursions;
- a PIA was conducted in advance;
- the organization has notified the OPC in advance;
- the organization has issued a public notice describing its practices; and,
- individuals retain the right to object.

While one option would be to create a broad “legitimate interest” exception as exists in Europe’s GDPR (and has existed in some national laws for some time), we would prefer as exceptions a list of more specific circumstances, such as the ones listed above.

This would be for two reasons: first, the concept of legitimate interests is very broad and may include several circumstances where an exception to consent is not necessary. Second, and related to the first, there is a risk that organizations might abuse this new concept as broad license to collect, use or disclose personal information, although the above list of conditions would mitigate that risk.

Use of such exceptions should only be permitted as a last resort, after every avenue to obtain consent had been explored and proven to be impossible or impracticable. Also, a new consent exception would necessarily have to be contingent on stronger enforcement powers (see below) that would authorize privacy regulators, where warranted, to assess whether the use of personal information was indeed for broader societal purposes and met the prescribed legal conditions. To clarify, this would not be accomplished with a prior-authorization regime but rather, the kind of proactive enforcement model we propose in the following section on governance.

**We also encourage Parliament to consider whether new exceptions to obtaining consent may be appropriate where consent is simply not possible or practicable.**

### OPC Actions

- OPC will issue guidance that will suggest appropriate methods of de-identification and will set out factors to be considered in evaluating, both qualitatively and quantitatively, when the risk of re-identification is sufficiently low as to authorize the use of information without consent.

### OPC Recommendations

- Parliament should examine the possibility of introducing new exceptions to consent to address activities where the societal benefits clearly outweigh the privacy incursions, subject to strict conditions and stronger enforcement.
- Parliament should examine the concept of pseudonymized information which may be exempt from consent requirements but still subject to all of the other PIPEDA protections.
- Parliament should consider how best to modernize the *Regulations Specifying Publicly Available Information* taking into account the need to balance potentially competing constitutional rights.

## Governance

The previous section outlined ways in which the consent model could be adapted to meet the challenges of a digital data-rich environment. We now move to mechanisms for ensuring that companies operationalize and respect their obligations under PIPEDA.

### Accountability

Accountability is a fundamental PIPEDA principle that requires organizations to develop and implement policies and practices to uphold the principles of Schedule 1 of the Act. Taken as a whole, these policies and practices should constitute a coherent privacy management program. During the consultations we heard that accountability should be made more prominent.

As the OPC's joint [Accountability Guidance](#) indicates, the Office currently has the implicit authority to require organizations to demonstrate compliance with their obligations under Principle 4.1 of PIPEDA in the course of an investigation or an

audit. The lack of demonstrable privacy policies and procedures has been called out in recent PIPEDA investigations, including the Ashley Madison case.

The OPC does not however have the power to make on-demand requests for organizations to demonstrate accountability. The new power to examine breach records on demand is a positive step in this direction, which we have welcomed, but it does not go far enough. We strongly believe that, in order for the OPC to effectively enforce PIPEDA compliance, accountability needs to be demonstrable not only after an unfortunate incident but also proactively. We take this opportunity to reiterate [our recommendation](#) that the government consider remedying this situation.

As our guidance on accountability noted, the purpose of a privacy management program is to facilitate organizations building privacy protection into the very design of a product or service, from the early phase of conception through to its execution, deployment and beyond. As noted earlier, stakeholders generally supported the use of PbD (a concept championed

by former Ontario Information and Privacy Commissioner Ann Cavoukian) but did not think it needed to be made an explicit requirement under the Act. They argued that the concept was already there implicitly and that it should not become overly prescriptive. Two elements of PbD that we find to be of greatest importance are its temporal requirements (as early as possible and continuously assessed) and the fact that it addresses both technological and organizational factors. Both of these aspects can be found in our guidance. In our view, both these elements are key and we expect them to be implemented. To aid smaller organizations in meeting their accountability obligations, we will be issuing a modified version of our accountability guidance aimed at small- and medium-sized businesses, and help move them along an accountability maturity model as their organization grows.

We also think that part of accountability requires organizations to be able to demonstrate the steps they have deliberately taken in order to design and implement an informed consent process that is understandable to their target audience and customized to the nature of their product or service. We have updated the online consent guidance to provide more clarity around these expectations, and are welcoming comments on this front.

As for the use of trust marks as another way of proactively demonstrating accountability, there was a general lack of support for trust mark schemes based on experience to date. Many were wary of trust-mark programs developed and operated by industry for industry, citing lack of independence as a major concern. A few participants, however, spoke favourably about trust marks overseen by a credible independent organization, such as the Better Business Bureau or the OPC. It is worth noting that Canada is a participant in the Asia Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CPBR) System. This is a voluntary system whereby a third-party body, referred to as an Accountability Agent, reviews the cross-border privacy policies and practices of interested organizations

in participating APEC member economies and certifies them as compliant with a set of program requirements based on the APEC Privacy Framework Information Principles. A Canada Gazette Notice for Accountability Agents under the CBPR was posted in December 2016, and we are monitoring developments with interest.

### Ethics

Stakeholders generally felt that the notion of independent ethics review boards, borrowed from the academic research context, does not transpose well in the commercial world. Nonetheless, we believe that incorporating an ethics lens into privacy protection is an important and worthwhile discussion, particularly given the potential discriminatory impacts of big data, and the as-of-yet unknown safety and societal implications of Internet of Things devices and wearable computing—not to mention the consequences of artificial intelligence and robotics on society and humanity as a whole. We acknowledge, however, that the incorporation of ethics into privacy law, whether in the form of consumer ethics boards or otherwise, is not yet developed enough to be practical in the short term. We will continue to monitor developments on this front and actively participate in furthering debate on these issues when and as the opportunities arise.

### Enforcement

In the [OPC's 2013 paper on why PIPEDA needed reform](#), we noted the vast changes that technology had brought in the short years since PIPEDA came into force and that greater incentives were needed for organizations to build privacy protections in from the start. At that time, we argued for stronger enforcement powers to create these incentives—a need which has become even greater in 2017. Technological development continues at an ever faster pace, and in the few years since our last case for PIPEDA Review, new businesses and services have evolved to such an extent that we are now witnessing the disruptive nature of new technologies and data-driven economies that were nascent when PIPEDA was passed. The so-called sharing economy, the Internet of Things,

artificial intelligence, augmented reality—these are examples of new and emerging services and technologies that are poised to radically change how Canadians interact with businesses, machines and each other—with their personal information being the new price of participation.

In our view, the time has come for Canada to change its regulatory model to ensure that the privacy rights of Canadians are adequately protected through privacy regulators who, like those of its trading partners in the U.S., the EU and elsewhere, have strong enforcement powers commensurate with the increasing risks that new disruptive technologies pose for privacy.

Canadians have told us that they are worried. Ninety-two percent say that they are concerned about their privacy. Focus group participants widely favoured the notion of government policing businesses to ensure they respected privacy law and agreed that enforcement should be both proactive and reactive. Focus group views largely mirrored the results of a recent OPC [public opinion poll](#), in which 69 percent of respondents supported granting the Privacy Commissioner order-making power to enforce recommendations made following an investigation and 70 percent said they would be more likely to do business with companies if they were subject to strict financial penalties for misusing their personal information.

PIPEDA was “enacted to alleviate consumer concerns about privacy and to allow Canada’s business community to compete in the global digital economy.”<sup>4</sup> The policy goal was to build trust in electronic commerce.<sup>5</sup> These goals are as valid today as they were then. However, Canadians do not feel protected by a law that has no teeth and organizations

that are held to no more than non-binding recommendations.

Other jurisdictions have been moving towards granting their data protection authorities the power to award damages, administer fines, and order an organization to change its practices or release personal information to an individual requesting it. Provincially, the private sector privacy laws in Alberta, B.C., and Quebec, and Ontario’s PHIPA provide for general order-making power, in contrast to PIPEDA. Internationally, many of the major data protection laws provide for order making power, including the GDPR, the U.K. and Irish *Data Protection Acts*. While none of our provincial acts provide the Commissioner with the power to impose financial penalties, fines or monetary settlements are becoming the norm internationally. Under the GDPR, fines will amount to four percent of the organization’s annual revenues; in the United States, the Federal Trade Commission (FTC) has leveled sanctions of \$20 million and higher in the form of settlement agreements; in Canada, the *Competition Act* provides for administrative monetary penalties to a maximum of \$15 million, based on a variety of factors. Canada needs powers comparable to those in other jurisdictions in terms of order-making powers and fines in order to have meaningful impact on privacy protection and continue to enjoy the trade partnerships we have forged with Europe and others. Moreover, regulatory and enforcement power

**The time has come for Canada to change its regulatory model to ensure that the privacy rights of Canadians are adequately protected through privacy regulators who, like those of its trading partners in the U.S., the EU and elsewhere, have strong enforcement powers commensurate with the increasing risks that new disruptive technologies pose for privacy.**

<sup>4</sup> From Industry Canada’s website: [Privacy for Business, Electronic Commerce in Canada](#)

<sup>5</sup> From the Honourable John Manley’s speaking notes, presentation to the Senate Committee Studying Bill C-6, December 2, 1999.

gaps may well prove a factor of consideration when Canada's adequacy status is reviewed by the EU.

Industry stakeholders took the position that stronger enforcement would stifle innovation and would adversely impact the good working relationship the OPC currently enjoys with organizations, a relationship which produces positive results for privacy. They also argued that stronger enforcement powers are not required as companies generally seek to be compliant, and the OPC has been quite successful in bringing offenders into line through existing tools such as publicizing findings of non-compliance.

We agree that many companies seek to comply with PIPEDA, but not all do, and those who do not cannot all be brought into compliance with existing powers of recommendations and the fear of bad publicity. Consumers need to be protected from bad actors as well as illegal conduct by organizations that are generally responsible but sometimes cross the line. Stronger enforcement can serve also as an incentive for company executives to focus the mind and invest in privacy. We heard from stakeholders that companies will put their compliance resources where the biggest

risk is, and the threat of penalties would help ensure companies adopt PIPEDA compliant practices. As a result, companies are more likely to listen to regulators like the FTC than the OPC. The fact that the FTC regularly imposes financial sanctions in the millions of dollars does not seem to have dampened innovation in the United States.

We recognize, however, that the factors for imposing a penalty would need to be carefully and thoughtfully

worked out to underscore what the ultimate aim is—to enhance compliance, rather than to punish. In this way PIPEDA would be similar to several longstanding Canadian regulatory regimes and due diligence (evidence that an organization has taken all reasonable steps to avoid the specific violation found by the regulator to have occurred) would be a complete defence exonerating the organization from having to pay an administrative monetary penalty (AMP). Parliament could also prescribe factors to consider in setting the amount of penalties. Such factors could include whether an organization has appropriate safeguards in place or could demonstrate a sound privacy management program or conversely, whether there is recidivism, recklessness or an egregious violation.

While we agree that Canada's largely reactive, complaints based model has had a measure of success in the past, it is facing formidable challenges in the digital age. The ombudsman model has been unable to make Canadians more confident that their privacy is protected and that they have a say in what happens to their personal information. The objective of PIPEDA, as outlined in section 3, is to balance individual privacy rights with the need of organizations to collect, use or disclose personal information for reasonable and appropriate purposes. Parliament has chosen specific oversight measures to achieve this objective. These measures, consisting largely in the reactive ombudsman model, made sense at the time PIPEDA was adopted. However, it is our view that such a model is no longer effective to achieve the overall objective of the Act.

First, a complaints-driven system does not give a complete picture of where privacy deficiencies may lie. Complaints determine which issues the OPC looks at, and often these are one-off concerns based on the experience of a single individual that may not be reflective of the broader reality. People are unlikely to file a complaint about something they do not know is happening, and in the age of big data and the Internet

**We are convinced the combination of proactive enforcement and demonstrable accountability is far more likely to achieve compliance with PIPEDA and respect for privacy rights than the current ombudsman model. This requires urgent changes.**



of Things, it is very difficult to know and understand what is happening to our personal information. Our Office, however, is better positioned to examine these often opaque data flows and to make determinations as to their appropriateness under PIPEDA.

This is in part why we think the Canadian model should become more proactive. The Privacy Commissioner already has the authority to initiate complaints, if satisfied that there are reasonable grounds to investigate a matter<sup>6</sup>. However, contrary to UK and French colleagues, we do not have the authority to verify compliance on demand, without grounds that a violation has occurred. Such powers are frequent in Canadian regulatory regimes, including employment standards, health and safety, food and restaurants, tobacco, and securities.

A proactive enforcement model would be most effective in ensuring that organizations are demonstrably accountable for their protection of consumer privacy. Throughout our consultations, we often heard that accountability needs to take a larger place in privacy protection, in a period where data flows and business models are becoming more complex, thus creating challenges for the consent model. While we believe consent continues to have an important role, we agree that the weight given to accountability should increase. Accordingly, organizations should be able to demonstrate accountability on demand as a means to ensure that privacy rights are respected.


For now, we will continue to explore how we could more proactively promote PIPEDA compliance under the current law. Proactive compliance and enforcement activities we are considering are more strategic and frequent use of formal powers, including our ability to carry out commissioner-initiated investigations pursuant to subsection 11(2) of the Act, including sector-wide investigations to address

systemic privacy risks to Canadians. We will also seek to provide advice to organizations.

However, proactive compliance and enforcement activities can be resource intensive, and it would be challenging to be much more active with that strategy while at the same time investigating close to all complaints filed by individuals. One solution would be a modest increase in resources so that we can undertake both reactive and proactive compliance.

Another would be to have broader discretion to decide which individual complaints will be investigated, and which ones should give way to systemic proactive reviews that stand to have broader positive impact on Canadians. Our preferred choice is the first of these two options. However, without the modest increase in resources needed to do so, we reluctantly recommend broadening our discretion to decline individual complaints so that we can reallocate limited resources to more proactive enforcement and produce what we have come to believe would be more impactful and sustainable results for Canadians. We would identify criteria for declining complaints that would take into account, for example, whether the complaint is of a one-off or more systemic nature and whether the individual has other options for seeking a fair remedy.

In order to ensure that individuals are not left without a remedy, we think Parliament should consider creating some form of judicial redress, such as a private right of action for PIPEDA violations, whereby individuals can still turn to the courts in



**When it came to the role of government in protecting personal information, there was widespread agreement among focus group participants that the role should be both proactive and reactive.**

<sup>6</sup> Subsection 11(2) of PIPEDA

cases where the OPC does not proceed to investigate and produce a report of findings.

In our view, the time has come to provide individuals with the option of direct access to judicial recourse, likely in the form of a private right of action based on violations of the statute. The introduction of a private right of action could usefully serve to compress what would otherwise be the lengthy development period of privacy tort law and provide a complementary enforcement tool and an alternative to the current complaint model. We recognize however that for a variety of reasons, including cost, time and access issues, a private right of action would not provide a suitable alternative to the current complaints regime in all cases. This would be taken into consideration in deciding how to exercise our discretion to decline an investigation.

We note that the Government has recently suspended the implementation of certain provisions in Canada's anti-spam legislation (CASL), which would have created a private right of action, allowing lawsuits to be filed for alleged violations of that legislation. It did so on the basis that while Canadians deserve

an effective law, the organizations subject to that law should not bear the burden of unnecessary red tape and costs in order to bring themselves into compliance with it.

We understand the Government's call for balance and are of the view that the introduction of an additional form of judicial recourse under PIPEDA, such as an independent private right of action, could be done in a manner that achieved that balance. Recent developments in Canadian tort law suggest that providing individuals with a private right of action for violations of PIPEDA would be a reasonable evolution of Canada's federal private-sector privacy protection regime. In our view, contrary to some of the red tape concerns expressed in the context of CASL, a more direct route to judicial recourse could in appropriate cases streamline access to effective redress for violations of the Act.

### OPC Actions

- The OPC will continue to enforce Privacy by Design through its accountability guidelines and PIPEDA's accountability principle.
- The OPC intends to adapt our current accountability framework to the needs of small-and medium-sized businesses and help guide their further evolution as they grow and mature.
- The OPC will make more frequent and strategic use of its power to conduct Commissioner-initiated investigations that focus on chronic or sector-specific problems, or other privacy issues related to opaque business models and uses of personal information.

### OPC Recommendations

- The government should amend PIPEDA to:
  - include a legislated requirement for demonstrable accountability;
  - give the Commissioner order-making powers and the ability to impose administrative monetary penalties;
  - give the Commissioner the power to conduct compliance reviews on demand, without grounds to believe that a PIPEDA violation has occurred
  - give the Commissioner the choice to investigate individual complaints or not, in order to focus limited resources on issues that pose the highest risk or may have greatest impact for Canadians; and
  - give individuals a private right of action for PIPEDA violations.



## ***Conclusion and next steps***

---

Consent remains central to personal autonomy, but in order to protect privacy more effectively, it needs to be supported by other mechanisms, including independent regulators.

In issuing these recommendations and proposed guidance, our intention is to ensure that the consent individuals provide is truly meaningful. We encourage organizations to be innovative in their approach to obtaining consent, to do a better job of harnessing technology to de-identify, and to be accountable for protecting personal information throughout its lifecycle. We also recommend that Parliament and government seriously consider the importance of certain needed amendments and a robust enforcement framework to protect Canadians' personal information in the 21<sup>st</sup> century and help uphold their trust in the digital economy.

## PIPEDA STUDY

The *Personal Information Protection and Electronic Documents Act*, or PIPEDA, sets out ground rules for the management of personal information in the private sector. The legislation balances an individual's right to the privacy of personal information with the need of organizations to collect, use or disclose personal information for legitimate business purposes. While its coming into force in 2001 was a milestone in the protection of Canadians' privacy, it has in many ways been overtaken by technology. Though a previous review of the legislation brought certain amendments, rapidly evolving technology brings a degree of change that is challenging the law's effectiveness and sustainability as an instrument for protecting the privacy of Canadians.

### Advice to Parliament

As with the *Privacy Act*, our Office has been advocating for the modernization of PIPEDA for a number of years. Thus, we were pleased when the House of Commons Standing Committee on Access to Information, Privacy and Ethics launched a study of the Act in February 2017.

Certainly, we do not question the important benefits that advances in information and communications technologies bring to individuals. They greatly facilitate communications; they make broadly available information of all sorts; and provide access to products and services from around the world—but these technologies also create important risks. Internet users want to share their views and search sensitive issues like health without fear that these activities will be tracked and shared with others who may have adverse interests.

Prior to the launch of the Parliamentary study, in a [letter to the Committee](#), the Privacy Commissioner outlined a number of concerns with the current legislation and proposed four broad issues as possible

areas of focus for the study. The Commissioner spoke to these same topics—reputation, consent, enforcement and adequacy—in an [appearance before the Committee](#).

Among his messages to the Parliamentary committee, the Commissioner discussed our Office's work on reputation, further outlined below. With respect to consent, he spoke about the need to modernize the current consent model and advised that his report on the matter was forthcoming. On enforcement, the Commissioner emphasized the challenges associated with limited powers and also highlighted the need for more proactive compliance activities.

The Commissioner also reminded Parliament of the impact of the coming into force in 2018 of the General Data Protection Regulation (GDPR) in the EU and the review of Canada's adequacy status. The EU has noted that Canada's adequacy status is "partial" in that it only covers PIPEDA, and that all future adequacy decisions will involve a comprehensive assessment of the country's privacy regime, including access to personal data by public authorities for law enforcement, national security and other public interest purposes. Given the far-reaching impacts of our country's adequacy status on trade, as well as the differences between the GDPR and PIPEDA, it will be important to keep this consideration in mind as the Committee moves forward with its study.

We look forward to providing further input and advice to the Committee as the study progresses. In particular, our extensive research and analysis on issues, such as consent and reputation, will help inform the recommendations for modernizing PIPEDA that we will be submitting to Parliament. This includes the recommendations for legislative change in the Consent chapter of this report at page 11.

## Reputation

While Canadians recognize the personal and professional benefits of participating in the online world, they are increasingly concerned about their online reputation. On one hand, individuals want an online presence and believe that being selective in what they post will help shape their online reputation. On the other hand, individuals have little control over what others may post about them, or how their personal information might be interpreted by individuals and organizations in other contexts, how long it will be retained, or how it will reflect on their reputation.

In 2016-17, our Office conducted a consultation and call for essays on the issue of online reputation as part of efforts to address one of our strategic privacy priorities—reputation and privacy. This consultation was informed by a [research paper on reputation and privacy](#) prepared by the OPC and published in January 2016. Our consultation solicited input for new and innovative ways to protect reputational privacy, and was aimed at enriching the public debate and ensuring our Office is in a strong position to provide Parliament with a variety of solutions to address issues related to online reputation.

Many of the [submissions we received during the consultations](#) commented on the “right to be forgotten”—in fact, many dealt exclusively with this topic. As defined by the Court of Justice of the European Union, this refers to the right of individuals to request that certain links be removed from search engine results, if those links point to information that is inaccurate, irrelevant, or out-of-date, unless there is a public interest in that information.

While there was recognition of the potential harm that can come from a “net that never forgets”, some submissions raised significant concern about what a formally recognized right to be forgotten would mean for freedom of expression. Others questioned

whether PIPEDA even applies to a number of aspects of online reputation, or to the search engines that are an important part of the debate, calling for other solutions instead. These ranged from greater use of targeted legislation to prevent specific harms, improved education on safe and appropriate use of the Internet (especially for vulnerable populations), and improved practices for websites and online services, such as social networks.

Based on our own research and the input and advice we received through our consultations, we have been looking at new and innovative ways to protect reputational privacy, including whether the right to be forgotten could find application in the Canadian context. PIPEDA does have a number of controls, including the ability to withdraw consent and to challenge the accuracy of information, as well as requiring organizations to retain information only as long as necessary for their stated purposes. There are also other controls emerging outside of PIPEDA, including newly recognized torts,<sup>7</sup> such as the public disclosure of embarrassing private facts, and new federal laws against cyberbullying and revenge porn.

