

Annual Report to Parliament 2014


# PRIVACY PROTECTION

**A Global Affair**

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



Office of the  
Privacy Commissioner  
of Canada



Since the flow  
of information  
in the modern  
world knows  
no boundaries,  
neither can data  
protection efforts.

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

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

© Minister of Public Works and Government Services Canada 2015

Cat. No. IP51-1E-PDF  
1913-3367

This publication is also available on our website at [www.priv.gc.ca](http://www.priv.gc.ca)

Follow us on Twitter: @PrivacyPrivee

**Privacy Commissioner  
of Canada**

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

**Commissaire à la protection  
de la vie privée du Canada**

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



June 2015

The Honourable Leo Housakos, Senator  
Speaker of the Senate  
The Senate of Canada  
Ottawa, Ontario K1A 0A4

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Personal Information Protection and Electronic Documents Act* for the period from January 1 to December 31, 2014.

Sincerely,

*Original signed by*

Daniel Therrien  
Privacy Commissioner of Canada



**Privacy Commissioner  
of Canada**

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

**Commissaire à la protection  
de la vie privée du Canada**

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



June 2015

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

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Personal Information Protection and Electronic Documents Act* for the period from January 1 to December 31, 2014.

Sincerely,

*Original signed by*

Daniel Therrien  
Privacy Commissioner of Canada





# Table of Contents

Message from the Commissioner .....	1
Privacy by the Numbers in 2014 .....	8
The Year in Review .....	11
Feature: <i>Privacy Protection: A Global Affair</i> .....	29
Investigation statistics.....	39
Appendix 1 — Definitions of Complaint Types under PIPEDA .....	46
Appendix 2 — Definitions of Findings and Other Dispositions .....	48
Appendix 3 — Investigation Process .....	50

## About PIPEDA

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.

PIPEDA applies across Canada to organizations that collect, use, or disclose personal information in the course of commercial activities, unless provincial privacy legislation deemed substantially similar to PIPEDA applies. Quebec, Alberta and British Columbia each have substantially similar legislation covering the private sector. In addition, Ontario, New Brunswick and Newfoundland and Labrador have substantially similar legislation covering certain organizations in the health sector.

In all provinces, PIPEDA applies in respect of federally regulated activities in the private sector. PIPEDA also protects employee information, but only in the federally regulated private sector.





# Message from the Commissioner

**S**ince becoming Privacy Commissioner, I have been struck by the fact that so many of the privacy risks facing Canadians are global in nature.

In this digital era, our economy and our society are increasingly international, resulting in more and more of our personal information crossing borders. A single issue can affect large numbers of people in multiple countries – something we saw in our investigations work during 2014.

In one case, for example, we received over two dozen complaints from Canadians about a website based in Romania that republishes legal findings. The site had made readily accessible to anyone with an Internet connection numerous court and tribunal decisions containing highly sensitive personal information related to divorce, custody, bankruptcy, labour relations, immigration and other matters.

Meanwhile, another investigation examined a massive data breach at Adobe Inc. in which hackers gained access to the personal information of millions of customers around the world.

For data protection authorities such as the Office of the Privacy Commissioner of Canada, these types of issues underscore the importance of working to stay ahead of emerging trends and also to continue to find ways to collaborate more closely with provincial and international counterparts.

The importance of thinking and working globally cannot be understated, which is why global privacy protection issues take centre stage in this 2014 Annual Report to Parliament.

This report also highlights the dramatic jump we have seen in complaints to our Office – perhaps a sign of growing public concern about privacy issues – and it describes some of the major investigations concluded over the course of the year.

As well, the report speaks to how rapidly changing technologies such as those tied to Big Data and the Internet of Things are raising new privacy concerns. It also discusses transparency issues related to government requests for access to personal information held by private sector companies such as telecommunications providers.

## **COLLABORATION WITH INTERNATIONAL PARTNERS**

Every hour of every day, individuals the world over rely on common information and communication technologies, platforms and networks. The data involved in these online activities can travel throughout the world, including to third party companies that may not be subject to privacy protection regimes. Changes in one company's privacy practices or a data breach can affect millions of people worldwide.

Consequently, international cooperation has been an established priority for the OPC over the last several years. Our feature article (see page 29) focuses on the evolution of international collaboration and some of the concrete actions we took with global partners

in 2014. These included, for example, the Global Privacy Enforcement Network Privacy Sweep, through which 26 privacy enforcement agencies, coordinated by our Office, examined how hundreds of popular mobile applications communicate their privacy policies to users. Actions on concerns that followed resulted in improvements to the privacy practices of more than 100 applications.

In addition, Canadians are already reaping the benefits of cooperative agreements the Office has established with counterparts in countries such as Ireland and the United Kingdom, and the member economies of the Asia–Pacific Economic Cooperation forum. In 2014, we added Dubai and Romania to the list of countries with which we have such agreements, allowing us to conduct joint investigations and as a result increase our effectiveness in addressing consumer concerns within a global economy marked more and more by multinationals.

Among the most exciting developments of 2014 was the acceptance of the Global Cross Border Enforcement Cooperation Arrangement by 55 of the world's data protection authorities. This Arrangement is aimed at fostering more coordinated approaches to addressing cross-border privacy issues. It meets an urgent need for data protection authorities to share confidential information, thereby enabling greater collaboration and more joint investigations.

This is a very positive development. Once the Arrangement is fully operational, organizations will be able to conduct privacy investigations with international implications through a coordinated process, rather than duplicating one another's efforts in a series of investigations at the national level. Findings and outcomes of investigations could in many instances be issued faster – leading to clearer and stronger messages to organizations and the public.

Going forward, it is safe to say that whenever an incident arises that has an international impact, data protection authorities will be looking to determine which partners they can best work with, and how.

In short, this is the new normal.

This wider collaboration should make possible the enforcement of privacy rights on a broader scale than ever before. And this will provide greater recourse to individuals who may be concerned that they have no control over their personal information in a borderless, digital world.