Our investigations of related issues raised by complainants are also helping shape our thinking on the issue of reputation. For example, the Romanian-based website Globe24h.com, which published court decisions from around the world, including Canada, was the subject of numerous complaints to our Office from individuals alleging Globe24h was using their personal information for profit without consent. In 2015, we published the [results of our Globe24h.com investigation](#) on our website.

<sup>7</sup> Wrongful acts that result in injury to a person, his property, reputation or the like and for which the injured party is entitled to compensation.

Following release of our investigation report, a complainant pursued the matter further in Federal Court, seeking damages from Globe24h as well as an enforceable order for the operator of the site to delete all Canadian court and tribunal decisions on its servers. Given the precedent-setting nature of the issues at play, our Office intervened in the litigation. In January 2017, the Federal Court confirmed the findings of our investigation and ordered Globe24h to remove Canadian court and tribunal decisions containing personal information from the website, and to refrain from further copying and republishing Canadian decisions in a manner that contravened PIPEDA. It also ordered the organization to pay for nominal damages incurred as a result of its offside practices.

The decision upholds the application of PIPEDA to the activities of organizations in other countries that involve personal information and that have a real and substantial connection to Canada. It also underscores how increasing trans-border flows of information have created global risks for privacy that require a global response.

Our Office is currently developing a policy position on online reputation which we will share with Parliament before the end of 2017. Ultimately, PIPEDA was good, and in some ways pioneering, legislation when it came into force in 2001 and it continues to provide a sound foundation upon which to build. However, the scale and pace of technological advances and commercial innovations in the years since, while creating remarkable opportunities, are putting significant strain on the ability of individuals to protect their privacy. To address the challenges to privacy in a digital world and to meet the privacy expectations of Canadians, PIPEDA must be modernized.

## PROACTIVE WORK IN SUPPORT OF PRIVACY: HELPING CANADIANS EXERCISE THEIR RIGHTS AND EDUCATING ORGANIZATIONS ABOUT THEIR OBLIGATIONS

---

Protecting Canadians' right to privacy must necessarily involve proactive efforts to help Canadians understand and exercise their rights and to help organizations understand their privacy obligations under federal law.

While OPC investigations of complaints have led to many positive changes to the privacy practices of organizations, the digital age has brought new challenges that we are not always able to address through our complaint-based model—people are unlikely to file a complaint about something they do not know is happening. And in the age of big data and the Internet of Things, it is very difficult to know and understand what's happening to our personal information.

According to our most recent survey, 92 per cent of Canadians expressed concern about the protection of their privacy. Nearly half said they felt as though they've lost control over how organizations collect and use their data. This is certainly troubling—something has to change or we run the risk that Canadians will lose trust in the digital economy, hindering its growth, and limiting their opportunity to enjoy all the benefits afforded by innovation. More fundamentally, it is quite unhealthy in a democracy when most citizens fear one of their basic rights is not being respected.

Moving forward, citizen empowerment will be a standard by which we measure the success of our activities. If our goal is to reduce the proportion of Canadians who are concerned about their privacy, our activities must be seen as useful to both individuals and organizations, and must help the latter reach compliance with Canada's privacy laws.

It should be noted that under PIPEDA, the OPC has a specific mandate to conduct such communications and outreach activities as well as research into privacy issues. In our submissions to Parliament on modernizing the *Privacy Act*, we have recommended that it be amended to provide a similar express authority for the Office to be more proactive with respect to raising awareness about privacy issues in the federal public sector.

Throughout the past year, the Office undertook a wide range of proactive work to support Canadians in the protection of their privacy and assist public sector and private sector institutions and organizations meet their privacy obligations.

### **Information and education for the public**

---

The OPC contributes to public education and awareness of privacy rights and issues through a variety of communications activities, from speaking engagements and special events to engaging Canadians through the media, and the distribution of promotional and educational material through a number of channels.

#### **New OPC website**

The OPC website attracts more than two million visits a year, making it our primary tool for reaching Canadians. In September 2016, we launched a revamped version of the website to make it more citizen-centric and to better meet the needs of its many users. Along with a new design and navigation features, information has been reorganized by topic to make it easier for users to find the information they need.

We have also added a new “feedback” tool visitors can use to tell us whether they found a particular piece of advice or guidance useful or not, and why, helping to inform future improvements.

### *Improve information and advice for Canadians*

In keeping with our goal to simplify public education materials and develop tips and guidance on issues of concern to Canadians, the OPC updated and/or produced new information and advice for individuals on a variety of key issues including, for example, privacy at airports and borders, wearable devices, online privacy, the Internet of Things accessing personal information and direct to consumer genetic testing. We are currently revising the latter in light of the recent adoption of Bill S-201, *Canada’s Genetic Non-Discrimination Act*, a major development for Canadians and one we supported before Parliament earlier this year.

Going forward, the OPC will continue to identify top issues for which information and advice for individuals is either sought or warranted, update or develop that content, and promote it actively through both traditional, as well as newer and innovative, communications and outreach channels.

### *Communications and outreach among vulnerable groups*

The OPC also undertook targeted communications and outreach initiatives to connect with certain vulnerable groups—in particular, seniors and youth—to help them better understand their privacy rights. These groups were identified during our [priority setting](#) exercise as those that would most benefit from receiving more information about and support on privacy issues. Youth—due to their early adoption of new technologies and tendency to share a vast amount of information about themselves online—were seen to be at particularly high risk of potential reputational harm. Seniors, due to their relative inexperience with new online technologies and their vulnerability to identity theft, were also seen to be at extra risk.

Over the past year, we directed a number of outreach initiatives to these two groups. Our seniors campaign involved, for example, placing editorial cartoons and messages on the due-date receipts at libraries across Canada; producing a series of radio spots highlighting issues of concern to seniors, such as identity theft and online privacy; as well as e-blasts to seniors through partners such as the Canadian Association of Retired Persons (CARP) and Fédération de l’Âge d’Or du Québec (FADOQ).

Our youth campaign involved delivering speeches (for example, to the Canadian Teachers’ Federation), exhibits at Parent and Kid Expos and other family oriented events across Canada, and a new OPC Facebook page offering information and advice to parents and the general public about online privacy. We also worked with our provincial and territorial partners, as well as MediaSmarts, to create lesson plans for the classroom, which will be launched in 2017–18. These lesson plans promote the competencies in the [International Competency Framework on Privacy Education](#), which was launched in October 2016 during the International Conference of Data Protection and Privacy Commissioners in Morocco and addresses the necessity and urgency of educating children on data protection and privacy in today’s digital world.

The OPC will be updating its seniors and youth outreach strategies as it continues efforts to support these two groups, including advocating in support of more concrete privacy education in school curricula across Canada.

## **Educating organizations about privacy responsibilities**

---

As mentioned above, PIPEDA provides the Office with a mandate to conduct public education and other activities to promote compliance with the legislation. One of the ways we do this is by undertaking initiatives to educate organizations about their privacy obligations.

### **Small business outreach**

The results of OPC's business poll suggest that small businesses have lower levels of awareness of privacy responsibilities than larger organizations, and the fewer the number of employees, the lower the level of awareness within an organization. We have engaged in a multi-year strategy aimed at helping small businesses better understand privacy responsibilities and comply with privacy law. That strategy takes both a sectoral and a broad-based approach.

In March 2017, we completed phase one of the strategy. Over the course of 18 months we focussed outreach on the rental accommodations and retail sectors—two sectors identified as having the highest number of small business privacy complaints. We met with industry associations, spoke and exhibited at events to reach these groups, produced sector-specific tips to address privacy challenges, and disseminated messages through other direct channels such as their e-newsletters.

We also engaged in activities reaching out to small businesses at-large. For example, we gave presentations to small businesses and exhibited at events in various cities across Canada, organized with Chambers of Commerce, Facebook and other industry associations geared toward key sectors, included an insert into a Canada Revenue Agency mail-out to over 500,000 small businesses, and promoted privacy advice and guidance via Innovation, Science and Economic Development Canada's popular Business Facebook and Twitter channels.

Moving forward, we intend to continue trying to educate small businesses about their privacy responsibilities. Additional effort will be made in the coming months to increase awareness among new sectors, in particular, online businesses and start-ups, as well as legal professionals.

### **Guidance for organizations**

In addition to the OPC's efforts directed at small businesses, we undertake a number of activities to help organizations in general understand their privacy responsibilities. This outreach and stakeholder relations can be a cost-effective way to promote proactive compliance with PIPEDA. These types of activities also allow the Office to gain valuable perspective and market intelligence on privacy issues, industry practices and consumer concerns, as well as emerging trends, challenges and opportunities.

Activities include, for example, the regular publication of summaries of [investigations into businesses](#), providing concrete examples of how PIPEDA applies to the day-to-day management of personal information by businesses. We reported on 28 cases on our website over the past year.

During 2016-17, the Office also updated existing information and produced new guidance for businesses in a number of different areas. This included information on the application of specific sections of PIPEDA and addressing employee snooping. Our investigation into a massive breach of the Ashley Madison online dating site also resulted in a number of "takeaways" businesses could use to improve privacy practices.

In addition, following the introduction of Bill S-4, the *Digital Privacy Act*, PIPEDA was amended in 2015 to allow, in certain circumstances, organizations to disclose personal information to another organization without the knowledge or consent of the individual in certain cases relating to investigations or fraud. Businesses were looking to our Office for guidance



on how the new legislation impacted their privacy obligations. We published [guidance on these provisions](#) and reminded organizations that these exceptions, while permissible under certain circumstances, do not permit the indiscriminate disclosure of personal information.

The Office also introduced a new initiative called the *Deconstruction Series*. These seminar-type events provide stakeholders with timely information and in-depth perspective on investigative findings in key cases, and an opportunity to engage in discussion and ask questions. We held two Deconstruction events last year, one focused on the Ashley Madison case and another on the CompuFinder investigation, which involved an OPC investigation under Canada's Anti-Spam Law. Both events were well attended and there are plans to hold more of these events in the future.

The Commissioner and representatives from our Office also made presentations at various conferences and learning events geared to federal public servants on privacy related issues, including, among others, at an ATIP Community Meeting in April 2016 and during a Security Awareness Week event in February 2017. In addition, we developed [key privacy protection tips for federal human resources professionals](#) based on real-life examples of *Privacy Act* investigations by our Office. We continue to liaise with the Treasury Board Secretariat (TBS) on matters related to privacy in the federal government.

In addition to the above, the OPC launched a blog series aimed at demystifying new and emerging information technologies and explain their privacy implications. To date we have shared information about, for example, ransomware, virtual assistants, virtual private networks and authentication.

## **Parliamentary appearances related to PIPEDA**

---

The Office reports to Parliament on issues that impact the privacy rights of Canadians through appearances and submissions to Parliament. In addition to those detailed in the Parliamentary appearances related to the *Privacy Act* section of this report (see page 80), the Office made a number of submissions and appearances in 2016-17 related specifically to issues under PIPEDA, several of which are discussed in detail in other sections of this report. Overall, we are seeing an encouraging increase in the attention given to privacy issues by Parliamentarians.

Throughout the year, our Office made 13 appearances and submitted 16 briefs to Parliamentary committees. In addition to our appearances and submissions on the PIPEDA study, *Privacy Act* reform and National Security related matters, we also advised Parliament on a variety of other issues, including impaired driving and connected and automated vehicles.

### **Connected cars**

The OPC appeared before the Senate Committee on Transportation and Communications as part of its study on the regulatory and technical issues related to the deployment of connected and automated vehicles. Though there are challenges ahead, the connected car and privacy protection are not inherently opposed. With the proper safeguards built in, Canadians may be reassured that their privacy will be protected, and thus better able to take advantage of the benefits of connected and autonomous cars.

As noted in the presentation to the Committee, modern cars are more than vehicles—they have become smartphones on wheels. Sensors capture an increasingly broad expanse of information about vehicle systems—data from which can be extrapolated further information about the vehicle's driver, including how and where they drive. In addition, the growing sophistication and connectivity of so-



called “infotainment systems” provide a conduit for information related to navigation, traffic, weather, or entertainment, such as streaming audio. These systems can be paired with a driver’s phone to enable hands-free communication, also giving the system access to the user’s contact list, as well as incoming calls, text messages and emails.

The Office stated its agreement with others who had appeared before the Committee, stressing the importance of Privacy by Design, whereby companies consider privacy from the outset, and from a whole organization perspective, in the development of new technologies such as the connected car. In the United States, for example, automakers worked together to develop and commit to a series of privacy principles similar to those found in PIPEDA.

The benefits available to Canadians through the arrival of connected and autonomous cars may be significant. However, consumers’ trust in these technologies will only take hold when the appropriate balance between information flow and privacy protection is reached. Our Office is also funding, through our Contributions Program (see below), a project aimed at developing a code of practice for connected cars.

## Research

---

### Contributions program

The OPC funds independent privacy research and related knowledge translation initiatives through its Contributions Program. A total of \$500,000 is available through the program each fiscal year.

The goal of the Program is to generate new ideas, approaches and knowledge about privacy that organizations can apply to better safeguard personal information, and that individual Canadians can use to make more informed decisions about protecting their privacy.

The Office issued three calls for proposals under its Contributions Program in 2016-17, granting funding to 14 [research and knowledge translation projects](#). Issues being studied range from youth privacy online and the privacy implications of genealogical services to the privacy risks of wearable technologies and data anonymization.

Of particular note, we funded a third [Pathways to Privacy Research Symposium](#) this year. Organized by the University of Toronto and titled “Online Privacy: A Human-Centered Approach,” the Symposium explored the values that underlie privacy protection online and examined how these values are threatened by technological developments.

## INVESTIGATIONS UNDER PIPEDA

The Office conducts independent and impartial investigations into the personal information handling practices of businesses subject to PIPEDA.

The overall volume of complaints accepted by the Office remained steady over the past year. We accepted 325 complaints in 2016-17, compared with 332 in the previous year<sup>8</sup>.

As in past years, the financial and internet sector continued to attract a high number of complaints. Together, these sectors accounted for more than a third (35%) of all complaints accepted. In terms of the types of issues we are seeing, more than half of the cases closed over the past year dealt with matters related to consent (30%) and access to personal information (30%).

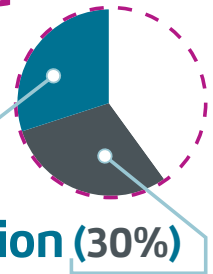
In 2016-17, we completed 294 investigations. The number of cases completed was comparable to the previous year, in which we completed 281.

### PIPEDA INVESTIGATIONS 2016–17

**325 complaints accepted**



**More than half of the 294 cases closed dealt with matters related to consent (30%) and access to personal information (30%)**



<sup>8</sup> "previous year" refers to a 12-month time frame starting April 1, 2015 and ending March 31, 2016. Statistical information for activities under PIPEDA in the [2015-16 Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act](#) reflects a 15 month time frame due to a transition in reporting period from calendar to fiscal year.

### Early resolution

We continued to invest efforts in resolving cases through early resolution, which provides a less formal, more expedient, and cost-effective means of handling relatively straightforward complaints. In 2016-17, we were able to close 70 percent of cases in this way, up from 50 percent the year before. This helped to reduce our overall treatment time for all complaints from an average of seven months in 2015-16 to 5.1 months in 2016-17. Early resolution cases were closed in an average 2.6 months, compared to an average of 10.7 months for complaints that required a full investigation.

### Early resolution case study

In addition to being efficient, early resolution can also achieve broader privacy-enhancing change. The following illustrates how early resolution resulted in improved privacy practices.

The Office received a complaint against an online service company that enables users to access their personal information held by other organizations through their software interfaces. The complainant alleged that an unrelated individual's personal information was being displayed to him, despite repeated attempts to get the service company to correct the problem. We contacted the service company and discovered that the issue was caused by a technical glitch involving another organization's software interface. Through discussions with both the online service company and the other organization, the glitch was corrected for all users, and the complainant's specific issue was resolved to his satisfaction.

As a result of OPC's intervention, the service company:

- changed its internal policies and procedures related to handling privacy concerns brought forward by customers to its Customer Service Center by way of integrating an escalation process to its Chief Privacy Officer;
- collaborated with the other organization to fix the technical issues that caused the inadvertent display of the wrong individual's personal information; and
- developed a multi-year contractual agreement with the other organization to cover any technical issues that may arise in providing services, providing enhanced user consent provisions and expanding on mutual benefits related to compliance with PIPEDA.

### *Declining, discontinuing investigations*

In addition to closing more cases through early resolution, in the interest of maximizing our investigative capacity and efficiency, we have also increased the use of our formal powers under PIPEDA to decline or discontinue remaining complaints when appropriate. This would apply, for example, when someone who has filed a complaint with our Office is also pursuing the matter in the courts. Over the past year, the Office more than doubled the number of declined or discontinued investigations, which now account for roughly 40 percent of our investigations closed outside of early resolution.

### *Making the most of resources*

Despite continued emphasis on resolving complaints through early resolution when appropriate and more judicious use of the authority to decline/discontinue investigations, we cannot keep up with the demands of complex complaints—cases which impacted a large number of individuals or concerned allegations of particularly egregious contraventions of the Act. Emerging technologies, and new business practices and models that use personal information add complexity to these complaints, making it more difficult to conclude investigations within the 12-month service standard specified in the Act.

### *Summaries of key investigations*

As in past years, the question of consent for the collection, use and disclosure of personal information continued to be a recurring theme in the complaint investigations completed in 2016-17. As noted in our report on this issue, consent is becoming increasingly complex in the digital age, and there are many questions about what constitutes publicly available information and how such information may be used. Here are a few key consent-related cases we investigated this past year:

#### **Wajam Internet Technologies—lack of consent to install Adware**

In June 2016, using the authority provided in PIPEDA, the Privacy Commissioner of Canada initiated a complaint against Wajam Internet Technologies Inc. (“Wajam”). This is the second complaint investigated by the OPC related to *Canada’s Anti-spam Legislation* (CASL).

The Canadian company developed a software program called “Wajam” (later re-named and promoted as “Social2Search”) that, once installed on an individual’s computer, tracks the user’s online search queries, and overlays the results with additional search results derived from content shared by an individual’s “friends” and contacts on social media networks. Wajam would also display ads based on the individual’s online searches. The software, installed primarily via third-party distributors, would be bundled as an add-on to other unrelated free software downloaded by individuals.

Our research uncovered a number of IT blogs, articles and anti-virus programs that classified Wajam as Adware or a “Potentially Unwanted Program”. We also noted online comments from users who could not recall consenting to the installation of the software and others stating it was very difficult to uninstall.

*Canada’s Anti-spam Legislation* (CASL) amended PIPEDA to severely restrict the circumstances in which an organization can collect and use personal information without consent, via software that has been installed on an individual’s computer. Our investigation into Wajam highlighted the importance of software developers obtaining meaningful, express, consent for the installation of software resulting in the collection and use of personal information.

Our Commissioner-initiated investigation looked at whether the company was obtaining meaningful consent from individuals to install the software; whether it was preventing users from withdrawing

consent by making it difficult to uninstall the software; and whether the company was adequately safeguarding users' personal information.

Our investigation concluded Wajam contravened PIPEDA in respect of each of the above issues. We also identified contraventions of other PIPEDA principles, including the lack of a privacy management framework (accountability); insufficient transparency about the functioning of the software and its collection and use of user personal information; and the indefinite retention of user personal information.

We made twelve recommendations to bring the company into compliance with PIPEDA. The recommendations included creating a privacy management program, privacy training for staff, improved measures for ensuring consent before installation, more accurate information about the functioning of the software and how user personal information is collected and used, deleting the personal information of users who had uninstalled the software, and the encryption of its main database.

During the course of our investigation, the company stopped distributing the software in Canada. We were ultimately informed that Wajam had sold its assets (including the software) to a company based in Hong-Kong called Iron Mountain Technology Limited (IMTL) and that IMTL did not intend to distribute the software in Canada.

Wajam also indicated that it had ceased to collect personal information from Canadians who had already installed the software and committed to the destruction of all users' personal information remaining in its possession.

For more information, [read the full report of findings from this investigation](#).

### **Publicly available information – Collection and use of personal information for property history reports**

An individual complained that a company in the business of preparing and selling property history reports was collecting, using and disclosing personal information without adequate consent. Information in the property history reports prepared by the company included sales history, insurance claims and whether a property had been used as a marijuana grow operation or to manufacture methamphetamines.

While the company stopped including sales history in its reports, it submitted that the remaining information in question was not subject to the consent provisions of PIPEDA. It asserted that this was not personal information, in that it related to a property, not an individual, and that drug activity information was publicly available.

We accepted that insurance details were not personal information based on the company's confirmation that its reports would only include information about claims for damage to the structure or building (e.g., storm, earthquake, flood, etc.), where a payment was not made directly to the individual.

We found, however, that drug activity does constitute personal information since, either by itself or combined with other readily available information, it could be linked to an identifiable individual (the owner or occupant of the property at the relevant times) and it may reveal that the individual had been involved in drug activity. We also found that such information does not fit within the definition of "publicly available" under the Act, in that information from police, which was used by the organization to deliver its services, does not fall within the specific and limited regulatory definition of publicly available information. We therefore found that this information cannot be collected, used, or disclosed without consent. The company acknowledged that it had not

attempted to obtain individuals’ consent, since it did not believe such information to be personal.

The company, which had stopped issuing its reports pending resolution of the complaint with our Office, agreed to resume doing so without the inclusion of drug activity information.

We therefore considered the matter to be well-founded and resolved. For more information, [read the full report of findings from this investigation](#).