## **PRIVACY'S RISING PROMINENCE**

In many ways, within Canada and around the world, privacy itself has never been in a brighter spotlight. Data breaches by major retailers attract widespread media attention. The growing interplay among law enforcement and national security organizations, and

commercial organizations holding consumer data has aroused public curiosity. And the increasing capacity to track and analyze consumer behaviour—both while on-line and on mobile devices—has led people to wonder exactly who is collecting their personal information, where it is going, how it is being used and how they can exert greater control over it.

This increased interest among consumers translated partly into a significant rise in enquiries and complaints to our Office under PIPEDA in 2014.

## **MEETING CONCERNS AND MANAGING GROWING DEMAND**

While complaints under PIPEDA jumped by 50 percent between 2013 and 2014<sup>1</sup>, I am pleased to note that the service we provide to complainants is becoming more efficient. Since 2012, the average time it takes to investigate new complaints has been reduced by 3.5 months.

This resulted from our Office adopting a calibrated approach to managing complaints and focusing our resources by choosing the appropriate tool to address specific privacy

<sup>1</sup> We accepted 402 PIPEDA complaints in 2014. When discounting the 170 complaints received about Bell's Relevant Advertising program in 2013 which were treated as one, new complaints increased 55 percent in 2014 compared to 2013.

issues. For example, we continue to seek opportunities to apply our successful early resolution approach to complaints, enabling us to address concerns without having to undertake a formal investigation. We have also been exercising our powers to decline to investigate a complaint or discontinue investigations<sup>2</sup> where appropriate in order to concentrate resources on matters of greatest privacy impact and concern.

## **KEEPING PACE WITH TECHNOLOGICAL DEVELOPMENTS**

Our growing level of activity—and our mission to protect and promote the privacy rights of individuals—compels us to identify and seek to stay ahead of emerging privacy issues. At the centre of many of these issues lies the unrelenting pace and ever-expanding breadth of technological development.

As network connectivity spreads from computers and mobile devices to everyday objects such as cars, appliances, clothing and accessories, the amount of personal information being collected and distributed is increasing dramatically. When harnessed

and analysed, the data these connected devices gather can reveal a great deal about our private lives, including our location, consumption and travel patterns, health status and even moods.

The age of the Internet of Things and wearable computing is only just beginning, but our Office is already working to ensure we can respond effectively to this emerging reality. This includes a research agenda to examine commercial data practices as they relate to these new technologies and other advances.

Simply put, we need to continually enhance our understanding of the privacy implications; determine how best to ensure and encourage greater respect for privacy by private sector organizations; and promote the competitive advantage that building citizen and consumer trust can offer. We look forward to sharing additional insights on this topic later in 2015.

## **TELECOMMUNICATIONS AND TRANSPARENCY**

While privacy is often synonymous with new and emerging trends, the issue of government access to private sector information, including telecommunications data, remains the subject of an important and ongoing debate. While understanding the need for adequate security and intelligence measures, our Office continues to encourage parties on both sides of such sharing of personal information to provide greater transparency for Canadians.

---

<sup>2</sup> Under section 12.2 (1) of PIPEDA, the Commissioner may discontinue the investigation of a complaint if the Commissioner is of the opinion that (a) there is insufficient evidence to pursue the investigation; (b) the complaint is trivial, frivolous or vexatious or is made in bad faith; (c) the organization has provided a fair and reasonable response to the complaint; (d) the matter is already the object of an ongoing investigation under this Part; (e) the matter has already been the subject of a report by the Commissioner.”

The Supreme Court of Canada's decision in *R. v. Spencer* was an important step forward in this discussion. In its unanimous decision, the Court held that there is a reasonable expectation of privacy in telecom subscriber information that can reveal Internet usage and that, absent exigent circumstances or a reasonable law, law enforcement officials need prior judicial authorization to obtain such data.

Left unanswered however, was the question of the circumstances in which organizations may voluntarily disclose other types of information in response to police and government requests. Consequently, in November 2014, I called on Parliament to provide guidance for organizations and Canadians to better understand when their personal information may be disclosed to public authorities without consent or judicial authorization.

In the wake of the Supreme Court's decision in *Spencer* and in light of Canadians' concerns regarding warrantless access requests, we welcome the publication of company transparency reports and applaud those who are changing their policies following the ruling. We are also working with service providers and encouraging them to be more transparent about how often and in what circumstances they respond to authorities' requests for personal information.

Transparency of this kind is central to privacy protection. It informs individuals about how their personal information will be used, supports their decision making and creates opportunities for companies to earn and maintain consumer trust.

### **SUPPORT FOR SOME PROPOSED CHANGES TO PIPEDA**

More than a decade ago, PIPEDA was enacted to build trust in the digital economy. Data breaches pose a threat to Canadians' confidence. Thus, we welcome the proposed amendment to PIPEDA in Bill S-4, the *Digital Privacy Act*, which seeks to implement mandatory breach notification. By obliging organizations to inform us of material breaches, we, in turn, will be able to work with companies—helping them to respond appropriately and to put practices in place to prevent future incidents. Mandatory notification will also provide a clearer picture of the frequency and type of data breaches experienced by organizations.

Mandatory notification would better inform Canadians of situations in which their personal information has been compromised. It would also enable Canada to keep pace with other jurisdictions where similar measures have been enacted or are being considered.

In addition, requiring organizations to keep and maintain a record of breaches, and provide us with such information upon request would be an important accountability mechanism. Our Office would be able to evaluate compliance with the notification provisions and assess how organizations are deciding whether to issue notifications.

We also look forward to the introduction of voluntary compliance agreements under PIPEDA. This is a tool our Office had requested as a means to help ensure that, after we close an investigation, the company honours its commitments to improve privacy practices.

While we have some concerns with some other provisions in this Bill (see page 27), voluntary compliance agreements and mandatory breach reporting are positive steps forward for privacy protection in Canada. In the interim, we have taken steps to expand our capacity for responding to breaches (see page 18).

## **THE WAY FORWARD**

Looking ahead, I see one of the main challenges of my mandate as ensuring that the Office continues to ensure it is keeping pace with the new realities of the privacy landscape.

Early in my mandate, I announced plans to engage with stakeholders across the country to help inform the selection of privacy priorities for the next five years. The aim was to establish priorities that will help focus our efforts and guide discretionary resource allocation decisions in order to increase our chances of making a real difference.