### **Compliance agreements**

The [Digital Privacy Act](#) (formerly known as Bill S-4), received Royal Assent in June 2015, resulting in a number of significant amendments to PIPEDA. Among the changes, a new provision allows the Privacy Commissioner to enter into Compliance Agreements with private sector organizations. These may be used in situations where the Commissioner has reasonable grounds to believe an organization has, or is likely to contravene PIPEDA, or failed to follow a recommendation that would bring it into compliance with the Act.

Under a Compliance Agreement, an organization agrees to take certain actions to bring itself into compliance with PIPEDA, and the Privacy Commissioner agrees not to pursue action against the organization in court.

The Office established the Compliance Monitoring Unit (CMU) in June 2016. The CMU monitors organizations’ adherence to Compliance Agreements and ensures ongoing oversight and timely implementation of recommendations flowing from complaints concluded as “well-founded and

conditionally resolved.” As part of this mandate, the CMU managed the negotiation of our first standalone Compliance Agreement—an agreement that is not linked to a formal investigation following a complaint. A standalone agreement is an effective and cost-efficient way for organizations to assure the OPC that appropriate corrective action will be fully implemented, in situations where full, resource-intensive investigations are not needed to uncover the pertinent facts.

### **Canada’s Anti-Spam Law**

[Canada’s anti-spam legislation](#) (CASL) is the federal law dealing with spam and other electronic threats. The OPC shares responsibility for enforcing CASL with the [Canadian Radio-television and Telecommunications Commission \(CRTC\)](#) and the federal [Competition Bureau](#).

Spam and other electronic threats know no borders and often involve players situated in, or targeting multiple jurisdictions. To help enable domestic and international cooperation in such investigations, we have entered into two Memoranda of Understanding (MOU): the first enables us to share information and collaborate in investigations with our CASL enforcement partners—the CRTC and Competition Bureau; the second enables us to share information and collaborate with international counterparts with similar mandates to combat spam, malware and other electronic threats, through our membership of the [Unsolicited Communications Enforcement Network \(UCENet\)](#).

The Wajam investigation as described on page 46, represents our second CASL-related investigation. As we reported in our [2015–16 Annual Report](#),

we released the findings of our first investigation under the “address-harvesting” provision of PIPEDA (introduced by CASL in July 2014). Sharing information with the CRTC, our Office conducted an [investigation of Compu-Finder](#), a Quebec-based professional training company. The investigation underlined the importance of cooperating with our enforcement partners in bringing anti-spam investigations to a successful conclusion.

After finding the Quebec-based company had used email addresses collected via address-harvesting software for marketing purposes, we entered into our very first voluntary Compliance Agreement. This year, we followed-up with Compu-Finder on implementation of the terms of the agreement and ultimately confirmed that Compu-Finder had satisfied all the agreed measures.

In support of its CASL work, the Office also engages with its international counterparts through UCENet, and with industry partners in the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG). Our participation in such networks helps to increase and share our understanding of online threats and trends alongside methods to combat them. In 2017, we also participated in the first UCENet regulatory “Sweep”, an intelligence-gathering initiative whereby various authorities conduct coordinated research into a specific theme. The exercise, which was inspired by the [Global Privacy Enforcement Network Privacy Sweep](#) (an idea initially conceptualized and developed by our Office), is being led by the CRTC and the UK Information Commissioner’s Office (ICO)

## Breaches

---

As was the case in previous years, we continued to receive a large number of breach reports under PIPEDA—close to 100 in each of the last two years. We expect the number of breach reports to grow significantly when mandatory breach reporting regulations come into force.

### Ashley Madison breach

In August 2016, the OPC issued a news release summarizing the [findings of an investigation into a major privacy breach related to AshleyMadison.com](#). The website, aimed at people seeking a discreet affair, is operated by Ruby Corp. (previously known as Avid Life Media [ALM]). This investigation was carried out in collaboration with the Australian Office of the Information and Privacy Commissioner and the United States Federal Trade Commission, which released its findings later in the year. The case exemplifies how offices half a world apart can work seamlessly to enforce their respective privacy laws.

Our investigation found that safeguards put in place by ALM to protect sensitive personal information were inadequate. The company’s security framework was lacking key elements such as documented security policies or practices and adequate staff training on privacy and security obligations. The case also raised issues at the intersection of privacy and consumer protection law: deception and consent. Our investigation found that the company was marketing itself as a “100% discreet service” but bolstered the claim with a “Trusted Security Award” icon on its homepage that company officials later admitted was fabricated. Investigators concluded the company’s use of a fictitious security trustmark meant individuals’ consent was improperly obtained.

We continue to closely monitor Ruby Corp’s implementation of its commitments to corrective action under a Compliance Agreement. Based on



the important findings on safeguards and other requirements in this investigation, we shared [Takeaways for all organizations](#). In addition, an OPC learning event dedicated to the findings of this investigation attracted significant interest from organizations subject to PIPEDA.

### World Anti-Doping Agency

In September, 2016, the Montreal-based World Anti-Doping Agency (WADA)—which, among other activities, oversees compliance with anti-doping regulations in sports—confirmed its database was accessed inappropriately and athletes’ data was compromised. The compromised information included confidential medical data such as Therapeutic Use Exemptions, which allow athletes to take medications that would otherwise be considered prohibited in order to treat an illness or injury.

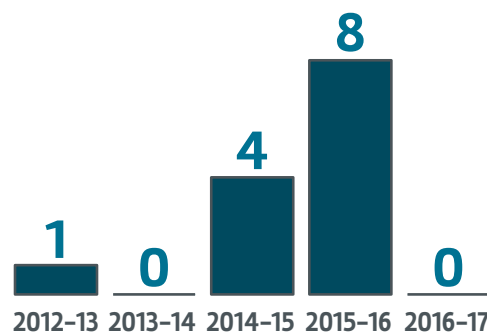
Given the sensitivity of the information, the nature of the breach and the potential impact on the privacy and careers of both Canadian and international athletes, the Privacy Commissioner exercised the authority under PIPEDA to begin a Commissioner-initiated investigation in November, 2016. The investigation is on-going.

### ***Disclosures without knowledge or consent: Notifications received from organizations regarding refusals to provide information to requestors***

Generally speaking, individuals can [request access to information](#) from organizations about disclosures they have made to government institutions pursuant to PIPEDA. However, in certain instances an organization must confer with relevant government institutions to determine whether the information can be disclosed to the requester. The government institution can object to the disclosure of the information for reasons stated under 9(2.3) of the Act, such as national security, money laundering, or the enforcement of any laws. In such instances, the

organization must refuse to provide the information and cannot disclose the fact that the government institution was notified. The organization must also notify the OPC of the refusal without delay.

Over the last 5 years, our Office has received 13 such notifications. Of these, 10 were from the financial sector (banks & credit unions) while the remaining 3 were from the telecommunications sector. Our Office has published a case summary providing guidance for organizations about how to respond to requests about disclosure of personal information to other parties, including law enforcement.



### **NUMBER OF NOTIFICATIONS UNDER 9(2.4)**



## PIPEDA IN THE COURTS

---

In overseeing compliance with PIPEDA, the Office is sometimes involved in judicial proceedings as a party, as an added party, or as an intervener, to seek enforcement of the Act, and/or to assist courts in advancing the legal interpretation and application of the Act.

### *Summaries of key cases*

---

#### *Royal Bank of Canada v. Trang, 2016 SCC 50*

Informed, express consent of the individual is required for the collection, use or disclosure of personal information, but there are exceptions—when necessary to comply with a court order, for example, or when an individual is judged to have given implied consent. In this case, the Supreme Court of Canada (SCC) provided important new guidance on the application of implied consent.

The Royal Bank of Canada (RBC) had obtained a debt-related judgment against two individuals and wanted to proceed with a sale of property owned by the debtors in order to enforce the judgment. Before it could proceed with the sale, RBC needed a discharge statement from another bank to show the current status of the mortgage.

As the property owners could not be located, RBC brought a motion seeking an order that the mortgagee bank produce the statement. The judge at first instance held that he was prevented from issuing such an order by PIPEDA.

On appeal, RBC made a number of arguments, including that the debtors had implicitly consented to disclosure of the statement in such circumstances.

A majority of the Ontario Court of Appeal ruled against RBC, holding that implied consent was absent on these facts and that although RBC could obtain a court order forcing the mortgagee to disclose the statement, the motion before the court did not qualify.

RBC was granted leave to appeal to the SCC. Although not a party to the action, the OPC participated in both the Court of Appeal and SCC appeals as a “friend of the Court.”

The SCC reversed the Ontario decision, holding that the motion originally brought by RBC was enough to ground an order against the mortgagee bank for disclosure of the statement. The SCC also held that the mortgagee bank could rely on the debtors’ implied consent to disclose the statement to RBC.

While confirming that informed consent is a foundational concept of PIPEDA, and generally requires express consent, the SCC also confirmed that an individual’s consent can be implied, but only in strictly defined circumstances. In determining whether implied consent is appropriate, an organization must undertake a contextual assessment of the sensitivity of the information and the reasonable expectations of the individual. Factors relevant to this assessment may include the public availability of related information and the interests and identity of the organization seeking disclosure of the information.

#### *Bertucci v. Royal Bank of Canada, 2016 FC 332*

In another case, the Royal Bank of Canada (RBC) closed accounts belonging to two individuals, but denied their request to see the information on which it based the decision to close the accounts. The individuals complained to the OPC, alleging the bank

was refusing access to their personal information. The OPC found in favour of RBC, on the grounds that releasing the information would reveal confidential commercial information—an exemption allowed under PIPEDA.

The complainants pursued the case in the Federal Court, which found that much of the information held by RBC was not confidential commercial information, but “raw data”—such as a newspaper article about the individuals—and, rather than a blanket refusal, the bank should have given the individuals access to the raw data with the proprietary parts blacked out. The Court noted that the standard for withholding information under the relevant section of PIPEDA is “very high” access to personal information is the rule, and withholding such information is the exception.

# The *Privacy Act*

## A year in review

### PRIVACY ACT REFORM

---

As we mentioned in our 2015-16 Annual Report, the *Privacy Act*, Canada's federal public sector privacy law, has existed virtually unchanged since it was proclaimed in 1983—a time when personal computing was in its infancy; the World Wide Web did not exist; and the creator of Facebook had yet to be born.

There is no question the rapid and persistent advance of digital technologies continues to deliver many advantages, such as improved service delivery and more efficient decision-making, but these technologies are having a profound impact on privacy, creating risks that could not have been imagined when the *Privacy Act* was conceived. Legislative protections once considered ground-breaking are now more than three decades old, and are simply not sufficient to safeguard Canadians' personal information in this new environment. As a result, we risk seeing excessive collection and sharing of personal information by government, massive privacy breaches and waning trust in both the digital economy and our federal institutions.

#### *Parliament takes first steps to modernization*

The Office of the Privacy Commissioner of Canada has long called on government to modernize Canada's public sector privacy legislation. When the House of Commons Standing Committee on Access to

Information, Privacy and Ethics (ETHI) announced in March 2016 that it would undertake a study of the *Privacy Act*, our Office eagerly participated.

In his statements and submissions to Committee, Commissioner Therrien sought to underline the importance of legislative reform and proposed a [series of amendments to address new and emerging threats to privacy](#). In December 2016, after hearing from some 45 witnesses, the Committee issued its final report: [Protecting the Privacy of Canadians: Review of the Privacy Act](#). We were pleased that the Committee concurred with virtually all our recommendations.

We were also pleased to hear the Minister of Justice state in response to the report that her government would lead its own thorough review with the aim of modernizing the *Privacy Act*. Our Office looks forward to participating in that review, which we believe should begin without delay. In doing so, we will continue to focus on the [16 recommendations](#) related to

technological changes, legislative amendments and greater transparency that we presented to ETHI.

A key recommendation proposed by our Office is to amend Section 4 of the *Privacy Act*, which reads: “no personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution.” To date, the OPC has interpreted this to mean that the information being collected must be necessary for the operation of a program or activity. This interpretation is consistent with the TBS [Directive on Privacy Practices](#), in that government institutions should only collect information that is demonstrably necessary or required.

However, this interpretation is not always applied. In fact, the Federal Court recently ruled against a “necessity” threshold (see page 82), in a case that is currently under appeal.

In the interest of greater clarity and certainty of outcome in the application of the *Privacy Act*, we’ve recommended that an explicit necessity requirement for the collection of personal information be included and defined in the Act, bringing the legislation in line with other privacy laws in Canada and abroad.

In our correspondence on this subject with the President of the Treasury Board and the Minister of Justice, the Ministers indicated they would consider this recommendation as part of their ongoing review of the *Privacy Act* and, in the interim, would advise federal institutions to apply the concept of necessity in their collection of personal information.

Prevention being key to protecting privacy, we have also recommended the *Privacy Act* include a specific legal requirement for federal institutions to conduct Privacy Impact Assessments (see page 76) on any new or significantly redesigned programs or services that could impact privacy. They should also be required by law to submit them to our Office so we may make comments and recommendations based on their risk analysis.

We have found, and institutions have told us, that the PIA process is invaluable in identifying and mitigating privacy risks prior to the implementation of a project. While this is a policy requirement, it is not universally followed, and institutions continue to submit PIAs just before, or even after implementing programs.

Similarly, we recommend government institutions be required to consult with our Office on draft legislation and regulations with privacy implications before they are tabled.

## NATIONAL SECURITY, PUBLIC SAFETY, BORDERS AND PRIVACY

---

Government surveillance was identified as one of four strategic privacy priorities on which we would focus our efforts. The goal for our work in this area is to contribute to the adoption and implementation of laws and other measures that will demonstrably protect both national security and privacy.

No one would contest the need to protect the safety of our citizens. Canadians want to be and feel secure, but not at any and all costs to their privacy. What they want is a balanced, well-measured and proportionate approach. It has become far too naive to believe that only “bad people’s” privacy is at stake or “if we have nothing to hide, we have nothing to fear.”

Similarly, everyone can agree that police and national security agencies require adequate tools to fulfill their key role in keeping Canadians safe; and also that these tools need to be adapted to the digital world. However, the powers of police and national security agencies have *already* been significantly increased—in particular with the passage of Bills [C-51 \(Anti-terrorism Act, 2015\)](#) and [C-13 \(Protecting Canadians from Online Crime Act\)](#).

We should remember as well that, during our history, we have seen too many cases of inappropriate and sometimes illegal conduct by state officials that impacted on the rights of ordinary people who were not suspected of criminal or terrorist activities. In our view, these serious incidents were caused by deficient legal standards that failed to set appropriate limits on government actions. Key lessons from history—from the Arar inquiry, to the Snowden revelations about mass surveillance, to more recent cases involving [lawful access \(see OPC op-ed on warrantless access\)](#) and metadata collection by the [CSE \(see OPC 2015–16 Annual Report\)](#), CSIS, and [police in Quebec \(see OPC op-ed on media surveillance\)](#)—remind us that clear safeguards are needed to protect rights and prevent abuse; that national security agencies must be subject to effective review; and that any new state powers must be justified on the basis of evidence.

We have said that through timely and useful advice on Privacy Impact Assessments, Information-Sharing Agreements and regulations, we would seek to reduce the privacy risks associated with the recently adopted *Anti-terrorism Act, 2015*. With regard to the lawful access provisions of Bill C-13, we said we would work with others and provide guidance to both public and private sectors to establish standards for transparency and accountability reports related to the communication of personal information by companies to law enforcement agencies. We also advised that we would examine and report on how national security legislation, such as Bill C-51 is

implemented. In addition, through our review and investigative powers we would examine the collection, use and sharing practices of institutions involved in surveillance activities to ensure that they conform with the *Privacy Act*.

In this section, we focus on the Office's work over the past year in the areas of national security, public safety and issues related to privacy and the border.

### **[Response to government's consultation on Canada's national security framework](#)**

---

In the fall of 2016, the federal government issued a [National Security Green Paper](#), to “prompt discussion and debate about Canada's national security framework.” In the discussion paper, the government suggested that existing state powers may no longer be up to the task of protecting us in the digital era. The paper described a number of areas where the powers of security and law enforcement agencies could be expanded—in many cases, making it easier for these agencies to collect and share Canadians' personal information.

In December 2016, in partnership with provincial and territorial counterparts, the [OPC made a formal submission in response to the National Security Green Paper](#), drawing attention to the privacy risks associated with a number of proposals in the discussion paper. In conjunction with the submission, a press conference was held at the National Press Theatre across from Parliament Hill. Accompanied by Ontario Information and Privacy Commissioner Brian Beamish, and Jean Chartier, President of the Commission d'accès à l'information du Québec, Commissioner Therrien highlighted our views and recommendations.

We said that the government should only propose and Parliament should only approve new state powers if they are demonstrated to be necessary and proportionate—not merely convenient.

The submission stressed the need to address privacy risks related to information sharing and collection of metadata, and raised concerns about government proposals on police access to basic subscriber data held by Internet Service Providers and encrypted communications.

### Metadata

While agreeing generally that law enforcement and national security investigators must be able to work as effectively in the digital world as they do in the physical, in our submission we disputed the notion that legal thresholds and safeguards must be reduced. To the contrary, safeguards which have long been part of our legal traditions must be maintained or further enhanced. They should also be adapted to the realities of modern communication tools, which may hold and transmit large volumes of extremely sensitive personal information.

In our view, it is important to maintain the role of judges in the authorization of warrants for the collection of metadata by law enforcement. Maintaining a judicial role is critical because judges have the necessary independence to ensure the protection of human rights.

Bill C-13, the *Protecting Canadians from Online Crime Act*, already lowered the legal thresholds required to access metadata. Under that legislation, a production order for certain types of metadata can be obtained from a judge only where there are “reasonable grounds to suspect.” Yet law enforcement officials would like existing standards to be further reduced. Do police officers really need access to metadata on less than a reasonable suspicion?

It is unclear to us why these low thresholds do not give law enforcement adequate tools to do their job. Recent cases of metadata collection show that existing standards for accessing metadata should actually

be tightened and privacy protections should be enhanced.

The government’s consultation discussion paper also considered issues related to metadata in the context of national security, but in our opinion failed to reflect the fact that metadata—far from being benign—can reveal much more about people than the actual content of their communications.

While the government maintains that metadata is essential for identifying threats, we said that recent cases demonstrate that CSE and CSIS activities related to metadata can affect the privacy of a large number of Canadians who are not threats to national security. The Commissioner has said these activities should be governed by stronger legal safeguards.

### Encryption

The government’s paper stressed that encryption can be a significant obstacle to lawful investigations and the enforcement of judicial orders.

However, the paper gave little weight to the fact that encryption is an essential tool for the protection of personal information and security of electronic devices such as smart phones. There’s no obvious way to give systemic access to government without simultaneously creating an important risk for the population at large. In our submission, we urged Parliament to proceed cautiously before attempting to legislate solutions in this complex area.

The government is not without rules to assist law enforcement agencies in addressing encryption issues. For instance, Bill C-13 introduced a provision that empowers a judge to attach an assistance order to any search warrant or other form of electronic surveillance. These orders compel any named person, including a suspect, to help “give effect” to the authorization, and these have been used in

investigations to defeat security features or compel decryption keys.

Given the experience and factors noted, the Commissioner said it would be preferable to explore the realm of technical solutions that might support discrete, lawfully authorized access to specific encrypted devices, as opposed to imposing new legislative requirements.

### Information sharing

Our submission noted that Bill C-51 put the privacy of ordinary Canadians at risk with the dramatic expansion of the scale and scope of government information sharing—a problem exacerbated by seriously deficient privacy protections.

We called on the government to consider changes under Bill C-51, specifically relating to provisions that allow for the sharing of personal information deemed merely “relevant” to the detection of new security threats. We emphasized that setting such a low standard is a key reason the risks to law abiding citizens are excessive. If, as stated in the CSIS Act, ‘strictly necessary’ is adequate for CSIS to collect, analyze and retain information, it is unclear why this cannot be adopted for all institutions involved in national security.

Our submission pointed out that the government has not clearly justified its need for the new information sharing provisions. It called for clear limits on how long information be retained; requirements for written information sharing agreements; and a legal obligation to conduct Privacy Impact Assessments to assess and mitigate risks to privacy in all national security programs.

The submission also noted that the information sharing provisions stemming from Bill C-51 are not the only mechanism by which information-sharing for national security purposes takes place. Safeguards such

as necessity and proportionality should apply to all domestic information sharing.

Commissioner Therrien said it’s also important that Parliament, following the lessons of the Arar inquiry, take steps to reduce the risk that information sharing with international partners will lead to serious human rights abuses and violations of Canada’s international obligations.

### Oversight

Commissioner Therrien said he welcomes the government’s plan to create a new National Security and Intelligence Committee of Parliamentarians as a good first step towards democratic accountability. However, he maintained that a review by experts with in-depth knowledge of both the operations of national security agencies and relevant laws is also necessary to ensure rights are effectively protected.

He also pointed out that many institutions with national security obligations, including the Canada Border Services Agency and the Privy Council Office, are not currently subject to dedicated, expert review. In conclusion, we said that this is not the time to further expand state powers and reduce individual rights. Rather, this is the time to enhance both legal standards and oversight to ensure we do not repeat past mistakes; and an opportunity to achieve real balance between security and respect for basic individual rights.

In June, the government tabled Bill C-59. Among other things, the national security bill proposes to create a new National Security and Intelligence Review Agency to oversee national security and intelligence activities across Canada and to investigate complaints related to CSIS, the CSE and the RCMP. It also seeks to create the new position of Intelligence Commissioner. We expect to share our views on this bill with Parliament in due course.



## Audits and reviews related to national security

### Review of SCISA: Operationalization of the Security of Canada Information Sharing Act

The *Security of Canada Information Sharing Act* (SCISA), introduced in January 2015 as part of Bill C-51, was enacted to encourage and facilitate the sharing of information between federal institutions for purposes of national security.

During the past year, we undertook the second phase of our review of the operationalization of SCISA. Whereas the first phase looked primarily at the extent of information sharing activities under the Act, the second part of the review focused on the nature of the information exchanges and mechanisms in place to ensure personal information was handled in accordance with legal and policy requirements.

Our review found significant procedural deficiencies in the operationalization of the Act, specifically relating to a lack of systems or processes for the monitoring and recording of information exchanged under the Act. Record keeping practices varied among institutions and not all disclosures or receipts of information under SCISA were recorded. As a result, we were not provided with complete and reconciled records of information sharing activity under the Act by all institutions. This means that our Office could not review the full extent of information sharing under SCISA and therefore could not assess whether or not all information sharing activity under SCISA was compliant with the *Privacy Act*.

However, for a majority of files we were able to review, disclosures had been made in response to formal requests for information, related to individuals who were the subject of investigations, and the information provided did not exceed the parameters of the request. We also found that many of the proactive disclosures were also preceded by a discussion between the two institutions involved in the exchange. While not systemic in nature, we did find instances where an institution had disclosed information about family members of individuals who were the subjects of an

investigation, and for which there was no evidence that such information satisfied the SCISA threshold of relevance.

Our key observations were that:

- Recordkeeping is incomplete and there is no formal structure in place to track and monitor the exchange of information under SCISA.
- Risk management activities have not been undertaken to identify and mitigate privacy risks related to the Act's operationalization.
- Some internal controls need to be improved to help ensure the proper handling of personal information.

In reflecting on the overall findings of our review, we note that many of our initial concerns with respect to SCISA continue to be relevant. In the absence of formal and standardized recordkeeping of disclosures government-wide and the implementation of robust internal controls, the risk of unauthorized and excessive sharing of personal information remains. And while the vast majority of the files we reviewed showed that the threshold for disclosure was satisfied, the standard of relevance in SCISA is extremely low. The fact that the Act establishes such a low threshold and that it is silent on the proper handling of information subject to disclosure means that a real possibility exists that SCISA will be used as a means to share information with respect to individuals who may not pose a threat to the security of Canada.

The full details of our observations and recommendations and the organization's response can be found in our [Review of SCISA](#).

### Review of the RCMP's Counter-Radicalization to Violence Efforts

The Government of Canada's Green Paper discussed efforts to combat "radicalization to violence". In our response to the Green Paper, we recognized the value of such efforts but noted our concern if prevention activities in this regard involved widespread internet

monitoring. Our submission advocated for an approach which focuses prevention activities or detection efforts on what reliable intelligence reveals are credible threats. It was in that vein that we conducted preliminary inquiries into the RCMP's Terrorism Prevention Program (TPP) in February 2017.

As part the TPP, the RCMP's National Security Intervention Team provides support to national security investigation files related to individuals who have been radicalized to violence but have not met the criminal threshold for charge approval. An assessment is conducted, using a variety of tools, to determine the likelihood of a successful intervention. The National Security Intervention Team has a support function; it does not have an investigative function.

The RCMP has confirmed that it does not utilize mass surveillance techniques or technologies in its efforts to detect and prevent national security threats, nor does it employ broad-based internet monitoring or scenario based targeting. Rather, national security investigations may commence as a result of information from various sources, including family members, the general public or the RCMP's law enforcement and security partners.

### Review of CBSA's Scenario Based Targeting of Travelers—National Security

Under Canadian law<sup>9</sup>, all commercial air carriers must provide the Canada Border Services Agency (CBSA) with Advance Passenger Information/Passenger Name Record (API/PNR) data for all persons travelling to Canada, including name, date of birth, citizenship, contact phone numbers, seat number, payment information and more. The CBSA uses this data to identify individuals who are or may be involved with terrorism or terrorism-related crimes or other

serious offences that are transnational in nature. The Scenario Based Targeting (SBT) program uses advanced analytics to evaluate this data against a set of conditions or scenarios.

Scenarios are made up of personal characteristics derived from API/PNR, such as age, gender, travel document origin, places visited and length and pattern of travel. If an individual matches a scenario, further manual risk assessments are conducted by National Targeting Centre officers. Risk assessments include checking individuals against international and domestic law enforcement and intelligence partners' databases, and may result in the individual being referred as a "target" for closer questioning or examination by a Border Services Officer at the port of entry.

The purpose of our review was to assess whether the CBSA has implemented adequate controls—including policies and procedures—to ensure that personal information handling practices under the SBT program comply with the *Privacy Act* and applicable government of Canada policies, directives, and guidance. We focused our review on scenarios developed for national security purposes, and a sample of files on individuals for whom a target was issued during a one year period between January 31, 2016 and January 31, 2017.

We found that the CBSA has implemented policies and procedures to guide the development and refinement of scenarios, the risk assessment process for individuals, and the evaluation of scenario effectiveness. However, some scenarios are written so broadly that large numbers of individuals—approximately 60,000 a year—are flagged for extra scrutiny based on factors that could include their age, gender, national origin and pattern of travels. Of these, a smaller subset is referred for further examination as a result of a target being issued. During the period we reviewed, 552 individuals had been referred.

<sup>9</sup> The requirement to provide API comes from s. 5(a)-(d) and (f) of the *Passenger Information (Customs) Regulations* (PICR) under the *Customs Act*, and s. 269(1)(a)-(d) and (f) of the *Immigration and Refugee Protection Regulations* (IRPR), under the *Immigration and Refugee Protection Act*.

While we recognize the importance of a program for assessing individuals arriving in Canada for potential national security threats, the vast majority of individuals identified as matching a scenario are found to pose no threat to national security, but their personal information has been collected, assessed and shared with certain of CBSA's domestic and international law enforcement and intelligence partners as part of the risk assessment process. In addition, while the CBSA acknowledges the need to assess scenarios for their potential impact on privacy, human rights and civil liberties, national security scenarios were launched without the benefit of such a review.

We also found that:

- Memoranda of Understanding (MOU) with CBSA's domestic and international partners do not contain specific provisions to limit the retention and use of data that is obtained from CBSA for purposes of database checks, particularly to mitigate against any ongoing suspicion of people who have been determined to not pose a threat to national security;
- The CBSA measures the success of its national security scenarios using wide-ranging criteria that include intermediate outcomes and which are not restricted to national security results; and
- Some personal information that is not directly related to the program's stated purpose, particularly from social media and about third parties, is collected and retained in CBSA systems.

The CBSA has accepted all of our recommendations.

On July 26, 2017 the Court of Justice of the European Union (CJEU) released its opinion on the compatibility of a proposed Canada-EU agreement on the transfer and processing of PNR data. The

EU-Canada agreement had been signed in 2014, but was subsequently referred to the CJEU by the European Parliament for a ruling on the agreement's compatibility with EU law, particularly with regard to the respect for private life and the protection of personal data. In its opinion, the Court noted that the agreement did not meet legal requirements of necessity and proportionality, particularly with regard to the retention of information of individuals found to pose no threat to national security. The CJEU concluded that the provisions of the agreement on the transfer of sensitive data to Canada and on the processing and retention of that data were incompatible with fundamental rights. Ultimately the Court found that the agreement could not be concluded in its current form and it outlined a number of provisions that should be included in a revised agreement.

This opinion further highlights the importance of ensuring that there are strict limits set on the retention and use of API/PNR data and other personal information subsequently collected by the CBSA for the administration of the SBT program, particularly for those individuals who have been assessed as posing no threat to national security.

Details of our observations and recommendations and the organization's response can be found in the full [report on our review of the SBT program](#).

### **Review of the CSIS Operational Data Analysis Centre**

In 2006, the Canadian Security Intelligence Service (CSIS) established the Operational Data Analysis Centre (ODAC). The ODAC provides support to various operational divisions of CSIS by analyzing and exploiting data, including that which is collected under the authority of a warrant under Section 21 of the *CSIS Act*. The ODAC generates intelligence products, linking information across multiple sources and databanks.

In the course of exercising warrants issued by the Court against individuals who pose a security threat, CSIS collects both the content of subjects' communications and their metadata—also known as associated data. Metadata, in a broad context, refers to information about a communication.

Since the ODAC's inception in 2006, CSIS has warehoused all acquired metadata within the ODAC, regardless of whether the content of the original communication was retained. An October 2016 [Federal Court judgement](#) found that CSIS had illegally retained third party, non-threat related metadata. Third party information relates to persons who are not targets of a CSIS investigation; non-threat-related information is information that does not relate to a "threat to the security of Canada", as defined in s. 2 of the CSIS Act.

The Federal Court's decision was clearly an important decision for privacy and for advancing privacy protection. In response, CSIS indicated it would prohibit access to the metadata in question pending its review of the Court's decision. CSIS also reached out to hold discussions with our Office. The Security Intelligence Review Committee (SIRC) was asked by the Minister of Public Safety to oversee the fencing off and control of the metadata in question.

Our review focused on the actions taken by CSIS to address the court's decision regarding the retention of third-party, non-threat related metadata by the ODAC. We have verified that the ODAC historical metadata holdings in the system have been fenced off and are unavailable for use by ODAC analysts until a final decision regarding disposition of the data is made. As well, while we were able to verify sequestration of metadata in the ODAC system, we have been informed that the same information resides elsewhere within CSIS as backups and that efforts are being made to ensure all requisite data is disposed of in accordance with the Court's decision.

We also made inquiries regarding the future management of metadata in the ODAC system. We reviewed the court-imposed rules for assessing third party data and CSIS's plan to operationalize those rules in practice. While work was ongoing at the time of this writing, based on our review, CSIS' plan is in keeping with the court's decision. We note that Bill C-59, tabled in the House of Commons on June 20, 2017, includes provisions dealing with the collection, retention and use of datasets, which would include metadata, by CSIS. This includes a requirement for specific authorizations for the retention of datasets that are not publicly available by the Minister of Public Safety, a new Intelligence Commissioner, and the Courts, depending on the nature of the datasets in question. While it is too early to tell what will become of the Bill, we are satisfied that CSIS's plan in the interim appears, on its face, to be consistent with the court's ruling.

### **Follow up on 2014 Review of Warrantless Access to Subscriber Information**

This year we followed up on our [2014 Review of the RCMP's Warrantless Access to Subscriber Information](#) to determine whether the RCMP had implemented a means to monitor and report on its collection of subscriber information, as recommended by our Office. These actions will contribute to promoting greater transparency surrounding the RCMP's warrantless requests for basic subscriber information (BSI) to Telecommunication Service Providers.

The RCMP stated that, since the release of our report in October 2014, it has established a working group to examine the challenges related to warrantless access to BSI. After the Supreme Court of Canada decision in [R v. Spencer](#), the RCMP now seeks BSI without obtaining a production order only in exigent circumstances.

The issue of BSI and the impact of the Spencer decision have also been studied by a federal, provincial

and territorial Cybercrime Working Group, which has included consultations with members of civil society. The Cybercrime Working Group has been tasked to develop possible options to ensure “appropriate, consistent and rapid” access to BSI by investigative agencies. Results have yet to be presented to the government for consideration.

In light of the fact that BSI is only being provided in exigent circumstances and the government is still examining the implication of Spencer and possible options, the RCMP informed us that it is deferring responding to our recommendation until the Government of Canada determines how it will proceed with an overall approach to transparency reporting to ensure any strategy it may implement does not run counter to potential future government objectives.

We note that warrantless requests made by the RCMP under exigent circumstances are not being tracked separately or reported publicly. As a result, a gap in public sector transparency reporting remains; and private sector organizations only provide limited information on how often this privacy intrusive power is used. More than three years have passed since the Spencer decision was issued and Canadians are still waiting for a modern approach to transparency reporting. We will continue to follow up with the RCMP on this matter.

On this issue, it is important to note that our recommendations on *Privacy Act* reform include a call for federal organizations to be open about the number, frequency and type of lawful access requests they make to ISPs and other private sector organizations entrusted with customer information.

### ***Protection of Canadians at the border***

---

Travellers at Canadian airports and U.S. border crossings are subject to close scrutiny and several layers of security measures. Airports, sea ports, international waterways and land border crossings are significantly different from other public places in Canada because the expectation of privacy is reduced—but this does not mean all rights to privacy are suspended in these environments.

We are seeing more and more expressions of concern from Canadians regarding their rights in these situations. We have a fact sheet for travellers about [privacy at airports and borders](#), that offers advice on what to expect and where individuals can turn for assistance should they believe their rights are being violated. That fact sheet has been a popular page on our website, particularly in recent months.

### ***Searches of electronic devices at Canadian and U.S. borders***

In fact, we recently received several complaints from individuals alleging that Canadian Border Services Officers have asked them to surrender their electronic devices for inspection—smart phones, tablets, laptops—often demanding the password to unlock the devices.

Generally speaking, at border crossings, CBSA officers have widespread powers to stop and search people, and examine their baggage and other possessions. Under Canada’s *Customs Act*, these activities may be conducted without a warrant.

Canadian courts have generally recognized that people have reduced expectations of privacy at border points. In this context, privacy and other Charter rights continue to apply but are limited by state imperatives of national sovereignty, immigration control, taxation and public safety and security. While the law is unsettled, CBSA policy states that examinations of personal devices should not be conducted as a matter

of routine; such searches may be conducted only if there are grounds or indications that “evidence of contraventions may be found on the digital device or media.”

That being said, our investigation into these complaints is ongoing and we will report on our findings in due course.

We have also received a number of questions lately about what Canadians traveling to the U.S. can expect at the border as there have been numerous reports of extensive interrogations by U.S. Customs and Border Patrol (CBP), as well as demands for passwords to electronic devices. We have cautioned Canadians to limit what they bring when travelling, or to remove sensitive information on devices that could be searched.

#### **Bill C-23—the Preclearance Act, 2016**

In June 2016, the government introduced Bill C-23, the *Preclearance Act, 2016*. The Bill would implement the terms of the *Canada-U.S. Agreement on Land, Rail, Marine, and Air Transport Preclearance* signed in March 2015. In essence, it would expand existing provisions under which travellers and goods bound for the U.S. can be precleared in Canada and vice versa. It should be noted that under C-23, body searches, including relatively non-intrusive pat-down searches, require reasonable grounds to suspect in order to be carried out by U.S. officers in Canada.

Our Office has concerns with the Bill as tabled, in light of recent pronouncements by the U.S. administration that it intends to search at its discretion and without legal grounds the electronic devices of any and all aliens who seek to enter the United States. In fact, as noted above, it appears to be happening already. Individuals are being required to provide the passwords for their phones or social media accounts. We are concerned, in part, because it appears that this policy would apply at preclearance locations in Canada.

By contrast, the Government of Canada’s policy is to perform this type of search only if there are grounds or indications that evidence of contraventions may be found on the digital device or media. The search of an electronic device is an extremely privacy intrusive procedure, and has been recognized as such by the Supreme Court of Canada on a number of occasions. The idea that electronic devices should be considered as mere goods and therefore subject to border searches without legal grounds is clearly outdated and does not reflect the realities of modern technology. Consequently, in June 2017, we recommended to Parliament that Bill C-23 be amended to place border searches of electronic devices on the same footing as body searches and therefore that their performance require reasonable grounds to suspect.

As with the existing Preclearance Agreement, under Bill C-23, preclearance officers would be required to comply with the laws of the host country while in that country—that is, CBSA officers working in the U.S. would have to comply with U.S. law, and U.S. officers working in Canada would have to comply with Canadian law, including the Canadian *Charter of Rights and Freedoms*, the *Canadian Bill of Rights*, and the *Canadian Human Rights Act*.

These protections, however, are somewhat hollow. Section 39 of the Bill provides that civil proceedings against the U.S. would be subject to the *State Immunity Act of 1985*, severely limiting access to civil remedies against the U.S. related to the actions of CBP officers performing preclearance duties in Canada. In many situations, it would appear that Canadians who wish to enter the U.S. at preclearance locations in Canada as well as at border points in the U.S., will have to face the difficult choice of either accepting a search of their devices without legal grounds or forego their plans to travel to the U.S.



### **Executive order letter**

Following an Executive Order issued by U.S. President Trump in January 2017, we received a number of inquiries about how it could impact on Canadians. Under the order, U.S. government agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or permanent residents from the protections of the U.S. *Privacy Act*.

In short, we concluded that while Canadians do have some privacy protection in the United States, that protection is fragile because it relies primarily on administrative agreements that do not have the force of law. The Commissioner has written to the Ministers of Justice, Public Safety and National Defence to ask for an explanation of how the Executive Order's implementation may impact on privacy provisions in those agreements. For instance, Canadians would want and deserve to know if the U.S. will continue to honour the privacy protections included in the Five Eyes and Beyond the Border agreements.

The Commissioner has also urged the government to ask that Canada be added to a list of designated countries under the U.S. Judicial Redress Act—a designation that already applies to 26 European countries, allowing their citizens to apply to have certain privacy rights enforced through access to U.S. courts.

As of this writing, the Commissioner was still awaiting a response from the Ministers.

### **Investigations related to national security, public safety and the border**

Over the 2016-17 fiscal year, we completed a number of investigations of complaints from individuals alleging federal agencies involved in national security had abused their rights under the *Privacy Act*. Summaries of several of these investigations

are included here, while other *Privacy Act* related investigations can be found at page 69.

#### **RCMP Canadian Police Information Centre—sharing Canadian's mental health information with U.S. authorities**

An individual alleged that the RCMP inappropriately disclosed information about a suicide attempt to U.S. border officials via the Canadian Police Information Centre (CPIC). Based on that information, she was denied entry to the United States by U.S. Customs and Border Protection (CBP).

Information regarding the complainant's suicide attempt was uploaded to CPIC by the Toronto Police Service (TPS), which responded when the complainant called 911. We noted that once certain types of information are in the CPIC database, they are shared with U.S. law enforcement agencies under the terms of a Memorandum of Cooperation (MOC) between the RCMP and the Federal Bureau of Investigation (FBI). It is our view that, as a signatory to the MOC and steward of CPIC, the RCMP bears responsibility for ensuring that all information shared between Canadian and U.S. agencies is done in accordance with the requirements set out in CPIC policies and the MOC. Moreover, we believe that the level of control that the RCMP has over CPIC makes it responsible for ensuring that all personal information that is shared with US law enforcement agencies via CPIC is done in accordance with the disclosure provisions of the *Privacy Act*.

In reviewing the MOC and CPIC policies, we noted that information in CPIC is “owned” by the agency that contributed the information—in this case, the TPS—and that the authority to use the information can be granted only by the contributing agency. The RCMP confirmed that this requirement was not met in that the complainant's personal information was used by a CBP officer without first obtaining permission for its use from the TPS and verifying its accuracy.



We ultimately found that the disclosure of the complainant's personal information was not authorized under the *Privacy Act*. Its use by CBP for an admissibility assessment was not consistent with the purpose for which it was obtained or compiled by the TPS—that purpose being to assist police officers in providing an appropriate response should they again encounter the complainant during the course of their policing activities. We concluded that information about an attempted suicide can only be shared with U.S. border officials where the individual can reasonably be considered to present a risk to others. There was no evidence to suggest in this case that the complainant posed a threat to public safety. We therefore considered the complaint to be well-founded.

Following numerous exchanges with the RCMP during this investigation, several changes were made to the CPIC policies and system. We provided the RCMP with our [final report of findings, which includes recommendations for additional changes to the CPIC system and CPIC policies](#). In January 2017, the RCMP advised that it did not agree with either our findings or recommendations. Overall, the RCMP takes the position that, the “Report of Findings is silent on acknowledging the crucial duty and role police have in protection of people, even from themselves.”

We recognize the importance of CPIC in enabling law enforcement and public safety partners to work together effectively. We agree with the RCMP that in some circumstances, the sharing of information relating to an attempted suicide could be consistent with the common law duties of police officers to preserve the peace, prevent and investigate crime, and the protection of life and property. However, we are of the view that CBP's admissibility assessment in the circumstances was not consistent with such purposes, and that additional controls should be in place to limit the flow of sensitive non-criminal personal information to U.S. border authorities.

We note that our findings are consistent with those of the Information and Privacy Commissioner of Ontario (OIPC) in the April 2014 report, *Crossing the Line: the Indiscriminate Disclosure of Attempted Suicide Information to U.S. Border Officials* via CPIC. More specially, we agree with the Mental Health Disclosure Test proposed in that report, which provides the circumstances under which the OIPC believes the disclosure of information relating to attempted suicides via CPIC would be warranted. While the RCMP is of the view that this test is too narrow in that it does not allow for disclosure where an individual may present a harm to themselves rather than to others, we note that in contrast, the TPS implemented new practices in August 2015 based on the Mental Health Disclosure Test and several other recommendations in the OIPC's report.

### IMSI Catchers

We investigated a complaint received from OpenMedia relating to the RCMP's refusal to confirm or deny whether it uses cell site simulators (sometimes referred to as “Stingray” devices or “IMSI catchers”) as part of its surveillance activities as had been reported by various media outlets. Typically, we would not disclose the identity of a complainant, but in this case, the complainant issued a press release and gave us explicit permission to disclose this information.

OpenMedia was particularly concerned that the RCMP may be using these types of devices to monitor large groups of people in a given location and that the devices are capable of intercepting the content of voice and text communications and extracting encryption keys that are used to protect data on personal electronic devices. The complainant is of the view that if these technologies are being used, the public has a right to know, since their use has the potential to subject innocent Canadians to privacy violations without their knowledge or consent.

The RCMP provided several media outlets with a “technical briefing” in April 2017. At the briefing, the

RCMP confirmed that it does in fact own and use cell site simulators, which it refers to as Mobile Device Identifiers (MDIs), in the conduct of certain types of investigations. In summary, the RCMP explained that:

- its use of cell site simulators complies with Canadian laws, including the *Charter of Rights and Freedoms*, the *Criminal Code of Canada*, and proper judicial processes as established by either jurisprudence and or common law in the courts; and
- the only personal information collected using its cell site simulators is the international mobile subscriber identity (IMSI) and international mobile equipment identity number (IMEI) associated with cell phones—which are standardized unique numbers that identify a mobile subscriber and device respectively—but they are not capable of collecting private communications, including voice and audio communications, email messages, text messages, contact lists, images, encryption keys or basic subscriber information.