At the time of this report's writing, our Office had met with stakeholders from business, government, consumer advocacy groups, civil society and academia to hear their views on the strategic areas that pose the greatest threat to Canadians' privacy, and the areas in which the OPC could have the greatest positive impact. We had also conducted focus groups with members of the general public to gain a deeper understanding of their privacy concerns and priorities.

Having heard from numerous voices and taking stock of their views, we are in the process of finalizing the new privacy priorities, and look forward to sharing these with Parliament. As the prevalence and complexity of privacy issues continues to grow, we believe these priorities will help us hone our focus to make the best use of resources and further our ability to protect and promote Canadians' privacy rights.

## **A FINAL WORD**

Finally, I would be remiss if I did not mention the 2014 passing of two of my predecessors: Bruce Phillips and George Radwanski. They filled this role, one after the other, from 1991 to 2003.

As Commissioner, Mr. Phillips urged the federal government to adopt privacy legislation that would apply to the private sector. His efforts led to the adoption of PIPEDA.

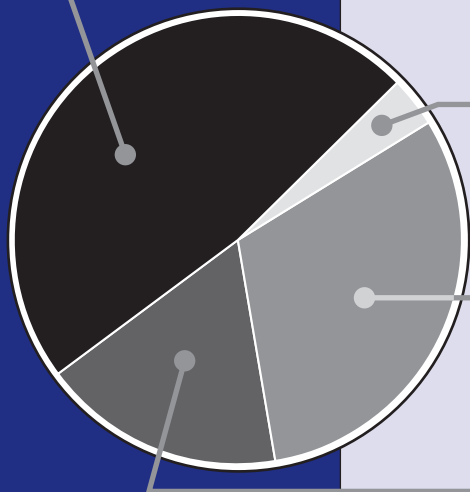
It was Mr. Radwanski who presided over PIPEDA's coming into force and whose early findings laid the groundwork for the application of the law.

As I look back on the past achievements of our Office and forward to new challenges, I can say with confidence that we are positioning ourselves to continue to effectively perform our role in an ever-changing world.

# Privacy by the Numbers 2014

Complaints accepted

402

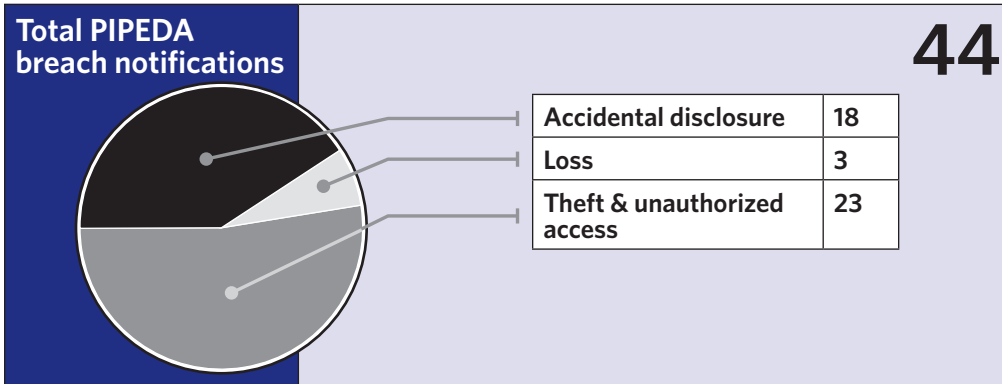
**Total PIPEDA  
complaints closed**
**375**


<b>Complaints closed by Early Resolution</b>	<b>180</b>
<b>Complaints discontinued under PIPEDA section 12.2<sup>3</sup></b>	<b>13</b>
<b>Complaints declined, withdrawn or outside OPC jurisdiction</b>	<b>117</b>
<b>Complaints closed with Report of Finding issued</b>	<b>65</b>
Complaints deemed not well-founded	25
Complaints deemed well-founded and resolved	24
Complaints deemed well-founded and conditionally resolved	7
Complaints deemed well-founded	2
Complaints settled	7

<sup>3</sup> Under section 12.2 (1) of PIPEDA, the Commissioner may discontinue the investigation of a complaint if the Commissioner is of the opinion that (a) there is insufficient evidence to pursue the investigation; (b) the complaint is trivial, frivolous or vexatious or is made in bad faith; (c) the organization has provided a fair and reasonable response to the complaint; (d) the matter is already the object of an ongoing investigation under this Part; (e) the matter has already been the subject of a report by the Commissioner.

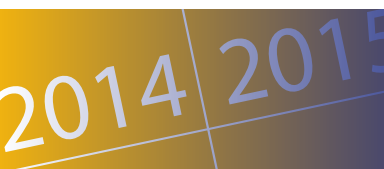


<b>Compliance through informal enforcement</b>	<b>56</b>
--	-----------



<b>PIPEDA information requests</b>	<b>3,651</b>
<b>Web visits</b>	<b>3,370,692</b>
<b>Visits to OPC blog</b>	<b>1,033,200</b>
<b>Visits to OPC YouTube channel</b>	<b>15,371</b>
<b>Tweets sent</b>	<b>437</b>
<b>Twitter followers as of Dec 31, 2014</b>	<b>8,868</b>
<b>External guidance issued (private sector)</b>	<b>7</b>
<b>Signed contributions agreements</b>	<b>14</b>
<b>Bills and legislation reviewed for privacy implication (private sector)</b>	<b>4</b>
<b>Parliamentary committee appearances (PIPEDA issues)</b>	<b>6</b>
<b>Formal briefs submitted (PIPEDA issues)</b>	<b>3</b>
<b>Interactions with parliamentarians (private sector)</b>	<b>14</b>





# The Year in Review

**O**ur various activities in 2014—investigations, stakeholder outreach, gearing up for new responsibilities to enforce Canada’s anti-spam legislation, and providing advice and information to Parliament—reflect the range of tools our Office has at its disposal to protect privacy and promote best practices among organizations subject to PIPEDA.

## INVESTIGATIONS

Canadians are increasingly concerned with how private sector organizations are handling their personal information and they are turning to us for assistance. Our intake team experienced another record year in 2014, with a total of 1,238 written submissions about privacy matters.