The information provided to the media by the RCMP was consistent with the representations that it had already made to our Office with respect to our investigation. That being the case, we worked to independently verify the technical capabilities of the RCMP's cell site simulators and sought additional information regarding the legal authority under which they are operated, and how the RCMP uses, retains, and disposes of the data collected by these devices.

The RCMP advised that it deployed MDI devices during the course of 125 criminal investigations over the past five years (2011-2016): 91 of those deployments were authorized by a General Warrant; 22 were authorized by a Transmission Data Recorder Warrant; in 13 deployments, no prior judicial authorization was obtained. The RCMP clarified that

of the 13 cases where no warrant was obtained, 7 cases presented exigent circumstances. In Canadian criminal law, “exigent circumstances” exist where a police officer has reason to believe that a particular action is necessary to prevent imminent loss or destruction of evidence or bodily harm or death to any person. A warrant may not be required in these circumstances. In the remaining 6 cases, the RCMP was, at the time of use, acting on legal advice that no warrant was required in order to deploy MDI devices.

The RCMP provided us with demonstration of how it uses its MDI devices and allowed us to inspect the devices themselves. We were able to establish that the MDI devices used by the RCMP are not capable of intercepting private communications such as voice communications, email messages, text messages, contact lists, images, encryption keys or basic subscriber information. We were also satisfied that, where the RCMP had obtained prior judicial authorization, the personal information collected during the MDI deployment was consistent with the *Privacy Act*, and that the collected information was properly segregated, secured, retained, and ultimately destroyed. Our conclusions are supported by a sample warrant provided to us by the RCMP, in which terms and conditions stipulate that all personal information collected using the MDI device will be protected from any use or disclosure for any purpose unless “ordered otherwise by a court of competent jurisdiction.” We are of the view that these terms and conditions provide an important safeguard for the personal information collected by these devices. However, in the six cases where the RCMP did not obtain a warrant and was not presented with exigent circumstances, we are of the view that the collection of personal information was in contravention of the *Privacy Act*.

We therefore concluded that this complaint is not well-founded where the MDI deployments were authorized by warrants. However, in the case of the six deployments of MDI devices for which no

warrants were obtained, and there were no exigent circumstances, the complaint is well-founded. Although we believe that the RCMP was operating in good faith based on legal advice it received, in these six cases, we do not believe the MDI deployments were lawfully executed.

Although we have concluded that the complaint is well-founded in the case of six MDI deployments, we believe that the RCMP has taken appropriate steps to remedy this situation, since it now requires prior judicial authorization for all MDI deployments unless presented with exigent circumstances, in which case a warrant may not be required.

For more information, read the full [report of findings from our RCMP IMSI catcher investigation](#).

Our investigation into another complaint alleging that the Correctional Service Canada (CSC) also used IMSI catchers at Warkworth Institution in Ontario, revealed in a number of media reports, remains ongoing.

### **Parole Board of Canada—denial of access**

In Canada, anyone looking to work or volunteer in a position of trust or authority with vulnerable sectors of the population—such as children, seniors and the disabled—may be required to undergo a Vulnerable Sector Verification (VSV). The VSV is an enhanced criminal record check, and includes confirming whether an individual has ever been granted a record suspension (previously referred to as a pardon) for certain sexual offences—information that would not be revealed through a basic criminal record check.

Under the *Criminal Records Act*, VSVs are obtained through a police service, which submits the individual's fingerprints to the Royal Canadian Mounted Police (RCMP). The RCMP then checks to determine whether the individual has received a record suspension for a relevant offence. Wait times for VSVs can sometimes exceed several months, which

can lead to the individual being denied employment, loss of volunteer opportunities or student placements. The end result is that in certain cases, eligible citizens will be unable to fully engage in activities.

To accelerate screening for its clients, a Canadian background vetting company developed a multi-service screening tool to emulate the lengthy VSV process. The new tool involved submitting a personal information request under the *Privacy Act* to the Parole Board of Canada (PBC). Receiving a response from the PBC that it holds no records pertaining to the requester would be informative in the screening process, as the PBC holds records of people that have been granted record suspensions.

After becoming inundated, the PBC stopped processing these requests by invoking the exemption provisions found at paragraph 22(1)(b) of the *Privacy Act*, which allows a government institution to refuse to disclose information that could be injurious to the enforcement of a law—in this case the *Criminal Records Act*. The PBC also began demanding more than the name and date of birth to prove the requester's identity, such as their Fingerprint Serial number, PBC reference number, and/or a copy of their criminal record.

The company complained to our Office. It alleged the PBC knew very well that most individuals, having never been convicted of an offence, would not possess the identity information it was requesting. The PBC for its part raised a number of arguments to support its actions and cautious approach given the sensitivity of the information involved.

After careful analysis, we agreed with the complainant. In our view, paragraph 22(1)(b) could only be relied upon to refuse to disclose information about a record suspension where there is a potential match but it could not be confirmed that the requester was the subject of the record suspension. Disclosing such sensitive information outside the excepted provisions

of the *Criminal Records Act* could indeed be a violation of that Act. However, providing a response that no records were found does not in our opinion violate the *Criminal Records Act*.

Further, requesting additional identification information from requesters in all cases was not, in our view, reasonable. The exception would be when the PBC uncovers a potential match to a record based on the requester's name and date of birth. In these rare cases, it would be acceptable for the PBC to attempt to further confirm the requester's identity.

We concluded the complaints to be well-founded. The PBC refused to accept our findings and

recommendations and continues to refuse to respond to requests under the *Privacy Act* unless requesters provide the additional identification information.

Following our investigation, the Minister of Public Safety and Emergency Preparedness wrote to our Office indicating that he had tasked his officials to reconcile provisions of the *Criminal Records Act* and the *Privacy Act* and applicable regulations. While we are of the view that the requirements of both Acts are not in conflict, as set out in our [Report of Findings](#), we welcome the opportunity to engage in further discussions with Public Safety Canada in this regard.

## INVESTIGATIONS UNDER THE *PRIVACY ACT*

The OPC is charged with overseeing compliance by federal government institutions with the requirements of the *Privacy Act*. It is legally required to conduct an investigation into all the complaints it receives under this Act.

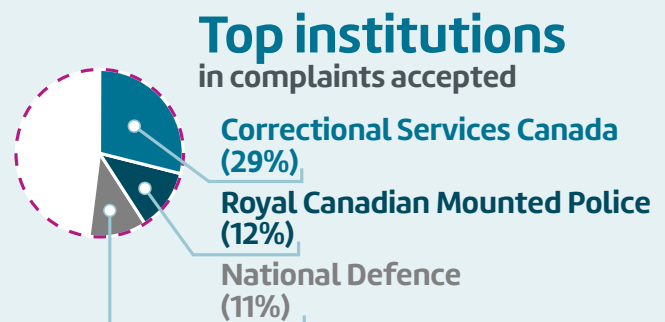
In 2016-17, the Office accepted a total of 1,357 complaints under the *Privacy Act*. This statistic excludes complaints generated under two important scenarios—the receipt of multiple complaints as a result of single incidents, and single individuals submitting multiple complaints.

When compared with the previous year, with multiple complaints excluded, the number of complaints accepted decreased slightly (2%). Nevertheless, over the last five years, the volume of complaints received by the OPC under the *Privacy Act* has increased about 22% (1,114 complaints in 2012-13 to 1,357 in 2016-17).

The Office closed 1,083 investigations under the *Privacy Act*. We continued to complete standard investigations within an average of 10 months in 2016-17, which is consistent with the previous year. However, when we look at the average treatment

### PRIVACY ACT INVESTIGATIONS 2016-17

**1,357** complaints accepted



### Most common types of complaints related to



time for all types of investigations (both standard and early resolution investigations) treatment time did increase slightly this year from 6.7 to 7.4 months. As complaint complexity grows, so does the time required to complete investigations. In turn, our inventory of active complaints over 12 months continues to increase.

### Managing complaints volume

Our multiple complaints strategy was implemented to address situations that could disproportionately impact our investigative resources—where single individuals submit multiple complaints. The strategy limits the number of investigations we undertake for one individual at any given time, allowing us to manage workload and ensure fair distribution of resources amongst all complainants.

In addition, we continue to increase the number of complaints cleared using our early resolution process where appropriate—almost 40 percent of public sector complaints were closed via this approach in 2016-17. However, treatment times for early resolution increased to an average 3.8 months, up from 2.2 months in the preceding year.

We also continue to look for new ways to make the most of our limited investigative resources. For example, over the past year, we have completed implementation of a new risk management framework, supporting our efforts to devote resources to complaints that have the greatest impact on privacy. In addition, work towards modernizing our case management system will help us better identify and report on trends, which will support outreach initiatives with institutions to proactively address privacy issues.

### Summaries of key investigations

---

Under the *Privacy Act*, the Privacy Commissioner of Canada is subject to strict confidentiality obligations, and can make the findings of investigations conducted under the Act public only through annual reports or special reports to Parliament.

While recognizing the importance of confidentiality to facilitating the ombudsman function of the Office, there are cases where releasing the findings of investigations would be in the public interest, in terms of informing parliamentary debate and public discussions in a timely way. As the examples of investigations summarized in this section demonstrate, public disclosure of the “lessons learned” in specific cases can also play a part in encouraging federal institutions to take proactive steps to prevent similar complaints in the future.

In reporting on its study of the *Privacy Act*, the Standing Committee on Access to Information, Privacy and Ethics has endorsed our recommendation to amend the Act to give the Commissioner the discretion to disclose the findings of an investigation when it is considered to be in the public interest to do so—rather than having to wait until the end of the reporting year (see section on *Privacy Act* Reform).

While we look forward to the possibility of legislative reform on this issue, we will continue to highlight key investigations in our reports to Parliament. Here are a few key cases we investigated this year, in addition to [those discussed previously](#).

### Privy Council Office – MyDemocracy.ca website

The Privy Council Office (PCO) launched the MyDemocracy.ca website in early December 2016 as part of a national dialogue on electoral reform. Participants were invited to participate in a survey and provide their opinions on a range of issues related to electoral reform. The website promised that individual

responses to the survey questions would always remain anonymous. After completing the survey questions, the results were displayed to participants in the form of a voter group profile or “Archetype” (Guardians, Challengers, Pragmatists, Cooperators or Innovators). The website encouraged participants to share their results with friends using social media.

We received a complaint alleging that, although the website indicated responses would be anonymous, the website used “Facebook Connect” tracking. The complainant raised concerns that the government may have been using tracking measures while publicly telling citizens that their responses were anonymous.

Our investigation confirmed that the MyDemocracy website was designed to allow for third party involvement, including Facebook (a “third party” in the context of this investigation is understood to include another organization that participates in, or facilitates, or adds content to the website). The Facebook Connect service was installed as a component on the website for sharing results (i.e. a Facebook “share” button).

Our investigation found no evidence that PCO was using measures to identify individual participants in the survey or to track individual responses to the survey questions. However, it was not demonstrated that the MyDemocracy website was designed in a privacy sensitive way.

Our review confirmed that the website design allowed for third party involvement that resulted in the disclosure of IP addresses and other web browsing information to these third parties as soon as the MyDemocracy home page was loaded—before a user specifically opted to initiate or complete a social sharing action. We concluded that, in some cases, this information could have been linked to specific individuals and thus would have constituted a disclosure of their personal information, thereby increasing the risk that users’ interaction with the

website could not be truly anonymous. It was not demonstrated that PCO obtained consent for the sharing of this personal information, and concluded the complaint to be well-founded.

An IP address can, in combination with other information, be used to build comprehensive profiles associated with an identifiable individual, and can be quite revealing about an individual’s Internet-based activities, as research indicates. As a matter of government policy, IP addresses are considered to be personal information.

Based on our technical analysis, a different design of the website could have avoided this premature disclosure of information by only loading third party components when they were needed (i.e. when a user specifically opted to initiate a social sharing action). We found that the sharing of this information was taking place even before individuals had a chance to learn about the website’s practices and make an informed choice about whether or not to interact with the website.

We acknowledge that the Government of Canada must keep pace with and embrace modern technologies and the communication tools offered online. Social media is one such tool that provides for increased connectivity and the opportunity to leverage social interaction as a means to engage with Canadians. The MyDemocracy initiative was an innovative platform to seek the opinions and views of Canadians. However, PCO should have demonstrated greater prudence in assessing the initiative to ensure that privacy risks were identified and mitigated before the website was launched, particularly when promises of anonymity were made.

We made several recommendations to PCO with a view to ensuring that privacy protection is a core consideration in the initial development and administration of any future similar initiatives. We are pleased to note that PCO acknowledged that



the issues we identified serve as a useful reminder about the need to understand online tools so that the safeguarding of individuals' privacy remains a key priority. We are also pleased to note PCO's commitment to protecting the privacy of Canadians and to ensuring that policies continue to adapt to new technologies while supporting the Government's efforts to engage Canadians in innovative ways. Going forward, PCO has also committed to undertaking Privacy Impact Assessments (PIAs) on the design and privacy implications of new projects.

For more information, read the full [report of findings from our investigation of MyDemocracy.ca](#).

### **Health Canada – Collection of personal information for Non-Insured Health Benefits**

A complaint was filed by a Member of Parliament on behalf of more than 20 physicians serving First Nations and Inuit communities, alleging more personal information than necessary was being collected in processing claims under Health Canada's Non-Insured Health Benefits (NIHB) Program.

The NIHB Program provides coverage to registered First Nations and recognized Inuit for health care services not covered by other plans and programs. Our investigation found this complaint to be well-founded, agreeing that the detailed diagnostic information collected by Health Canada was beyond what was needed to process a benefit claim, and had an undue impact on the privacy of First Nations and Inuit patients, particularly considering the sensitivity of personal health information.

During the conduct of our investigation, Health Canada agreed to amend its claim processing form by removing the section that contributed to the over collection of personal information.

For more information, read the full [report of findings from our investigation of the NIHB program](#).

### **Breaches**

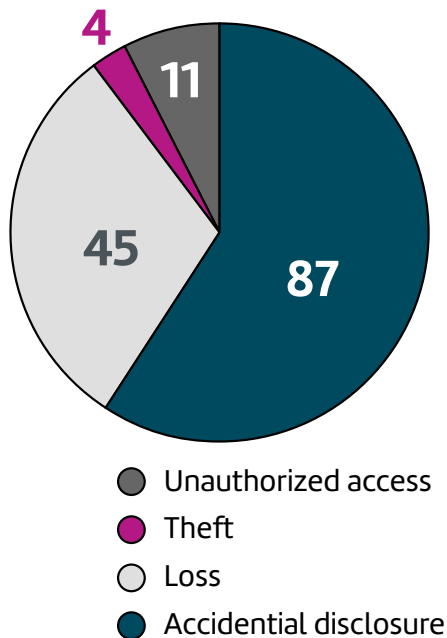
Treasury Board Secretariat policy requires all federal institutions to report material privacy breaches<sup>10</sup> to the OPC. In reviewing these types of incidents, the Office looks at the circumstances that led to the breach—to assess whether it relates to a systemic issue—as well as measures the institution may have taken to mitigate the risk. Depending on what we learn, we may recommend corrective measures to help prevent similar occurrences in the future.

However, not all institutions comply with this Treasury Board policy in all cases. We have recommended the *Privacy Act* be amended to place a specific legal obligation on federal government institutions to report material privacy breaches to our Office. This would ensure we have a better picture of the scope of the problem across the federal government; that we are consulted in the process of responding to the breach and mitigating its impact on individuals; and that we can advise institutions on actions they can take to reduce the risk of future breaches.

To illustrate this reporting incongruity, after steady annual increases since our Office began tracking public sector data breaches, during 2016-17, only 27 federal government institutions out of the more than 250 institutions subject to the Act formally notified our Office of a total of 147 privacy breaches, less than half the number reported the previous year. This drop in notifications was across the board, with one outlier—Employment and Social Development Canada—reporting a great deal more breaches. However, as observed in previous years, just a handful of institutions were responsible for close to two-thirds of the total reports. See Appendix 2—Statistical tables *Privacy Act* breaches by institution.

<sup>10</sup> A material privacy breach has the highest risk impact and is defined as involving sensitive personal information and could reasonably be expected to cause serious injury or harm to the individual and/or involves a large number of affected individuals.





### TYPES OF BREACHES REPORTED

Also consistent with previous years, there was a seemingly negligible number of cyber incidents reported by institutions. In fact, only one web hacking incident was reported in 2016-17. In past years, 2014-15 for example, our Office received only two cyber breach notifications, one involving a cyber intrusion of the National Research Council's network and one related to the infamous Heartbleed vulnerability incident. The Heartbleed matter was also only reported by a single institution—the CRA.

The OPC has raised the matter with the Treasury Board Secretariat and encouraged the federal Access to Information and Privacy (ATIP) community to actively engage Departmental Security Officers and Chief Information Officers to increase their awareness of cyber security incidents.

No clear explanation exists for the significant drop in reported data breaches this year. We will be following up with institutions in the coming months to better understand the decline.

### Summaries of key breaches

#### Phoenix Pay System

Public Services and Procurement Canada (PSPC) administers pay for 101 federal government institutions, with a total of some 290,000 employees, making it one of the largest payroll providers in the country. In early 2016, PSPC launched the Phoenix Pay System, an application developed by IBM. In 2016-17, PSPC notified the OPC of breaches related to the Phoenix system.

At that time, our Office was advised that the breaches involved a limited number of institutions, involved only employee names and Personal Record Identifier (PRI) numbers, and that the information was available only to a limited number of federal public servants. PSPC submitted that, in its view, the risk to affected individuals was “very low”.

Subsequent to receiving the breach reports, we received three complaints about the breaches. The complainants alleged that the breaches were much broader in scope than what had been reported and that PSPC was aware of a potential privacy issue well before the launch of Phoenix. During the initial stage of our investigation, PSPC reiterated in its early representations that the breaches involved a limited number of departments, only involved employee names and PRI numbers, and the information was only available to a limited number of federal public servants. However, the institution added that in at least two cases, the issues that led to the breaches had not been resolved. Our investigation established that at least 11 breaches occurred and the personal information at issue included employee names and PRI, as well as salary information. Most of the vulnerabilities were government-wide, meaning the information of all employees in the Phoenix system at the time of each breach was at risk. We also established that for some breaches, information in Phoenix could be changed and transactions could be conducted. Furthermore, we determined that there

may be persistent vulnerabilities that could lead to future breaches.

Particularly troubling in this case is that PSPC is unable to monitor or audit who accesses personal information used by Phoenix—a feature that is recommended by the Treasury Board to be included in new information technology systems. According to PSPC officials, enabling such a feature would have a substantial impact on the performance of Phoenix. PSPC did clarify, however, that it can audit transactions in Phoenix. Although we found no evidence that the personal information at issue in the breaches investigated was disclosed to individuals outside the government, in other circumstances we have seen cases of employee snooping in other departments as well as PSPC. For example, in April of 2017, PSPC reported another breach to our Office that involved a contract employee who used access to Phoenix to snoop on family members. Generally speaking, identity theft and financial fraud are potential harms that can result from the unauthorized disclosure of personal information.

Our investigation determined that the breaches were the result of a combination of inadequate testing, coding errors, and insufficient monitors and controls of the Phoenix system, and concluded that the complaints were well-founded. We made several recommendations to assist PSPC in resolving the issues that contributed to the breaches, including a recommendation that it develop and implement controls to monitor and document access to personal information held in Phoenix.

The institution accepted most of our recommendations. With respect to the recommendation above, PSPC indicated that it is committed to working toward finding a practical solution. We asked that PSPC follow-up with our Office in six months to report on its progress in implementing our recommendations.

For more information, read the full [report of findings from our investigation of the Phoenix Pay System](#).

### **Public Services and Procurement Canada email disclosure of employees' personal information**

In addition to the Phoenix Pay System breaches, we were informed in September 2016 by PSPC of another breach affecting public servants. PSPC reported that an email from a human resources officer was sent to 180 senior officials in the institution with an attached Excel spreadsheet containing their employees' personal information for HR planning purposes. The attachment also inadvertently contained a tab covering all 14,241 PSPC employees, which included their name, age, gender, salary, pension information, and employment equity status. Our Office subsequently received several complaints from affected individuals. We noted in our follow up that PSPC's containment measures included a key corrective action consisting of a searching deletion command that allowed Shared Services Canada staff to automatically delete the email and attachment from all PSPC accounts. The complaints were resolved through our Early Resolution process to the satisfaction of the complainants in October 2016.

### **Veterans Affairs Canada accidental disclosure of personal health information**

In January 2017, Veterans Affairs Canada (VAC) reported that a letter sent to some 3,300 veterans by Medavie Blue Cross went out in a windowed envelope through which the subject line, "re: Cannabis for Medical Purposes—New Reimbursement Information" was visible. Our Office has received a number of complaints from affected individuals and is investigating the matter.

### **Canada Revenue Agency loss of encrypted data DVD**

Also in January 2017, the Canada Revenue Agency (CRA) notified our Office that a DVD containing

tax information of 28,000 residents of Yukon sent by registered courier to the territorial government never reached its destination. While it is overall concerning that sensitive data of such a large segment of the Canadian population could be put at risk as a result of a shipping process, we were pleased to learn from the CRA that the DVD was password-protected and that the information was encrypted to a very high standard—two recommendations our Office has made with respect to portable storage device use (See our [Tips for Federal Institutions Using Portable Storage Devices](#)). As a result, we were satisfied that the CRA had taken appropriate action to protect the information, and we agreed with the CRA that the risk that taxpayers' information would be compromised was very low, even if an unauthorized individual were to gain possession of the DVD.

### Passports

The Office has received notice of a significant number of breaches, as well as a handful of complaints, related

to the loss and unauthorized disclosure of passport information. Of the 45 incidents of this type reported in 2016–17, close to half involved lost passports.

Our review of these incidents has been complicated by the need to clarify accountabilities—Passport Canada ceased to exist in 2013 and the program became part of Immigration, Refugees and Citizenship Canada (IRCC). Service Canada, which falls under Employment and Social Development Canada (ESDC), has some responsibility for passport operations, including the network of passport offices. In addition, the delivery of passports by the Canada Post Corporation (CPC) is subject to a Memorandum of Understanding between CPC and IRCC. Global Affairs Canada also submitted a handful of breach reports involving passports being lost in transit to, and between, Canadian missions (consulates and embassies) abroad.

## AUDITS AND REVIEWS

The *Privacy Act* and PIPEDA give the OPC the authority to audit the privacy practices of federal institutions and private sector organizations—although, under PIPEDA, the Office cannot launch an audit of a private sector organization unless there is reason to believe the organization has contravened a provision in the Act or is not following a recommendation contained in Schedule 1.

This authority to undertake audits is one of the ways the OPC fulfills its mission to protect and promote privacy rights, enabling the Office to verify that an organization is managing its personal information holdings according to their obligations under the legislation. Among other things, audits may look at the physical and security controls used to protect the personal information that the organization holds; the policies, procedures and practices that are in place; and how the organization manages privacy incidents. In doing so, the Office is able to proactively identify

areas for improvement as well as highlight good privacy practices.

Much of our audit activity during 2016–17 reflected our ongoing concern with the privacy implications of recently enacted legislation and programs related to national security—initiatives which often provide federal institutions with the authority to collect and share great amounts of personal information with limited or no oversight, transparency or accountability.

### ***The Financial Transactions and Reports Analysis Centre***

In addition to the audits related to national security reported on page 54, the Office also conducted its third review of the privacy practices of the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

FINTRAC was established in 2001 under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. Under that legislation, persons and entities in various sectors must scrutinize and report on the financial transactions of clients. These entities—potentially as many as 300,000—transmit reports containing Canadians' sensitive personal information to FINTRAC. Some of these reports may be submitted without the knowledge of the individuals concerned, reporting entities do not require the individuals' consent to submit the reports, and the information may not be accessible to those individuals.

The requirement to safeguard information assets, while common to all government departments, is heightened for organizations such as FINTRAC. The personal information collected by FINTRAC is both highly sensitive and extensive—in 2012, it was estimated the Centre's databases held some 165 million reports containing personal information. Recognizing this, the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* requires the OPC to review the measures taken by FINTRAC to protect information it receives or collects under the Act on a regular basis. We have audited FINTRAC on two occasions in the past. In those audits, [one in 2009](#) and a [second in 2013](#), we identified a number of concerns, and offered a number of recommendations to address these concerns.

### Audit of FINTRAC

We conducted our third audit of FINTRAC during the last fiscal year. In this instance, we focused on the technical structure supporting FINTRAC data and the role of Shared Services Canada (SSC) in safeguarding the IT infrastructure on which FINTRAC information resides. We also reviewed the progress made by FINTRAC in addressing the recommendations from our 2013 audit.

In previous audits, we found that FINTRAC was acquiring and retaining information that exceeded its legislative authority and that FINTRAC's screening and ongoing monitoring of reports needed

improvement to ensure that its information holdings are both relevant and not excessive. In this third audit, while recognizing efforts to improve its privacy practices, we found that FINTRAC had made limited progress in dealing with recommendations from our 2013 audit, notably, to limit the receipt, collection and retention of personal information to only that which is directly relevant to the execution of its mandate. We recommended FINTRAC continue its efforts to implement robust and comprehensive front-end screening for incoming submissions to ensure the records and reports it retains in its database meet legislated reporting thresholds and do not contain unnecessary and/or excessive personal information. We also recommended FINTRAC dispose of reports identified as not meeting reporting thresholds.

Similarly, we also found that while performing compliance activities to ensure reporting entities meet their obligations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, FINTRAC had collected sensitive information unrelated to its compliance activities, such as data relating to employees of reporting entities. This is not in line with FINTRAC internal policies and relevant Treasury Board of Canada Secretariat policies. We recommended FINTRAC undertake an internal data minimization and purging exercise in order to dispose of personal information in its compliance examination files that is not needed to support its work in this regard. We also recommended FINTRAC expand its outreach efforts to specifically address the issue of personal information unnecessarily provided by entities during compliance examinations.

Our current audit identified a number of other privacy concerns, including a lack of a formal agreement between FINTRAC and SSC that clearly defines their respective roles and responsibilities in assuring the security of the IT infrastructure. The current business arrangement between both parties does not include relevant privacy and security requirements for the protection of FINTRAC's information holdings. Without a clear definition of roles and responsibilities, there is a risk that personal

information could be inappropriately accessed, used or disclosed. We recommended FINTRAC work with SSC to develop an agreement to define IT security roles and responsibilities and includes the appropriate privacy and security provisions.

In this most recent audit, we noted that no Security Assessment and Authorization (SA&A) activities had been completed by SSC on the infrastructure supporting FINTRAC systems since it was transferred to SSC in 2012. Instead, we found that FINTRAC had itself updated previous security assessments for its systems without engaging SSC management. SA&A activities are formal and ongoing processes designed to ensure that a system or service has been reviewed for security considerations and any deficiencies identified have been addressed. Failing to assess potential privacy risks via these processes creates the possibility that privacy and security risks to FINTRAC's sensitive information have not been identified and mitigated. We recommended FINTRAC submit a formal request to SSC to initiate the SA&A process to ensure that

the SSC IT infrastructure on which FINTRAC's data resides is certified and accredited.

Entities submit reports about Electronic Funds Transfers of \$10,000 or more to FINTRAC and to CRA. Operationally, reports are transmitted to CRA through a SSC system which does not have a SA&A. Without formal management authorization for this service to operate, there is no certainty that the security requirements established for the service are met and that the controls and safeguards work as intended. Although this is solely the responsibility of SSC, since FINTRAC must use this system, we recommended that FINTRAC submit a formal request to SSC to initiate the SA&A process to ensure the IT infrastructure on which FINTRAC's data flows is certified and accredited.

FINTRAC has accepted all of our recommendations. The full details of FINTRAC's response can be found in our [FINTRAC audit report](#).

## PRIVACY IMPACT ASSESSMENTS

A proactive approach is essential to the protection of privacy—and where prevention is concerned, Privacy Impact Assessments (PIAs) are among the most important tools available to identify and mitigate privacy risks that may be associated with new government programs or services. Government policy requires virtually all federal institutions to conduct a PIA before launching any new or redesigned program or service that could impact privacy. Completed PIAs are submitted to the OPC for review, and the Office may make recommendations to address any privacy concerns identified.

PIAs provide government institutions with an opportunity to demonstrate accountability for the protection of Canadians' personal information. They assist institutions in identifying risks to privacy, assessing their impact and resolving them through the implementation of appropriate mitigating measures.

As departments deploy new technologies and techniques that enable them to collect an ever-growing amount and variety of personal information, the value of comprehensive PIAs in mitigating risks to privacy also increases.

The TBS *Policy on Privacy Protection* requires government institutions to notify the Privacy Commissioner of any planned initiatives (legislation, regulations, policies, programs) that could relate to the Act or to any of its provisions, or that may have an impact on the privacy of Canadians. According to the Policy, this must take place at a sufficiently early stage to allow the Commissioner to review and discuss the issues involved. In addition, the *Directive on Privacy Impact Assessment* specifically emphasizes the crucial role of the PIA in ensuring that privacy implications are resolved *before* government programs or activities involving personal information are launched.

Some government institutions do make positive efforts to consult with our office in advance of implementation of potentially privacy invasive programs and activities, and they submit their PIAs early enough for meaningful advice to be given and to be acted upon. However, there are many instances where we are not consulted on initiatives that have an impact on the privacy of Canadians, and instances where PIAs are not done at all. This includes certain institutions which we know use sensitive personal information to administer potentially privacy invasive programs and activities. This is regrettable.

Equally regrettable is the fact that, even when PIAs are submitted as required, there are many occasions when they are given to our Office very close to, or even after, implementation of a program. Submitting PIAs at a sufficiently early stage permits us to conduct more comprehensive reviews and provide advice, comments, consultation and recommendations in *advance* of program implementation, which substantially reduces the risk of having to consider either ending or modifying programs or services after implementation in order to comply with privacy requirements. The examples cited in this section demonstrate how the Office, based on its reviews of PIAs, can offer recommendations for often simple steps that departments can take to address risks to privacy—as well as the risks involved when PIAs are not submitted in time for a proper review, or when OPC recommendations are not implemented.

Given the key role they can play in protecting privacy, rather than a matter of policy, we believe government institutions should have a legal obligation to conduct PIAs for new or significantly modified programs and submit them to OPC prior to implementation. We have recommended the *Privacy Act* be amended accordingly.

## PIAs in 2016–17

---

In 2016–17, a total of 95 PIAs were submitted to the OPC by 31 different federal institutions. While we review all PIAs, we do not provide detailed comments in all cases—we have a triage function that allows us to focus our resources on the most privacy intrusive initiatives. We sent 22 letters of recommendation following our review of PIAs, offering detailed advice and guidance on how to eliminate, reduce or mitigate privacy risks associated with specific initiatives. In addition, a number of federal departments approached the Office for advice or guidance on a total of 18 potentially privacy intrusive initiatives being considered in advance of a PIA being conducted.

### Statistics Canada: the Canadian Health Measures Survey

The Canadian Health Measures Survey (CHMS) is a national survey led by Statistics Canada, in partnership with Health Canada and the Public Health Agency of Canada. In addition to information about their general health, Statistics Canada collects blood and urine samples from Canadians who volunteer to participate in the survey. After reviewing the PIA on the survey, our Office made a number of recommendations to address risks to the privacy of this highly sensitive personal information.

In response, the agency made a number of privacy-enhancing changes, including the creation of a comprehensive governance structure for the Biobank (where samples are stored). Continuous oversight of the Biobank by three, independent third-party groups was added, and CHMS staff conduct on-site audits of laboratory procedures at the Biobank storage facility on an annual basis.

Statistics Canada also updated the Biobank website, adding a more prominent link to information about how participants can withdraw from the Biobank. Other changes included revising the Information and Consent booklet to include new information on withdrawing samples, and not allowing third-party researchers direct access to personal identifiers or biospecimen.



### **Privy Council Office: Appointment process for the Prime Minister’s Youth Council**

In July 2016, the Prime Minister’s Youth Council, an advisory board that supports the Prime Minister in his role as Minister of Youth, issued a call for applicants. In addition to requesting the biographic and contact information, education and work experience of applicants (aged 16-24), the application also asked them to describe, in a detailed fashion, their personal experiences which, according to the application, may have included stories of immigration, mental or physical health conditions, addiction issues or interactions with the justice system. The application process also involved the use of several third-party vendors.

In response to our recommendations, Privy Council Office (PCO) ceased its use of an open-text field for collecting potentially sensitive personal information in the first step of the on-line application process. It also revised the privacy notice on its website to provide potential applicants with a clear description of the privacy implications of having their personal information stored on the servers of the private sector companies PCO hired to manage the application process.

Based on our PIA review, PCO also revised the PIA to detail security measures and retention timelines to protect personal information collected during the application process. It no longer asks for extensive personal information from backup candidates, unless they have been selected for further evaluation, and clarified that application information held on private servers will be segregated and viewable only by required PCO staff. PCO also updated agreements with its private sector contractors to include specific privacy protections, including written confirmation that personal information collected by the contractors has been purged once it is no longer required for the purposes for which it was collected.

### **Immigration, Refugees and Citizenship Canada: information sharing with the United Kingdom**

Beginning in 2000, the UK Home Office and Immigration, Refugees and Citizenship Canada (IRCC) have exchanged immigration information on a case-by-case basis under a Statement of Mutual Understanding (SMU) for the purpose of administering or enforcing laws governing immigration, citizenship, refugee resettlement and asylum systems. In September 2015, IRCC updated the agreement and added the CBSA as a participant, which prompted the need for a PIA.

In response to our recommendations issued during our review of the PIA for the MOU, IRCC instructed its staff to ensure minimal disclosure of personal information during these exchanges, including a requirement that each disclosure be justified in writing. IRCC also advised that Annexes to the agreement would clearly list what personal information can be disclosed and collected, and that Program Delivery Instructions would be updated to include detailed procedures for collection and disposal of information.

### **RCMP: Canadian Anti-Fraud Centre**

The Canadian Anti-Fraud Centre is the national fraud complaint database in place to collect, store, analyze and disseminate data generated by complainants and victims of fraudulent activities. It assists law enforcement and investigative bodies in detecting, prosecuting and preventing fraud and other economic crime. Given that the Centre houses potentially sensitive information related to suspected perpetrators as well as victims of fraud, our office raised concerns about potential over-collection and extended retention of information.

Based on our recommendations, the RCMP agreed to retain the personal information of complainants and victims of fraud for a maximum 10 years, instead of 20, except when necessary to operations. The RCMP also confirmed it had implemented our recommendation to ensure clear internal guidance, training and monitoring to help ensure the



appropriate collection and use of publicly available personal information related to complaints submitted to the Centre.

### **Treasury Board of Canada Secretariat: Standard on Security Screening**

While the Office had been providing Treasury Board Secretariat (TBS) with ongoing advice and recommendations in the development of a new Standard on Security Screening since 2011, TBS did not submit a PIA until after the Standard came into effect in October 2014.

We have consistently raised concerns regarding the increased scope of security screening processes, which will result in the collection and retention of increased amounts of sensitive personal information. In particular, we have questioned the necessity and effectiveness of credit checks for all positions in the Public Service; the necessity for and accuracy of open source enquiries; and the requirements for the Law Enforcement Records Check (LERC)—a search of police occurrence databases which is more

comprehensive than the Criminal Records Check, and reveals information about a range of an individual's interactions with law enforcement, regardless of whether the individual was convicted of anything.

We advised TBS that the link between the objectives of the Standard and the personal information gathered through each individual measure required by the Standard had not been established, nor had TBS provided analysis to demonstrate that each measure mandated by the Standard is necessary, effective, and the least privacy intrusive measure available.

While TBS accepted some of our recommendations, it proceeded to introduce the Standard in the absence of analysis justifying the increased collection and use of personal information. Departments have until October 2017 to fully comply with requirements of the Standard; however, to date, promised guidance from TBS on implementation has not yet been made available. Our discussions with TBS on the Standard remain ongoing.

## **PUBLIC INTEREST DISCLOSURES**

---

Consent is central to the concept of privacy. Granting or withholding consent to the collection, use or disclosure of their personal information provides individuals with the means to protect their privacy rights.

At the same time, there may be specific circumstances when it is necessary to disclose the personal information of an individual without consent. The provisions of subsection 8(2) of the *Privacy Act* set out the circumstances in which government institutions may disclose personal information without an individual's consent, such as subsection 8(2)(m) which allows for disclosure in situations where the head of the institution believes the public interest in disclosing the information clearly outweighs any resulting invasion of privacy, or when the disclosure would clearly benefit the individual.

It is important to understand that this section of the Act is not intended to deal with the disclosure of personal information on a systematic or routine basis; rather, it is meant to be used only in situations where government institutions must consider the greater public interest, and must balance transparency—the public's right to know—with the right to privacy.

When a federal department or agency is considering a disclosure in the public interest, it is the responsibility of the head of the institution to ensure that the public interest clearly outweighs the privacy concerns of the individual(s) involved. The head of the institution also has a duty to notify the Privacy Commissioner of the proposed disclosure. The Privacy Commissioner does not have the authority to stop the disclosure, but may express concerns about the disclosure and may notify the individual whose information will be disclosed.

During the 2016-17 fiscal year, the Office received notice of 376 disclosures in the public interest. Eighty-nine percent of the notifications received in 2016-17 came from four departments. These included Royal Canadian Mounted Police notices to the media about the release of offenders with a high risk to re-offend, and Employment and Social Development Canada informing police of clients of the Department

who had threatened serious harm to themselves or others.

Reports of investigations into the deaths of members of the Canadian Forces were provided to their next-of-kin by the Department of National Defence. Correctional Services Canada reported similar disclosures to the next-of-kin of inmates who had died in custody.

## PRIVACY ACT RELATED PARLIAMENTARY APPEARANCES

The Office of the Privacy Commissioner of Canada (OPC) reports directly to Parliament, providing input and advice on issues that have the potential to impact on the privacy rights of Canadians.

During 2016-17, the Office made submissions to and appeared before Parliamentary committees on a number of matters related to the *Privacy Act*—most notably on legislative reform, as discussed in some detail earlier in this report.

Other topics on which the Office was asked to provide analysis from a privacy perspective included:

### **Bill C-37: Opening Canadians' mail**

In an [appearance before a Senate Committee to discuss Bill C-37](#), an *Act to amend the Controlled Drugs and Substances Act and to make related amendments to other Acts*, the Privacy Commissioner agreed that allowing customs and border agents to open mail weighing less than 30 grams without consent is justified, given evidence that the international mail system was being used to import drugs responsible for the deaths of a large number of Canadians. However, the Privacy Commissioner also recommended that the bill itself would clearly benefit from additional policy measures to protect Canadians' privacy, specifically, to ensure that correspondence is not read in cases where no contraband is found.

### **Bill C-226: Expanding police authority to conduct random breath tests**

Among other proposed changes to the *Criminal Code*, this *Bill—an Act to amend the Criminal Code (Impaired Driving Act)*—would allow police to demand a breath sample from a driver at any time, even if there was no reason to suspect the person had consumed alcohol. While recognizing the seriousness, societal impact and clear dangers of impaired driving, the [Privacy Commissioner suggested](#) to a Parliamentary committee that the privacy implications of the change be analyzed within a framework based on factors the Supreme Court has taken into consideration in its decisions on the constitutionality of random breath checks.

In addition, the Commissioner expressed concern over a provision that would allow the results of breath and other sobriety tests to be shared for the enforcement of any federal or provincial law, suggesting the Committee examine whether the objectives of these other laws are important enough to justify the sharing of sensitive, state-compelled personal information.

### **Bill C-4: Publication of personal financial information by unions**

Bill C-4, *An Act to Amend the Canada Labour Code, the Parliamentary Employment and Staff Relations Act, the Public Service Labour Relations Act and the Income Tax Act*, would repeal Bill C-377, which required

unions to name and publish the salaries and other personal information of certain of their employees, including information about their political activities. At a committee appearance, while acknowledging the importance of transparency and accountability as fundamental to the effective functioning of robust, democratic institutions, the [Privacy Commissioner expressed support for the Bill](#). In doing so, the Commissioner reiterated his concerns with the previous Bill, noting that efforts to increase transparency must be carefully balanced with the need to protect sensitive personal information. Among others, the Commissioner questioned whether the transparency achieved in forcing unions to name and detail the political activities of specific individuals was proportionate to such a significant intrusion on their privacy.

#### **Bill C-15 the Budget Implementation Act 2016, No. 1 (provisions related to Income Tax Act)**

In addition to collecting taxes, the Canada Revenue Agency (CRA) also collects amounts owing under certain other federal and provincial programs—student loans, for example. As part of the *Budget Implementation Act 2016*, a section of the *Income Tax Act* would be amended to allow CRA personnel involved in tax collection to share “taxpayer information” with CRA personnel engaged in the collection of non-tax debts. As part of a Senate Committee study on the Bill, [our Office cautioned](#) that, although we understood how this amendment would avoid a duplication of efforts and simplify individuals’ interactions with the CRA, the information shared should be limited to that which is necessary to fulfill the stated purpose—that is, the Agency’s collection of amounts owing. This would be consistent with the *Privacy Act*.

We also commented on an amendment that would allow the sharing of taxpayer information with the Office of the Chief Actuary. The amendment allowed certain taxpayer information to be shared solely for the purpose of enabling the Chief Actuary to conduct

actuarial reviews of pension plans established under the *Old Age Security Act* as required by the *Public Pensions Reporting Act*.

We understood that the government’s intention was to mask or de-identify certain information, which we noted should be done in a way that ensures the information cannot be re-identified. As well, we understood that the information to be shared does not include all taxpayer information, but specific data limited to what is necessary to fulfill the legislated mandate. Arrangements would also be developed to include privacy protection measures limiting collection, establishing retention times and providing for the destruction of the information.

Our position was that the privacy principle of exchanging only information that is necessary for the stated purpose be upheld, and that formal information sharing agreements that include privacy protection measures should be established between departments disclosing the information and the Office of the Chief Actuary, as the recipient of the information.

#### **Transfer of Information to the U.S. Internal Revenue Service (IRS)**

Under an agreement enacted in 2014, the Canada Revenue Agency collects information from Canadian financial institutions on certain accounts held by certain U.S. persons, and shares this information with the IRS. While recognizing the legitimacy of information-sharing to fight tax evasion, the [Privacy Commissioner cautioned](#) during a Parliamentary appearance that the personal information collected must be limited to what is necessary, with similar limits on how the information is used, disclosed and retained.

## PRIVACY ACT CASES IN THE COURTS

---

In the past year, our Office has appeared in court on a number of interventions and applications, including among others:

### *Attorney General of Canada v. Larry Philip Fontaine et al*, SCC 37037 (decision under reserve)

The fate of the records created as part of the Independent Assessment Process under the Indian Residential Schools Settlement Agreement (IRSSA) has been the subject of court proceedings in which our Office has participated. As a party to the IRSSA, the Government of Canada argues that the IAP records it holds—which contain the personal stories of abuse told by thousands of residential school survivors—are government files, and thus subject to the provisions of the *Privacy Act*, the *Access to Information Act* and the *Library and Archives Canada Act*.