We also accepted 402 PIPEDA complaints, considerably more than the approximately 250 new files we would take on in an average year. Compared with 2013—and discounting the 170 complaints received about Bell’s Relevant Advertising Program that year, which were handled by one, all-

encompassing, Commissioner-initiated investigation—new complaints still increased by more than 50 percent.

During 2014, we noticed a trend toward multiple complaints about one issue. For example, we received:

- 27 complaints against the website Globe 24h.com and how it collects and publishes the personal information of Canadians (see page 32);
- 34 complaints against telecommunications companies

stemming from an academic project examining the industry’s data retention and disclosure policies; and

- 56 complaints from members of one union about a new authentication process being implemented by an airline. (In this case, we declined to investigate, since a grievance/arbitration process was already underway which would effectively deal with the matter.)

Given increased media and public interest in privacy matters, we anticipate this trend to continue. Still, as demands increase, we are pleased to report that our treatment times for handling complaints actually continue to decrease. Our average treatment time in 2014 for new complaints was 4.8 months, down from 5.3 months in 2013 and 8.3 months in 2012.

We attribute this growing efficiency to our calibrated approach to managing complaints and focusing our limited resources on addressing issues of greatest privacy concern to Canadians. This includes a special focus on early resolution, alternative case resolutions and seeking efficiencies at every stage of our investigative process by using the appropriate tool for each specific privacy matter.

The following sets out a number of investigations of note, along with successes we have had in employing the various tools in our compliance toolbox.

### ***An accountability gap at Microsoft***

A man complained to our Office when he was unable, even with significant effort, to get Microsoft to delete his email address from his customer account.

Our investigation revealed that the company’s inability to respond to a customer’s privacy request was due primarily to a technical design issue, but was compounded by important gaps in privacy accountability.

A previously undetected technical design issue meant that Microsoft could not delete the complainant’s email address. As a result, Microsoft had continued to use that email address without the complainant’s consent.

More troubling however, was that none of the dozen or so customer service representatives the complainant spoke with about getting his email address deleted—not even those specifically designated to address privacy-related matters—recognized that the complainant’s concern was privacy-related.

Although it became clear to us during the investigation that Microsoft had devoted significant resources and thought to its privacy management program, weaknesses in the area of customer support for privacy were evident. For example, customer service representatives had not been sufficiently trained to recognize privacy issues and refer them to the dedicated Privacy Response Center—nor had the

dedicated privacy agents received formal privacy training over and above that received by other customer service representatives.

Further, Privacy Response Center staff did not generally escalate unresolved privacy issues to Microsoft's Privacy Office, which, in turn, did not monitor Privacy Response Center operations. As such, there was an operational disconnect and a resulting gap in accountability between the Privacy Office and the Privacy Response Center's handling of customers' privacy concerns.

Microsoft resolved both the complainant's original concern as well as the accountability problems we identified. The company fixed the underlying system design issue, such that email addresses can now be deleted from account files. Among other measures, it also developed specialized privacy training for customer service representatives and augmented Privacy Office engagement in the resolution of privacy issues raised through the various customer support channels.

### ***An unsatisfactory response from Sobeys***

A woman alleged that she slipped on a puddle of water inside the supermarket in September 2011, fell and suffered an injury, after which she filed a report of the incident on a form provided by the supermarket.

In late November 2011, she sent a letter to the supermarket's head office, describing some

concerns about the incident and requesting a copy of the incident report as she had not been given a copy at the time she completed the report.

While the complainant and company eventually reached a settlement agreement over the original incident, she continued emailing the company requesting access to her personal information.

The supermarket replied in late August 2013, advising the complainant that her most recent request had been forwarded to "the appropriate individuals." These individuals were not identified and the complainant received no further contact from the supermarket, nor did she receive access to her personal information.

During our investigation, we contacted Sobeys on several occasions. However, much to our disappointment, Sobeys neither responded, nor provided representations, nor participated in the investigative process. We concluded that Sobeys had contravened PIPEDA by failing to provide the woman with access to her requested personal information.

Subsequent to our investigation, we brought an application to the Federal Court for a hearing on the matter. Eventually, Sobeys provided the information the woman sought, to our satisfaction, and thus the matter was resolved. The court proceeding was discontinued on January 8, 2015.

### *Protecting children’s privacy*

A company providing services aimed at children and youth has a special responsibility to ensure that they and their parents can easily learn about the services offered; understand what personal information is being collected; how such data will be used; and with whom it will be shared. Our Office initiated an investigation into the privacy practices of the popular Canadian children’s website [www.webkinz.com](http://www.webkinz.com) to examine some of these important issues.

Our investigation found that, although the website owner, Ganz, had given considerable thought to protecting the privacy of its young users (aged six to 13)—who register with the site to create and care for virtual pets—there was still room for improvement.

For example, the company did not use age-appropriate language and methods to clearly tell children that they needed to involve their parents when registering on the site.

Ganz also inadvertently collected full names of children when they created user names. We were concerned that this, combined with the collection of parents’ email addresses and other information, could lead to users being identified.

Testing on the site showed that—unbeknownst to Ganz—some advertisers appeared to be tracking user activity and therefore, could have

### Youth privacy resources

PIPEDA does not single out children or youth, but the requirement that organizations must obtain meaningful consent nonetheless calls for special consideration when young people are involved. Indeed, our Office has consistently viewed the personal information of children and youth as being of particular sensitivity. Organizations that collect, use or disclose such data need to bear this in mind and consider whether it requires any personal information at all to provide appropriate online services.

To promote the lessons learned from the Ganz investigation and two earlier files, we released a list of [key privacy tips](#) for companies providing services aimed at children and youth.

This builds on our wide variety of privacy resources developed for parents, teachers, businesses, and children and youth themselves.

been profiling children based on their surfing habits.

Ganz cooperated fully with the investigation and agreed to implement a number of measures to address our 11 recommendations within

### Link

#### Key privacy tips for services aimed at children

[https://www.priv.gc.ca/resource/fs-fi/02\\_05\\_d\\_62\\_tips\\_e.asp](https://www.priv.gc.ca/resource/fs-fi/02_05_d_62_tips_e.asp)

nine months. As a result, our Office found the matters arising from the investigation to be well-founded and conditionally resolved. Overall, our findings resulted in lessons learned for Ganz and any company that operates websites aimed at children, including:

- do not collect children’s personal information unless you absolutely need it;
- make sure that younger users are able to understand the privacy information they are being provided—or understand the need to involve an adult in making decisions; and
- make clear *who* needs to agree to terms and conditions. Children should not be expected to “agree” to legalistic language.

***Bell’s advertising program raises significant privacy concerns***

In October 2013, our Office received an unprecedented number of complaints following the introduction of Bell’s “Relevant Advertising Program.” This program involved tracking of customers’ Internet browsing, app usage, telephone calling and television viewing activity. Then, upon combining it with account demographic data collected from customer accounts, the program created detailed profiles to help third-party advertisers deliver targeted ads to Bell subscribers, for a fee.

We launched one all-encompassing, Commissioner-initiated investigation to address the full breadth of privacy issues raised in the 170 complaints received about the program.

In the investigation, we accepted that the program’s use of customers’ information was for an “appropriate purpose” under PIPEDA. However, after considering the sensitivity of the information used and customers’ reasonable expectations regarding the use of their information, we found that Bell was not obtaining adequate consent for the program. Bell put the onus on customers unwilling to participate in the program to take steps to opt out, while we concluded that customers should instead be asked to opt in.

Bell, as a provider of telephone, wireless, Internet and television services, can track every website its customers visit, every app they use, every TV show they watch and every call they make. In our view, much of this information is sensitive in its own right and we found that profile information is likely to be considered more sensitive when combined to create a rich, multi-dimensional portrait of individual subscribers. Furthermore, Bell’s program introduced a new use of customers’ personal information. Initially, customers provided personal information to Bell so it could deliver them paid telecommunications and broadcasting distribution services. This

program however involved using customers' personal information for the secondary purpose of enabling behaviourally targeted advertising by third parties. We were of the view that Bell customers would reasonably expect the company to obtain their express, opt-in consent for such a practice.

In 2011, our Office released [guidelines on online behavioural advertising](#). These indicate that opt-out consent may be appropriate in certain circumstances. In our investigation of Bell, however, we made clear that our guidelines do not render opt-out consent as the default. In determining the appropriate form of consent, organizations should be careful to consider all of the circumstances surrounding their behaviourally targeted advertising programs, including those contextual factors we considered in this investigation. As featured in our 2013 annual report, our [Guidelines for Online Consent](#), developed in concert with our Alberta and British Columbia provincial counterparts, outline some of the key considerations organizations need to consider when obtaining meaningful consent online.

In addition, our investigation found that Bell was failing to fully respect the choice of customers who took steps to opt out. That is, Bell continued building profiles of such customers—in case they may decide to one day opt back in. In response to our recommendation, Bell agreed, upon receiving an opt-out request, to immediately cease tracking the customer and delete the individual's profile information. The company also agreed with certain other recommendations, including to:

- include language in its contract with advertisers prohibiting them from linking profile information obtained from Bell to an identifiable individual (i.e., via their own cookies, device fingerprinting, account information, or other tracking methods);
- not use credit score information in its customer profiles, which our Office found inappropriate;
- use only partial rather than full customer postal codes in profiles, which could lead to the targeting of a much smaller group than intended; and
- remove The Source, a retail electronics store owned by the company, from the list of Bell affiliates with which Bell could share information.

## Links

### Guidelines on Online Behavioural Advertising

[https://www.priv.gc.ca/information/guide/2011/gl\\_ba\\_1112\\_e.asp](https://www.priv.gc.ca/information/guide/2011/gl_ba_1112_e.asp)

### Guidelines for Online Consent

[https://www.priv.gc.ca/information/guide/2014/gl\\_oc\\_201405\\_e.asp](https://www.priv.gc.ca/information/guide/2014/gl_oc_201405_e.asp)



Following our investigation's conclusion, Bell advised us that it had decided to withdraw its program and to delete all existing customer profiles related to the initiative. It has since advised that it plans to launch a similar program in the future using opt-in consent.

While our investigation is now considered resolved, our Office will be following further developments in this matter with active interest.

## **INTAKE AND EARLY RESOLUTION**

Our intake unit plays an important role in determining how we can best handle the hundreds of complaints we receive each year. A first step is to review a complaint to see whether further information is necessary in order to determine whether to accept it. Often, an intake officer will encourage individuals to discuss the issue with the chief privacy officer at the organization who may be in a position to resolve the matter immediately.

In 2014, we closed 180 complaints through early resolution, a 35 percent increase from 2013. We are maintaining our focus on this valuable approach and whenever appropriate, seek to engage both parties in a constructive dialogue with a view to resolving issues efficiently, effectively and satisfactorily without the need for a time- and resource-intensive formal investigation.

We are pleased to report that private sector organizations are very often eager to resolve the privacy concerns of their customers as expeditiously as possible. Complainants are similarly happy to have their matters resolved quickly.

### *Examples of early resolution*

In 2014, for example, we worked with a store to come up with an alternative approach to collecting information about customers' renting equipment that did not involve scanning drivers' licences. The store implemented the new policy and retrained its staff at all its locations.

In another instance, we were able, without launching a formal investigation, to ensure that a car dealership finally deleted a complainant's personal information—his social insurance number and a copy of his driver's licence, in particular—after having ignored a number of requests from him to do so.

## DATA BREACHES

In 2014, companies voluntarily reported 44 data breaches to us compared with 60 in 2013. (As breach reporting under PIPEDA is voluntary, we are not able to tell if this signifies a change in the number of actual breaches or less diligent reporting among organizations). Given the prevalence of breaches and the serious harm that can result to individuals whose information is compromised, we assigned a dedicated officer to work with organizations that suffer a breach. The officer ensures the organization properly investigated the incident, notified affected individuals as appropriate and implemented measures to prevent a reoccurrence. We also regularly work in concert with our provincial and international counterparts on breach matters, recognizing these often have wide, cross-border impact.