In 2016, a majority of the Ontario Court of Appeal upheld a lower court ruling, stating that the records do not belong to the federal government, and that it is up to residential school survivors themselves to decide whether their stories should be archived or destroyed after a 15-year retention period.

With intervenor status before the Court of Appeal, our Office assisted the Court in determining whether the level of privacy protection offered by federal privacy and access legislation was compatible with the near-absolute confidentiality negotiated by the parties under the IRSSA. Our Office also underlined the importance of survivors of residential schools retaining control over this highly personal information.

The Attorney General of Canada was granted leave to appeal to the Supreme Court of Canada, which heard the appeal in May 2017. Our Office intervened in the appeal by way of written submissions.

### *Union of Canadian Correctional Officers (UCCO) v. Attorney General of Canada*, 2016 FC 1289 (decision under appeal)

In Federal Court, the union argued that mandatory credit checks for correctional officers, as required by a new Treasury Board Standard on Security Screening, violated both the *Privacy Act* and the *Canadian Charter of Rights and Freedoms*.

The Court found that credit information can help determine whether officers are vulnerable to corruption, thus there is a direct link between collecting officers' credit information and the security screening program—and therefore it is allowed under the *Privacy Act* and reasonable under the Charter.

As an intervenor in the proceeding, our Office argued that, in order to guard against excessive collection of information, government institutions are required to demonstrate the personal information they want to collect is necessary to the effective operation of a program or activity, and not merely helpful or potentially useful.

The Privacy Commissioner reiterated these arguments in a subsequent letter to the President of the Treasury Board and the Minister of Justice, observing that the Federal Court ruling underscores the importance of amending the *Privacy Act* to include an explicit necessity requirement for the collection of personal information, consistent with other privacy laws in Canada and abroad.

The union has appealed the Federal Court's decision. The OPC was granted leave to intervene in the appeal, which is ongoing.

***Oleynik v. Canada (Privacy Commissioner), 2016 FC 1167***

In this case, an individual filed an application in Federal Court, alleging our Office refused to grant access to personal information under its control. The individual questioned whether our Office properly applied various exemptions allowed under the *Privacy Act*, and whether the refusal to search back-up servers for more information was appropriate.

The Court found that in processing the thousands of pages involved in the request, the exemptions applied by the OPC were correct in the vast majority of cases. The Court also upheld our Office's decision not to search back-up servers, agreeing the information sought was not "reasonably retrievable" in the circumstances.

***Alberta (Information and Privacy Commissioner) v. University of Calgary, 2016 SCC 53***

The OPC, the Office of the Information Commissioner and several provincial and territorial information and privacy commissioners filed a joint intervention before the Supreme Court of Canada in a case brought by the Alberta Information and Privacy Commissioner. Our Office and its co-intervenors argued that the Alberta *Freedom of Information and Protection of Privacy Act* gives the Alberta Commissioner the authority to demand access to recordsheld by a public institution, such as a university, even if the institution claims solicitor-client privilege—and that this authority is essential for the investigation of access complaints against public institutions.

The Court ruled against the Alberta Commissioner, finding that the Alberta legislation does not include the explicit authority needed to compel the production of records over which a public body has claimed solicitor-client privilege.

## 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 the 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 STATISTICS

#### PIPEDA 2016–17 – Complaints accepted\* by industry sector

Sector Category	Number	Proportion of all complaints accepted **
Financial	79	24%
Internet	35	11%
Transportation	35	11%
Professionals	33	10%
Telecommunications	31	10%
Services	26	8%
Insurance	19	6%
Sales/retail	19	6%
Other sectors	18	6%
Health	13	4%
Accommodations	6	2%
Government	6	2%
Entertainment	5	2%
<b>Total</b>	<b>325</b>	<b>100%</b>

\* PIPEDA complaints accepted based on count of 1 for series of complaints dealing with related issue; excluded complaints total 30.

\*\* Figures may not sum to total due to rounding.

### PIPEDA 2016–17 – Complaints accepted\* by complaint type

Complaint type	Number	Proportion of all complaints accepted
Access	116	36%
Accountability	0	0%
Accuracy	13	4%
Appropriate purposes	4	1%
Collection	20	6%
Consent	79	24%
Correction/notation	10	3%
Openness	5	2%
Retention	1	0%
Safeguards	26	8%
Use and disclosure	51	16%
<b>Grand total</b>	<b>325</b>	<b>100%</b>

\* PIPEDA complaints accepted based on count of 1 for series of complaints dealing with related issue; excluded complaints total 30.

**PIPEDA 2016–17 – 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	43		8		1		4	1	2		16	59
Government	4		2	1			1				4	8
Not for profit	1										0	1
Transportation	18		2		1					1	4	22
Telecommunications	20		1		1		1		8		11	31
Services	23		4			2	2		1		9	32
Internet	24		8		1					1	10	34
Other sectors	21		5	1	2	1	3	2	3		17	38
Insurance	10		4				1		3	1	9	19
Sales/retail	15				3						3	18
Accommodations	6		3								3	9
Professionals	17						1			1	2	19
Entertainment	3							1			1	4
<b>Total</b>	<b>205</b>	<b>0</b>	<b>37</b>	<b>2</b>	<b>9</b>	<b>3</b>	<b>13</b>	<b>4</b>	<b>17</b>	<b>4</b>	<b>89</b>	<b>294</b>

\* PIPEDA Investigations based on count of 1 for each series of related complaints (32 excluded)

**PIPEDA 2016–17 – 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	68	2		1	2	3	1	2	7	1	87
Use and disclosure	29	8		1	5		6	2			51
Collection	12	2							1		15
Appropriate purposes	2								1		3
Safeguards	16	5					1		2	1	25
Consent	60	16			2		5		2	2	87
Accuracy	8								1		9
Accountability									2		2
Correction/notation	8	3									11
Openness	1	1									2
Identifying purposes									1		1
Retention	1										1
<b>Total</b>	<b>205</b>	<b>37</b>	<b>0</b>	<b>2</b>	<b>9</b>	<b>3</b>	<b>13</b>	<b>4</b>	<b>17</b>	<b>4</b>	<b>294</b>

\* PIPEDA Investigations based on count of 1 for series of related complaints (32 excluded)

**PIPEDA 2016–17 – Investigations average treatment times by disposition (investigations\*)**

Disposition	Number	Average treatment time in months
ER-resolved	205	2.6
Settled	3	7.0
Discontinued (under 12.2)	37	5.5
Withdrawn	9	8.0
No jurisdiction	2	12.0
Not well-founded	13	14.3
Well-founded conditionally resolved	4	21.6
Well-founded resolved	17	18.3
Well-founded	4	13.4
<b>Total cases</b>	<b>294</b>	
<b>Overall weighted average</b>		<b>5.1</b>

\* PIPEDA Investigations based on count of 1 for series of related complaints (32 excluded)

**PIPEDA 2016–17 – Investigations\* average treatment times by complaint and resolution types**

Complaint type	Early resolution		All other resolutions (not ER)		All investigations	
	Number of cases	Average treatment time in month	Number of cases	Average treatment time in month	Number of cases	Average treatment time in month
Access	68	2.7	19	15.5	87	5.5
Accountability			2	18.5	2	18.5
Accuracy	8	2.5	1	7.6	9	3.1
Appropriate purposes	2	4.7	1	12.7	3	7.3
Collection	12	2.1	3	6.3	15	2.9
Consent	60	2.5	27	11.0	87	5.1
Correction/notation	8	3.3	3	5.2	11	3.8
Retention	1	2.4			1	2.4
Identifying purposes			1	7.4	1	7.4
Openness	1	3.4	1	8.0	2	5.7
Safeguards	16	2.2	9	7.3	25	4.0
Use and disclosure	29	2.9	22	8.7	51	5.4
<b>Grand total</b>	<b>205</b>	<b>2.6</b>	<b>89</b>	<b>10.7</b>	<b>294</b>	<b>5.1</b>

\* PIPEDA Investigations based on count of 1 for series of related complaints (32 excluded)



**PIPEDA 2016–17 – PIPEDA voluntary breach notifications – by industry sector and type of incident**

Sector	Incident type			Total incidents per sector	% of total incidents*
	Accidental disclosure	Loss	Theft and unauthorized access		
Accommodation	1			1	1%
Entertainment	1		3	4	4%
Financial	15		9	24	25%
Health	4	1	2	7	7%
Insurance	4			4	4%
Internet			10	10	11%
Not for profit organizations	2		7	9	9%
Other sectors	2		8	10	11%
Sales/retail	1		7	8	8%
Services	3	3	6	12	13%
Telecommunications	3		3	6	6%
<b>Grand total</b>	<b>36</b>	<b>4</b>	<b>55</b>	<b>95</b>	<b>100%</b>

\* Figures may not sum to total due to rounding.

## STATISTICAL TABLES RELATED TO THE *PRIVACY ACT*

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

Respondent	Well-founded	Well-founded resolved	Not well-founded	No jurisdiction	Resolved	Discontinued	ER-resolved	Settled	Grand total
Agriculture and Agri-food Canada							2		2
Bank of Canada						1	1		2
Canada Border Services Agency	6		9		1	2	40		58
Canada Post Corporation	3		1			1	12		17
Canada Revenue Agency		6	7				30		43
Canada School of Public Service		1							1
Canadian Broadcasting Corporation							3		3
Canadian Food Inspection Agency						1			1
Canadian Heritage							1		1
Canadian Human Rights Commission						1			1
Canadian Radio-Television and Telecommunications Commission			2						2
Canadian Security Intelligence Service			15				9		24
Communications Security Establishment Canada							1	1	2
Correctional Service Canada	3	3	15		2	4	67	9	103
Department of Finance Canada			1				1		2
Department of Justice Canada			4			2	2		8
Department of National Defence	3	3	9			2	34		51
Employment and Social Development Canada			2			3	14		19
Environment and Climate Change Canada							10		10
Fisheries and Oceans Canada							2		2
Global Affairs Canada			1		1		9		11
Health Canada	1					2	4		7
Immigration and Refugee Board of Canada							1		1
Immigration, Refugees and Citizenship Canada		1	1			15	16	1	34
Indigenous and Northern Affairs Canada		1	1		1	1			4

Respondent	Well-founded	Well-founded resolved	Not well-founded	No jurisdiction	Resolved	Discontinued	ER-resolved	Settled	Grand total
Innovation, Science and Economic Development Canada		1				1	3		5
Library and Archives Canada							4		4
Marine Atlantic Inc.							1		1
National Energy Board		1				1			2
National Research Council Canada		1					1		2
Natural Resources Canada			2	1	1	1	2	1	8
Office of the Commissioner of Official Languages			1						1
Parks Canada Agency							4		4
Parole Board of Canada	2	1	4				10		17
Privy Council Office								1	1
Public Health Agency of Canada						1	6		7
Public Prosecution Service of Canada		1					3		4
Public Service Commission of Canada						3			3
Public Services and Procurement Canada			1			2	10		13
Revera Inc.		1							1
Royal Canadian Mounted Police	2	1	13		1	5	63	1	86
Security Intelligence Review Committee							2		2
Service Canada			2		2		2		6
Shared Services Canada							1		1
Social Sciences and Humanities Research Council of Canada			1						1
Standards Council of Canada			1						1
Statistics Canada							12		12
Transport Canada						1	2		3
Treasury Board of Canada Secretariat		1				2	1		4
Veterans Affairs Canada			2				4		6
Veterans Review and Appeal Board							2		2
<b>Grand total</b>	<b>20</b>	<b>23</b>	<b>95</b>	<b>1</b>	<b>9</b>	<b>52</b>	<b>392</b>	<b>14</b>	<b>606</b>

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

Complaint type	Count	Average treatment time (months)
<b>Access</b>	<b>245</b>	<b>3.75</b>
Access	234	3.81
Correction – notation	8	3.19
Denial of access	1	0.67
Language	2	2.43
<b>Time limits</b>	<b>32</b>	<b>0.59</b>
<b>Privacy</b>	<b>146</b>	<b>4.46</b>
Use and disclosure	101	4.88
Collection	28	3.58
Retention and disposal	14	3.59
Accuracy	3	2.54
<b>Grand total</b>	<b>423</b>	<b>3.76</b>

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

Complaint tType	Count	Average treatment time (months)
<b>Access</b>	<b>144</b>	<b>18.56</b>
Access	136	18.76
Correction – notation	2	14.10
Language	6	15.59
<b>Time limits</b>	<b>445</b>	<b>5.22</b>
Time limits	399	5.27
Correction – TL	5	9.80
Extension notice	41	4.16
<b>Privacy</b>	<b>71</b>	<b>20.80</b>
Use and disclosure	51	22.22
Collection	16	16.50
Retention and disposal	2	17.92
Accuracy	2	21.94
<b>Grand total</b>	<b>660</b>	<b>9.80</b>

### Privacy Act treatment times – all closed files by disposition

Complaint type	Count	Average treatment time (months)
<b>Standard complaints</b>	<b>660</b>	<b>9.80</b>
Well-founded	412	5.94
Not well-founded	119	15.22
Discontinued	77	11.44
Well-founded resolved	25	32.17
Settled	14	17.03
No jurisdiction	3	10.85
Resolved	10	25.66
<b>ER-resolved</b>	<b>423</b>	<b>3.76</b>
<b>Grand total *</b>	<b>1083</b>	<b>7.44</b>

\* Includes 1 representative complaint for each of several series of related complaints and complaints submitted by a small number of individual complainants; excluded complaints total 4685

**Privacy Act breaches by institution**

<b>Respondent</b>	<b>Incident</b>
Canadian Broadcasting Corporation	2
Canada Revenue Agency	10
Canadian Food Inspection Agency	1
Canadian Institutes of Health Research	1
Communications Security Establishment Canada	1
Correctional Service Canada	12
Employment and Social Development Canada	45
Fisheries and Oceans Canada	2
Global Affairs Canada	10
Health Canada	3
Immigration, Refugees and Citizenship Canada	8
Indigenous and Northern Affairs Canada	4
National Defence	1
Natural Resources Canada	1
Parole Board of Canada	1
Public Health Agency of Canada	1
Public Prosecution Service of Canada	2
Public Safety Canada	3
Public Service Commission Canada	3
Public Services and Procurement Canada	9
Revera Inc.	1
Royal Canadian Mounted Police	14
Shared Services Canada	1
Statistics Canada	3
Transport Canada	5
Treasury Board of Canada Secretariat	2
Veterans Affairs Canada	1
<b>Grand total</b>	<b>147</b>

## Privacy Act complaints and breaches

### Privacy Act complaints 2016–17

Category	Total
<b>Accepted</b>	
Access	424
Time limits	619
Privacy	314
<b>Total accepted*</b>	<b>1357</b>
<b>Closed through early resolution</b>	
Access	245
Time limits	32
Privacy	146
<b>Total</b>	<b>423</b>
<b>Closed through standard investigation</b>	
Access	144
Time limits	445
Privacy	71
<b>Total</b>	<b>660</b>
<b>Total closed †</b>	<b>1083</b>
<b>Breaches received</b>	
Accidental disclosure	87
Theft	4
Loss	45
Unauthorized access	11
<b>Total received</b>	<b>147</b>

\* Includes 1 representative complaint for each of several series of related complaints and complaints submitted by a small number of individual complainants; excluded complaints total 2152

† Includes 1 representative complaint for each of several series of related complaints and complaints submitted by a small number of individual complainants; excluded complaints total 4685



**Privacy Act complaints accepted by complaint type\***

Complaint type	Early resolution		Investigation		Total count	Total percentage**
	Count	Percentage	Count	Percentage		
Access						
Access	251	50%	154	18%	405	30%
Correction – notation	7	1%	4	0%	11	1%
Denial of access	1	0%	0	0%	1	0%
Language	5	1%	2	0%	7	1%
Time limits						
Time limits	32	6%	544	64%	576	42%
Extension	0	0%	41	5%	41	3%
Correction – time limits	0	0%	2	0%	2	0%
Privacy						
Use and disclosure	139	28%	73	9%	212	16%
Collection	40	8%	30	4%	70	5%
Retention and disposal	21	4%	4	0%	25	2%
Accuracy	5	1%	2	0%	7	1%
Grand total	501	100%	856	100%	1357	100%

\* Includes 1 representative complaint for each of several series of related complaints and complaints submitted by a small number of individual complainants (excluded complaints total 2152)

\*\* Figures may not sum to total due to rounding.

### 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	34	27	13	286	24	13	<b>397</b>
Royal Canadian Mounted Police	43	16	2	61	16	24	<b>162</b>
National Defence	42	6	4	78	10	7	<b>147</b>
Canada Border Services Agency	29	6	5	40	18	9	<b>107</b>
Canada Revenue Agency	17	4	2	21	17	4	<b>65</b>
Immigration, Refugees and Citizenship Canada	10	11	1	22	14	2	<b>60</b>
Employment and Social Development Canada	9	4	1	9	9	4	<b>36</b>
Military Police Complaints Commission	0	12	0	16	7	14	<b>49</b>
Canadian Security Intelligence Service	13	17	0	0	0	0	<b>30</b>
Public Services and Procurement Canada	2	3	1	8	10	1	<b>25</b>
<b>Grand total*</b>	<b>199</b>	<b>106</b>	<b>29</b>	<b>541</b>	<b>125</b>	<b>78</b>	<b>1078</b>

\* Includes 1 representative complaint for each of several series of related complaints and complaints submitted by a small number of individual complainants (excluded complaints total 52)

### Privacy Act top 10 institutions in 2016/17 by complaints accepted and fiscal year

Organization	2013/14	2014/15	2015/16	2016/17
Correctional Services Canada	514	314	547	397
Royal Canadian Mounted Police	265	140	120	162
National Defence	84	68	77	147
Canada Border Services Agency	56	66	88	107
Canada Revenue Agency	61	106	85	65
Immigration, Refugees and Citizenship Canada	53	42	44	60
Employment and Social Development Canada	78	35	42	36
Military Police Complaints Commission	0	0	0	49
Canadian Security Intelligence Service	17	21	31	30
Public Services and Procurement Canada	13	9	10	25
<b>Grand total</b>	<b>1141</b>	<b>801</b>	<b>1044</b>	<b>1078</b>

### Privacy Act complaints accepted by institution

Respondent	Early resolution	Investigation	Grand total
Administrative Tribunals Support Service of Canada	0	1	1
Agriculture and Agri-food Canada	2	0	2
Bank of Canada	2	1	3
Canada Border Services Agency	52	55	107
Canada Industrial Relations Board	0	1	1
Canada Mortgage and Housing Corporation	1	0	1
Canada Post Corporation	16	3	19
Canada Revenue Agency	36	29	65
Canadian Air Transport Security Authority	0	2	2
Canadian Broadcasting Corporation	2	0	2
Canadian Food Inspection Agency	1	2	3
Canadian Heritage	1	1	2
Canadian Human Rights Commission	3	3	6
Canadian Museum of History	1	0	1
Canadian Radio-Television and Telecommunications Commission	0	2	2
Canadian Security Intelligence Service	13	17	30
Canadian Transportation Agency	0	1	1
Communications Security Establishment Canada	1	0	1
Correctional Service Canada	71	326	397
Department of Finance Canada	1	4	5
Department of Justice Canada	3	10	13
Department of National Defence	56	91	147
Employment and Social Development Canada	19	17	36
Environment and Climate Change Canada	2	8	10
Financial Transaction and Reports Analysis Centre of Canada	0	1	1
Fisheries and Oceans Canada	5	9	14
Global Affairs Canada	7	2	9
Health Canada	5	7	12
Immigration and Refugee Board of Canada	5	0	5
Immigration, Refugees and Citizenship Canada	25	35	60
Indigenous and Northern Affairs Canada	0	2	2
Innovation, Science and Economic Development Canada	4	2	6

Respondent	Early resolution	Investigation	Grand total
Library and Archives Canada	2	1	3
Marine Atlantic Inc.	1	0	1
Military Police Complaints Commission	7	42	49
National Energy Board	1	1	2
National Research Council Canada	3	0	3
Natural Resources Canada	3	6	9
Office of the Commissioner of Official Languages	0	5	5
Office of the Correctional Investigator	0	1	1
Office of the Information Commissioner of Canada	1	0	1
Parks Canada Agency	2	1	3
Parole Board of Canada	11	4	15
Privy Council Office	0	2	2
Public Health Agency of Canada	4	0	4
Public Prosecution Service of Canada	4	3	7
Public Safety Canada	1	1	2
Office of the Public Sector Integrity Commissioner of Canada	0	1	1
Public Service Commission of Canada	6	9	15
Public Service Labour Relations and Employment Board	1	0	1
Public Services and Procurement Canada	13	12	25
Royal Canadian Mounted Police	61	101	162
RCMP External Review Committee	0	5	5
Security Intelligence Review Committee	0	1	1
Service Canada	3	3	6
Shared Services Canada	1	0	1
Social Sciences and Humanities Research Council of Canada	0	1	1
Statistics Canada	21	1	22
Sustainable Development Technology Canada	1	2	3
Transport Canada	6	11	17
Treasury Board of Canada Secretariat	2	5	7
Veterans Affairs Canada	8	5	13
Veterans Review and Appeal Board	2	0	2
VIA Rail Canada	2	0	2
<b>Grand total*</b>	<b>501</b>	<b>856</b>	<b>1357</b>

\* Includes 1 representative complaint for each of several series of related complaints and complaints submitted by a small number of individual complainants (excluded complaints total 2152)