More than one third (16) of the breaches reported to our Office in 2014 originated from organizations in the financial sector, followed by the Internet sector (seven) and the insurance sector (six). Together, these three sectors accounted for nearly two-thirds of all breaches reported.

The majority of these incidents were the result of either theft or unauthorized access to personal information by unidentified third parties or by employees or former employees. The second most common cause was the

### **Credit card issuer takes immediate action in response to data breach**

**A credit card issuer reported to us that a printing error had caused the names and credit limits of some account holders to be erroneously included in correspondence destined for others. Overall, the incident affected 14,000 people.**

**In the course of our discussion with the company, we learned that it had investigated the cause of the breach, immediately notified all the individuals affected by the incident, deactivated their credit cards, and implemented additional printing verification controls to prevent future recurrence.**

**Rather than judging organizations solely on the basis of isolated breaches, our Office strives to emphasize the importance of identifying and mitigating risks to avoid such incidents in the first place, while being prepared to respond diligently to minimize potential harm when a breach does occur.**

accidental disclosure of personal information, resulting from either human error or a technological failing.

***Insufficient safeguards and unnecessary storage leaves sensitive data vulnerable***

In October 2013, Peoples Trust, a federally regulated financial institution headquartered in Vancouver, notified us of a data breach. Sensitive personal information—including names, dates of birth, social insurance numbers, and mothers’ maiden names—of some 12,000 customers was compromised after being provided by customers in online applications for deposit or secured credit card products. Following several complaints, we launched a Commissioner-initiated investigation that sought to assess the organization’s information security safeguards and retention practices.

Our investigation observed that the company did not implement sufficiently strong safeguards in developing its online application web portal in order to protect the sensitive personal information being collected from customers. As well, when the breach occurred, the company lacked a comprehensive information security policy.

There was also a lack of ongoing monitoring and maintenance to identify and address evolving digital vulnerabilities and threats. As a result, unbeknownst to the organization, a copy of the customer information—a duplicate of data held in the company’s internal database—was being stored unnecessarily, unencrypted, and in perpetuity, on a web server that had not been updated to address

a well-known vulnerability. Had this unnecessary duplicate not been on the web server in the first place, it would not have been compromised during the breach.

We also noted that during our investigation, Peoples Trust was very cooperative with our Office and demonstrated a timely and comprehensive breach response. For example, it immediately hired a consultant to identify the breach’s cause and “plug the leak.” It also implemented new measures to help affected individuals and reduce the risk of a future breach.

These included:

- providing clear and comprehensive notifications and offering credit alerts to those affected by the breach;
- ending the unnecessary retention of customers’ personal information on the web server;
- enhancing technological safeguards to protect information collected online; and
- developing procedures and associated internal communications to support privacy protection practices, such as requiring greater diligence in selecting and hiring third parties for developing information management systems.

As a result, we concluded that the matter was well-founded and resolved.

## STAKEHOLDER OUTREACH

Our Office’s mandate includes public education and therefore reaching out to stakeholders— businesses and consumers—to inform them about PIPEDA and its requirements is an important part of our activities. Outreach efforts can address emerging privacy issues, particularly as we learn about industry practices, trends and challenges, and consumers’ key concerns. Through our efforts, we build relationships with organizations subject to the law to facilitate complaint resolution. Outreach and education provide a cost-effective means of increasing compliance with PIPEDA.

In 2014, we undertook numerous outreach activities under PIPEDA, including:

- a series of stakeholder information sessions across Canada in conjunction with Industry Canada and the Canadian Radio-television and Telecommunications Commission prior to the coming into force of Canada’s anti-spam legislation (CASL);
- a presentation to the Investment Industry Regulatory Organization of Canada Ontario District Council, examining privacy considerations for investment dealers that collect personal information to comply with requirements to obtain data about risk tolerance, assets, liabilities and household sources of income to

better assess the suitability of proposed transactions for clients;

- speaking at events focused on information security such as: RSi2014 *Rendez-vous de la sécurité de l’information*, where we addressed the challenges posed by the Internet of Things (for more on this subject, read on to page 22); and Hackfest, where we focused on privacy breaches and metadata;
- participation at key conferences and trade shows for industries in which the use of personal information is growing, such as: DX3, an annual conference for digital marketing, digital advertising and digital retail professionals; Restaurants Canada Show, to reach food service and hospitality industry professionals; and Fitness Business Canada, an annual conference of gym and fitness industry professionals; and
- discussions in multiple forums regarding both the prevention of data breaches and our breach investigation process.

### Link

#### Ten Tips for Reducing the Likelihood of a Privacy Breach

[https://www.priv.gc.ca/resource/fs-fi/02\\_05\\_d\\_60\\_tips\\_e.asp](https://www.priv.gc.ca/resource/fs-fi/02_05_d_60_tips_e.asp)

**In June, we released useful and practical information guiding organizations on steps they can take to help prevent breaches.**

**[Ten Tips for Reducing the Likelihood of a Privacy Breach](https://www.priv.gc.ca/resource/fs-fi/02_05_d_60_tips_e.asp)**

## ANTI-SPAM LEGISLATION COMES INTO FORCE

Key provisions of Canada's anti-spam legislation (CASL) came into force on July 1, 2014, including amendments to PIPEDA. Our specific mandate under the new law focuses on two areas:

- the harvesting of electronic addresses, in which bulk lists of email addresses are compiled through mechanisms that include the use of computer programs to automatically mine the Internet for addresses; and
- the collection of personal information through illicit access to other people's computer systems, primarily through means such as spyware.

To prepare for our role in the joint enforcement of the new legislation, we entered into a cooperation, coordination and information-sharing agreement with our partners, the Canadian Radio-television and Telecommunications Commission (CRTC) and the Competition Bureau.

Other activities in the first half of the year included:

- enhancing our investigative processes, tools and case management system to better accommodate more intelligence-

### Anti-spam resources

We updated our website in 2014 to explain our responsibilities under CASL to industry stakeholders and the general public. In early 2015, we continued to add further, helpful resources at [www.priv.gc.ca/casl](http://www.priv.gc.ca/casl).

driven—rather than traditional complaint-driven—investigations;

- strengthening the analytical capabilities and security of our technology laboratory; and
- training investigators and front-line intake and Information Centre staff.

As one of the CASL enforcement partners, we have access both to submissions made by the general public through Industry Canada's [www.fightspam.gc.ca](http://www.fightspam.gc.ca) website and to third-party data sources reporting directly to the CRTC's Spam Reporting Centre (SRC). Working with our designated SRC analyst (an OPC-funded position), we spent the second half of 2014 familiarizing ourselves with the functions of the reporting centre and analyzing its database to identify possible address-harvesting and spyware cases for investigation. By year-end, we had launched our first investigation and were evaluating other potential cases.

## POLICY AND RESEARCH

Our policy and research function supports our efforts to promote and protect privacy rights under PIPEDA. It plays a key role in developing the Office’s positions on emerging privacy issues and offers guidance to organizations. Meanwhile, our Contributions Program also supports the advancement of privacy knowledge and expertise. Together, these efforts help to ensure our effectiveness in helping organizations better protect Canadians’ personal information as new challenges continue to emerge.

### *Retention and disposal of personal information*

In today’s information age, a great many organizations collect personal information—in physical or electronic forms—as a matter of routine. Information is gathered from citizens, employees, clients and prospective clients. As more and more organizations climb onto the “Big Data” bandwagon, the push to amass enormous volumes of personal information for yet undetermined purposes has never been greater. This ever-growing capacity and desire to collect, analyse and indefinitely retain massive amounts of personal information also increases the risks and consequences of a potential data breach. Data breaches are not the only worry—the longer information is kept, the greater the risk that it may be used in ways individuals may not have expected when they consented to provide their information.

Once collected, organizations need to make informed choices about how long to keep personal information, and when and how to dispose of it.

In June, we published [guidelines](#) to help organizations adopt smart retention and disposal policies and practices related to their handling of personal information.

These guidelines cover general collection, retention and disposal protocols, as well as practical information on choosing disposal methods and developing policies and procedures that set out clear retention and disposal schedules.

### *The Internet of Things*

OPC research conducted in 2014 will help individuals understand how their privacy may be affected by the online networking of a multitude of uniquely identified, everyday objects—the so-called Internet of Things.

These papers will build on some of the privacy issues we discussed in the OPC’s [Wearable Computing research paper](#) released in 2014.

An introductory paper will provide an overview of the privacy issues involved, setting the context for companion reports on tracking purchasing decisions in the retail context and the advent of smart homes and devices. The reports will be finalised and released later in 2015.

## Links

### Retention and disposal guidelines

[https://www.priv.gc.ca/information/pub/gd\\_rd\\_201406\\_e.asp](https://www.priv.gc.ca/information/pub/gd_rd_201406_e.asp)

### Wearable computing research paper

[https://www.priv.gc.ca/information/research-recherche/2014/wc\\_201401\\_e.asp](https://www.priv.gc.ca/information/research-recherche/2014/wc_201401_e.asp)

## Big Data and the Internet of Things

Two notable facets of the ongoing explosion of data generation, collection and use are “Big Data” and the Internet of Things. Both have significant implications for privacy protection—in Canada and around the world.

As the New Scientist has reported, “thanks to cheaper storage, faster processing and better algorithms,” individuals’ actions can be turned into data. In turn, organizations such as retailers can analyze and mine this data to learn as much as possible about past consumer behaviour in order to hone marketing strategies and develop new products and services.

Ever-increasing computing capacity has also led to analysis about future behaviour. “Predictive analytics” can yield benefits for commercial organizations. It may contribute to product innovation, more effective marketing and better-targeted research. It could equally result in discriminatory and invasive practices.

Big Data will only get bigger with the emergence of the Internet of Things. This evolution is already emerging. In 2008, the number of objects connected to the Internet was already greater than the number of people on the planet. A December 2013 Gartner study estimated that 26 billion devices (not counting desktop computers, laptops, tablets and smart phones) will be connected to the Internet by 2020.

Information collected by sensors within objects that are connected to each other can yield a tremendous amount of data that can be combined, analyzed and acted upon, all potentially without adequate accountability, transparency, security or meaningful consent. Combining the information collected can lead to detailed profiles about individuals, triggering privacy concerns.

### *Genetic testing*

Currently, there are no laws in Canada that specifically address the use of genetic test results by insurance companies. This has raised fears that potential genetic discrimination might act as a deterrent to undergoing genetic testing, even when it is clinically advisable.

In light of these concerns, we have been examining the privacy implications arising from the collection and use of genetic information. Based on this work, we released a **statement** in July 2014 on the use of genetic test results by life and health insurance companies.

We called on the industry to refrain from asking for existing test results to assess insurance risk until insurers can clearly show that these tests are necessary and effective in assessing risk.

Finally, in October, the Commissioner and two OPC officials **appeared** before the Senate Standing Committee on Human Rights to comment on Bill S-201. The Bill sought to prohibit organizations from requiring an individual to undergo genetic testing or disclose existing test results as a condition of receiving goods or services.

### **Links**

#### **Statement on the use of genetic test results**

[https://www.priv.gc.ca/media/nr-c/2014/s-d\\_140710\\_e.asp](https://www.priv.gc.ca/media/nr-c/2014/s-d_140710_e.asp)

#### **Appearance on Bill S-201**

[https://www.priv.gc.ca/parl/2014/parl\\_20141002\\_e.asp](https://www.priv.gc.ca/parl/2014/parl_20141002_e.asp)

### **Commissioner's remarks to the Senate Standing Committee on Human Rights, October 2, 2014**

**"Bill S-201 recognizes the overriding societal benefits of protecting applicants' right to privacy and of providing all persons with insurance coverage regardless of their genetic heritage. We are also encouraged by the Government's commitment in the Speech from the Throne to prevent employers and insurance companies from discriminating against Canadians on the basis of genetic test results.**

**"I welcome the public debate that this Bill engenders, but if legislation is not forthcoming, my Office would urge the insurance industry, patient advocacy groups, the federal and provincial governments and other interested parties to work together to come up with a non-legislative, binding solution, such as exists in the United Kingdom for example, to ensure that genetic information is adequately protected and used only as appropriate and necessary."**



## *Data brokers*

Data brokers have been defined as companies that collect personal information about consumers from a variety of public and non-public sources and resell the information to other companies.<sup>4</sup>

Our [research paper](#), released in September 2014, aimed to provide individuals and businesses with an overview of the privacy compliance requirements for data brokers based on the Canadian and American privacy environments.