### Privacy Act complaints accepted by province/territory

Province/territory	Early resolution		Investigation		Total count	Total percentage
	Count	Percentage	Count	Percentage		
Alberta	36	2.65%	80	5.90%	116	8.55%
British Columbia	101	7.44%	144	10.61%	245	18.05%
Manitoba	21	1.55%	18	1.33%	39	2.87%
New Brunswick	13	0.96%	42	3.10%	55	4.05%
Newfoundland and Labrador	2	0.15%	3	0.22%	5	0.37%
Northwest Territories	0	0.00%	0	0.00%	0	0.00%
Not specified	5	0.37%	0	0.00%	5	0.37%
Nova Scotia	13	0.96%	30	2.21%	43	3.17%
Nunavut	1	0.07%	0	0.00%	1	0.07%
Ontario	212	15.62%	362	26.68%	574	42.30%
Other (not US)	6	0.44%	4	0.29%	10	0.74%
Prince Edward Island	0	0.00%	1	0.07%	1	0.07%
Quebec	71	5.23%	148	10.91%	219	16.14%
Saskatchewan	16	1.18%	21	1.55%	37	2.73%
United States	3	0.22%	0	0.00%	3	0.22%
Yukon	0	0.00%	0	0.00%	0	0.00%
Blank	1	0.07%	3	0.22%	4	0.29%
<b>Grand total*</b>	<b>501</b>	<b>36.92%</b>	<b>856</b>	<b>63.08%</b>	<b>1357</b>	<b>100.00%</b>

\* Includes 1 representative complaint for each of several series of related complaints and complaints submitted by a small number of individual complainants (excluded complaints total 2152)

**Privacy Act dispositions by complaint type**

Complaint type	Well-founded	Well-founded resolved	Not well-founded	No jurisdiction	Resolved	Discontinued	ER-resolved	Settled	Grand total
<b>Access</b>									
Access	5	23	67	1	6	28	234	6	<b>370</b>
Correction – notation			1		1		8		<b>10</b>
Denial of access							1		<b>1</b>
Language							2	6	<b>8</b>
<b>Time limits</b>									
Time limits	361	1	14	1		22	32		<b>431</b>
Extension	29	1	9	1		1			<b>41</b>
Correction – time limits	2		1			2			<b>5</b>
<b>Privacy</b>									
Use and disclosure	12		22		2	13	101	2	<b>152</b>
Collection	2		4		1	9	28		<b>44</b>
Retention and disposal						2	14		<b>16</b>
Accuracy	1		1				3		<b>5</b>
<b>Grand total *</b>	<b>412</b>	<b>25</b>	<b>119</b>	<b>3</b>	<b>10</b>	<b>77</b>	<b>423</b>	<b>14</b>	<b>1083</b>

\* Includes 1 representative complaint for each of several series of related complaints and complaints submitted by a small number of individual complainants; excluded complaints total 4685

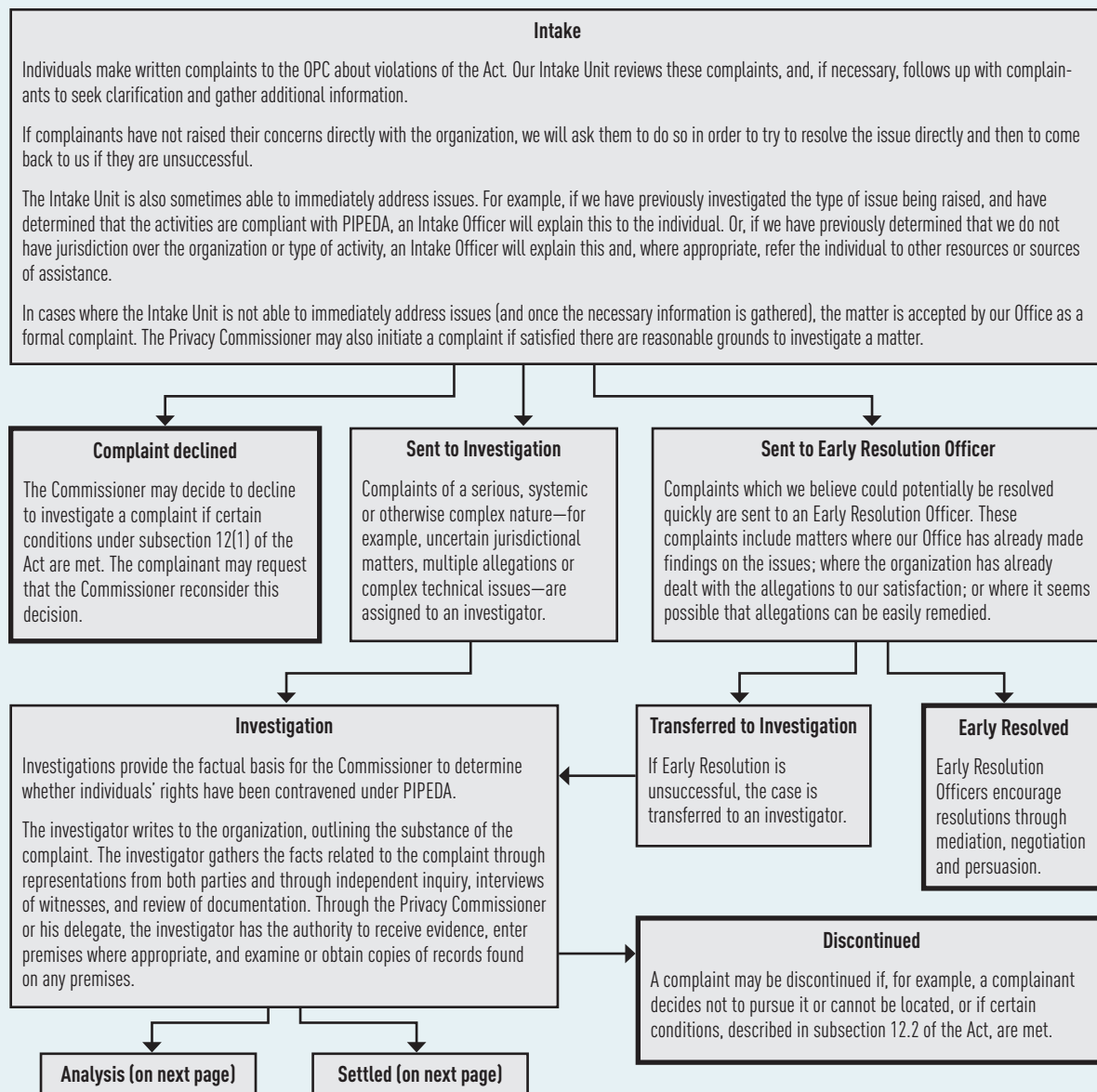


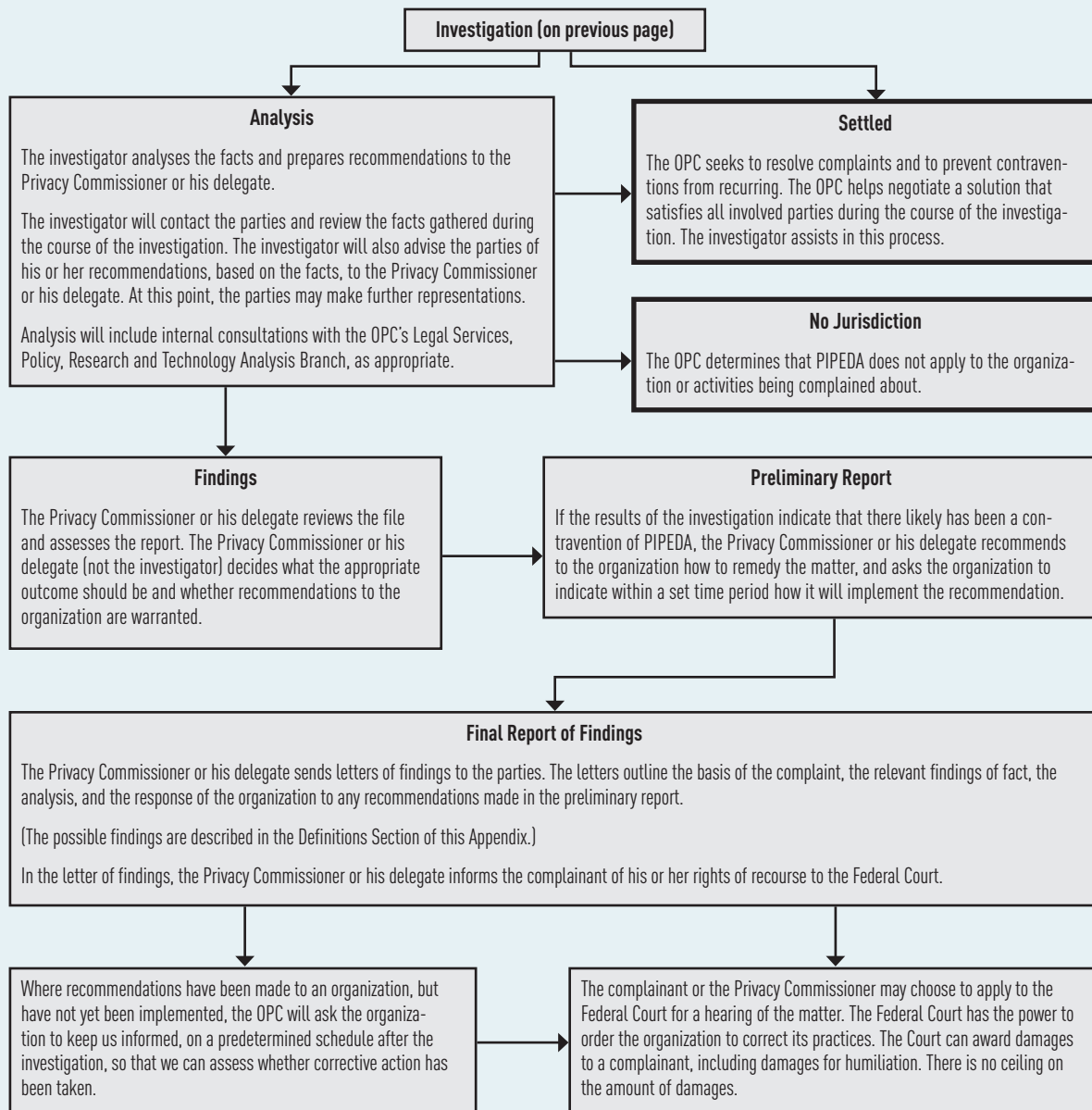
### Privacy Act dispositions of time limits by institution

Respondent	Well-founded	Well-founded resolved	Not well-founded	No jurisdiction	Resolved	Discontinued	ER-resolved	Grand total
Canada Border Services Agency	27		1			6	5	39
Canada Industrial Relations Board	1							1
Canada Post Corporation			1					1
Canada Revenue Agency	20		1			1	2	24
Canada School of Public Service	2							2
Canadian Heritage	1							1
Correctional Service Canada	171		5			10	13	199
Department of Finance Canada	4							4
Department of Justice Canada	1		1					2
Department of National Defence	71		4			2	4	81
Employment and Social Development Canada	8						1	9
Environment and Climate Change Canada	1		2					3
Fisheries and Oceans Canada							2	2
Freshwater Fish Marketing Corporation						1		1
Global Affairs Canada	2							2
Health Canada	2							2
Immigration, Refugees and Citizenship Canada	18		1			1	1	21
Innovation, Science and Economic Development Canada			1				1	2
Military Police Complaints Commission	16							16
Natural Resources Canada	3							3
Parole Board of Canada	1							1
Public Prosecution Service of Canada	2							2
Public Service Commission of Canada	1					2		3
Public Services and Procurement Canada	1						1	2
Royal Canadian Mounted Police	36	2	2	2			2	44
RCMP External Review Committee			2					2
Security Intelligence Review Committee	1							1
Transport Canada	1		1					2
Treasury Board of Canada Secretariat	1		2			2		5
<b>Grand total</b>	<b>392</b>	<b>2</b>	<b>24</b>	<b>2</b>	<b>0</b>	<b>25</b>	<b>32</b>	<b>477</b>

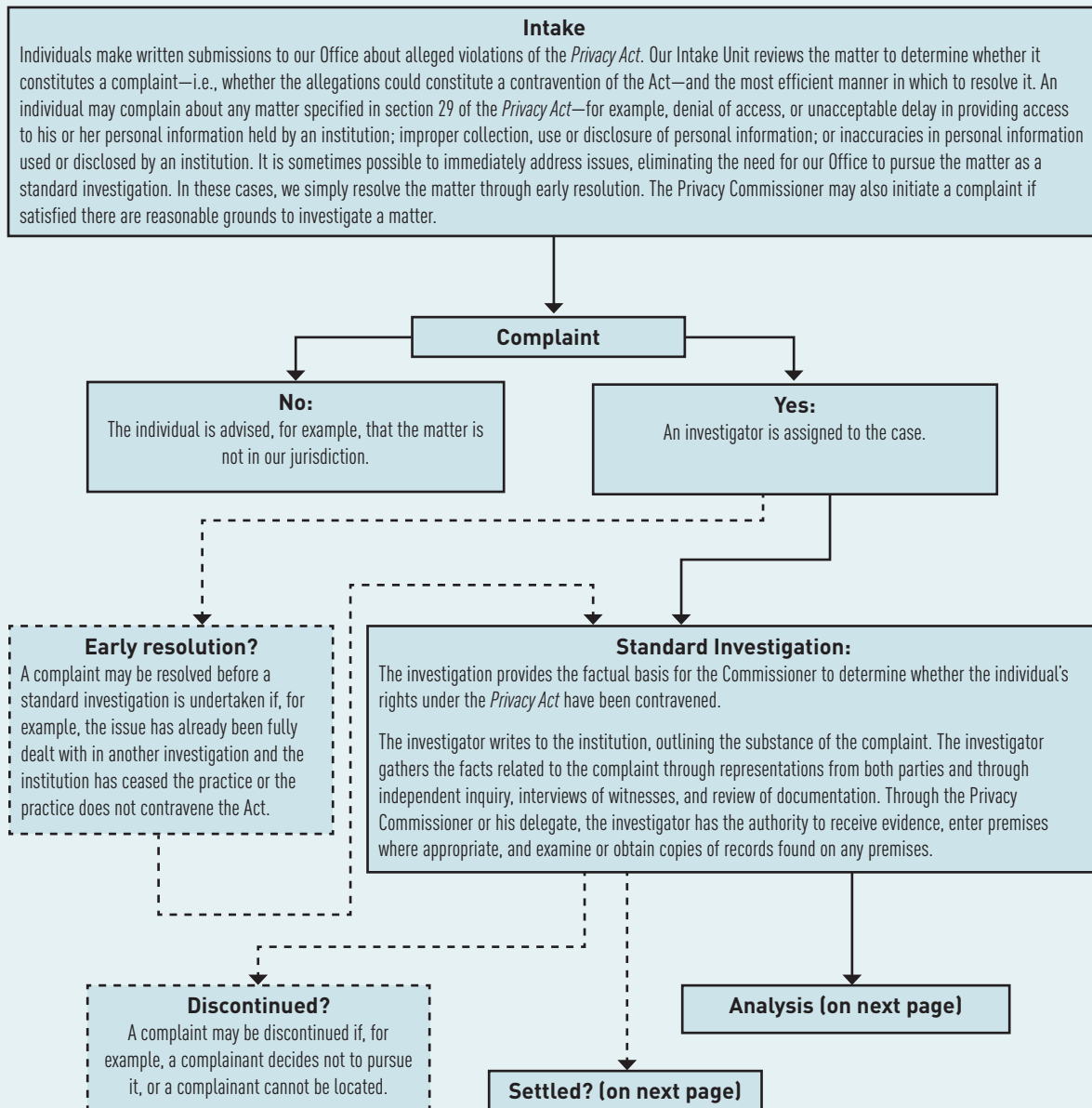
## Appendix 3—Investigation processes

### PIPEDA INVESTIGATION PROCESS

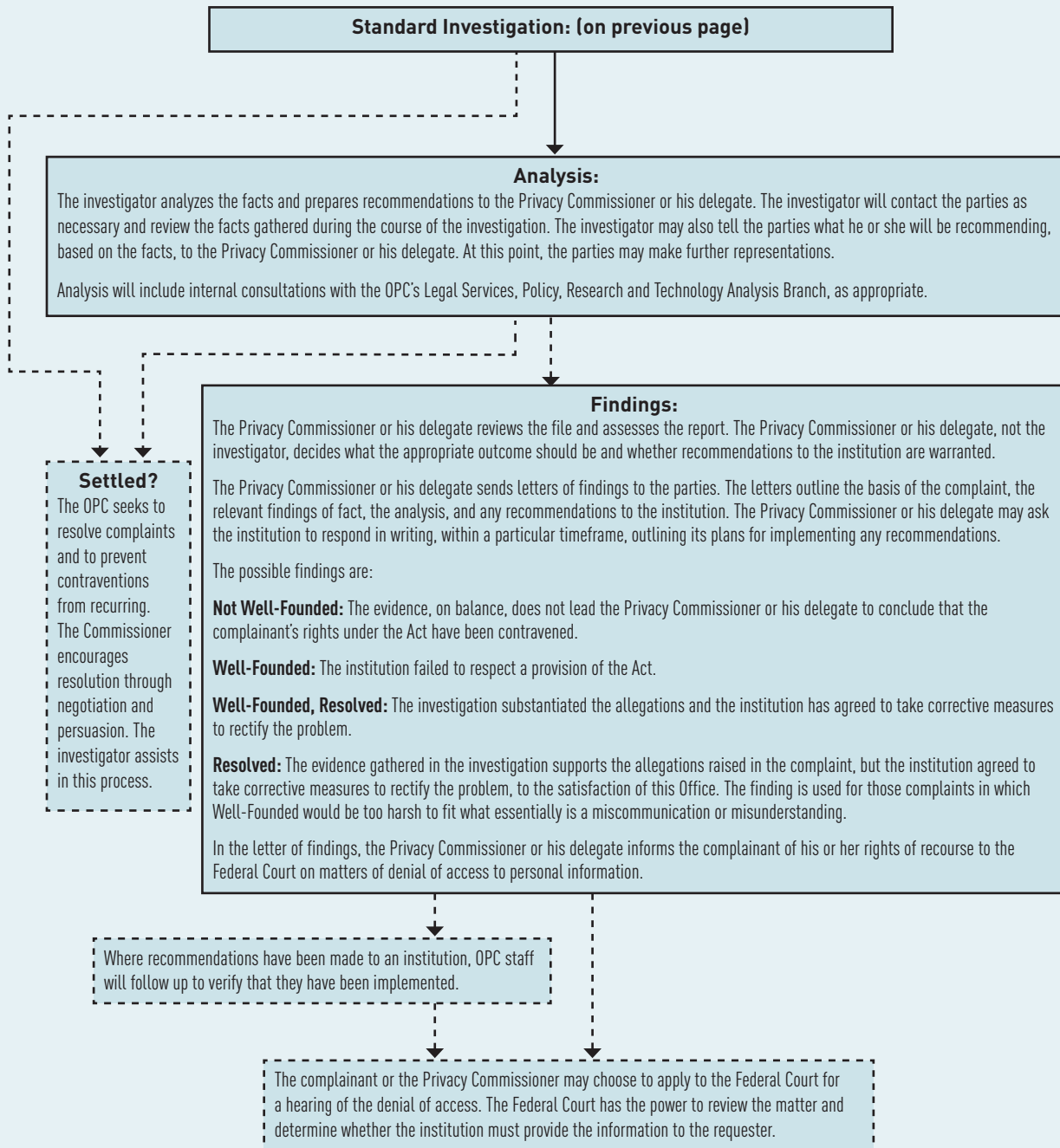




## PRIVACY ACT INVESTIGATION PROCESS



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



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

## Appendix 4–Report of the Privacy Commissioner, Ad Hoc, for 2016–17

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.

The Privacy Commissioner has 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 so that I can investigate complaints lodged against the OPC under the Act.

### *Outstanding complaints from previous years*

Our office had one outstanding complaint from the previous year. This complaint had been made by an individual who alleged that the OPC had not provided all records in its response. My investigation concluded that all records had indeed been provided.

### *New complaints this year*

Four complaints were received this year; all were investigated and disposed of by the end of the fiscal year.

The issue in two complaints arose from the loss of personal information in mail packages delivered to the OPC. In both complaints, the loss of the personal information had occurred in the mail room. The mail room was set up in a way that mail could find its way into bins slated for shredding. My investigation concluded that the fate of the lost two pieces of mail could not be determined with certainty, but that the most likely explanation was that they had been accidentally shredded. I was satisfied with the steps that the OPC had taken to improve its mail-handling processes in order to prevent this from happening in future. I therefore found these complaints were well-founded and resolved.

One complaint concerned to the application of section 22.1(1) of the Act, which exempts from production information obtained or created in the course of an investigation by the OPC. Once the investigation and all related proceedings are finally concluded, the exemption is partially lifted: it no longer applies to documents the OPC itself created during the investigation.

My investigation revealed that the disputed documents had been obtained during the course of the OPC's own investigations. I therefore found that the OPC properly applied the mandatory exemption in refusing to disclose the requested documents.

The fourth complaint was made by an individual who alleged that the OPC had improperly disclosed their personal information. Details of a personal meeting had inadvertently been made available within the OPC for a short period of time, allowing a small number of people to see the information. Although I concluded the complaint to be well-founded, I also concluded that disclosure was accidental.

In addition to these four complaints, this Office received correspondence from a number of individuals who were dissatisfied with how the OPC had investigated their complaints about other institutions or about delay in dealing with those complaints. This Office does not have jurisdiction to investigate concerns about how the OPC has investigated complaints that have been made to it as the oversight body under the Act. Nor can my Office investigate concerns about delay by the OPC in processing such complaints. My mandate is limited to receiving and investigating complaints that an access request for a record under the control of the OPC itself may have been improperly handled.

### Conclusion

The existence of an independent Commissioner, Ad Hoc helps to ensure the integrity of the OPC's handling of requests made to it as an institution, and therefore contributes to the proper functioning of the Act. My Office looks forward to continuing to play this part.

Respectfully submitted,

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

May 2017