It is important to note that the data broker industry in Canada operates under a comprehensive privacy and regulatory compliance framework that is distinct from that in place in the United States.

In an interconnected, international digital economy, data cross borders easily and organizations are accessing personal information in new and innovative ways. Whether data brokers based in other jurisdictions know of PIPEDA and comply with its requirements when doing business in Canada is not always assured.

As data brokers become informed of these requirements, they will gain a better understanding of their obligations, helping to inform their practices to support consumer control, trust and transparency. Consumers, in turn, provided with knowledge about data brokers and their practices will be better able to exercise consent and control choices related to their personal information.

## [Link](#)

### [Research Paper](#)

[https://www.priv.gc.ca/information/research-recherche/2014/db\\_201409\\_e.asp](https://www.priv.gc.ca/information/research-recherche/2014/db_201409_e.asp)

---

<sup>4</sup> The Federal Trade Commission, “FTC to Study Data Broker Industry’s Collection and Use of Consumer Data.” News release, December 18, 2012.

### Evaluating the OPC's Contributions Program

Launched in 2004, the OPC's Contributions Program funds independent privacy research and related knowledge translation initiatives. In fiscal year 2014-2015, the Program provided over \$470,000 in funding for nine new, independent research and knowledge translation projects. The projects will generate and share new knowledge about privacy risks and protections that can be applied by government institutions, organizations and individual Canadians. Some examples of last year's projects include:

- a study of smart vehicle technology;
- a documentary about privacy and genealogy;
- an analysis of the privacy policies of online payday lenders;
- a study of mental health information privacy; and
- an app to educate kids about online privacy.

The Program also awarded funding for the organization and hosting of the third *Pathways to Privacy Research Symposium*, a series originally introduced by the OPC in 2012 to increase awareness of the outcomes of privacy research and knowledge translation projects in Canada. The theme for the third Symposium, which was held in February 2015, was "A Return to First Principles for Privacy at the Cutting-Edge." It explored the values that underlie privacy protection and examined how these values are furthered, and/or threatened, by technological and scientific developments.

As with all contributions programs administered by federal institutions, an independent evaluation of its performance and ongoing relevance is required every five years. The latest evaluation was conducted in 2014, following which the Program was renewed for another five years.

## PARLIAMENTARY ACTIVITIES

In June 2014, our Office provided a submission to the Senate Standing Committee on Transport and Communications followed by an appearance before the committee, on the various proposed amendments to PIPEDA stemming from Bill S-4, the *Digital Privacy Act*.

In our submission and appearance, we welcomed the proposals to introduce mandatory breach notification, enhance consent requirements and voluntary compliance agreement provisions—measures that will make it easier for us to ensure that companies meet the commitments they make at the conclusion of investigations. In general, we also supported other proposed amendments that address problems or gaps that have become apparent during the years that PIPEDA has been in force.

However, we also expressed reservations about two of the proposed additions—7(3)(d.1) and (d.2)—that would allow an organization, in certain circumstances, to disclose personal information to another organization without consent. We suggested that these two new paragraphs could lead to excessive disclosures that would be invisible both to the individuals concerned and to our Office.

We also recommended that organizations be required “to publicly report on the number of disclosures they make to law enforcement under paragraph 7(3)(c.1), without knowledge

### Other parliamentary activity of note

- [Appearance](#) before the Standing Senate Committee on Transport and Communications regarding the practice of collecting and analyzing data from Bell customers for commercial purposes including targeted advertising (April 29, 2014)
- [Appearance](#) before the Standing Senate Committee on National Finance on Bill C-31, Economic Action Plan 2014 Act No. 1 (May 13, 2014; [submission](#))
- [Appearance](#) before the House of Commons Standing Committee on Justice and Human Rights (JUST) on Bill C-13, An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act (June 10, 2014; [submission](#))
- [Appearance](#) before the Senate Standing Committee on Human Rights on Bill S-201, An Act to Prohibit and Prevent Genetic Discrimination, The Genetic Non-Discrimination Act (October 2, 2014)

or consent, and without judicial warrant, in order to shed light on the frequency and use of this extraordinary exception.”

The full [submission](#) can be found on our web site.

### Links

**Bell appearance**  
[https://www.priv.gc.ca/parl/2014/parl\\_20140429\\_cb\\_e.asp](https://www.priv.gc.ca/parl/2014/parl_20140429_cb_e.asp)

**Bill C-31 appearance**  
[https://www.priv.gc.ca/parl/2014/parl\\_20140513\\_cb\\_e.asp](https://www.priv.gc.ca/parl/2014/parl_20140513_cb_e.asp)

**Bill C-31 submission**  
[https://www.priv.gc.ca/parl/2014/parl\\_sub\\_140512\\_sen\\_e.asp](https://www.priv.gc.ca/parl/2014/parl_sub_140512_sen_e.asp)

**Bill C-13 appearance**  
[https://www.priv.gc.ca/parl/2014/parl\\_20140610\\_e.asp](https://www.priv.gc.ca/parl/2014/parl_20140610_e.asp)

**Bill C-13 submission**  
[https://www.priv.gc.ca/parl/2014/parl\\_sub\\_140609\\_e.asp](https://www.priv.gc.ca/parl/2014/parl_sub_140609_e.asp)

**Bill S-201 appearance**  
[https://www.priv.gc.ca/parl/2014/parl\\_20141002\\_e.asp](https://www.priv.gc.ca/parl/2014/parl_20141002_e.asp)

**Bill S-4 submission**  
[https://www.priv.gc.ca/parl/2014/parl\\_sub\\_140604\\_sen\\_e.asp](https://www.priv.gc.ca/parl/2014/parl_sub_140604_sen_e.asp)





## *Feature*

# Privacy protection: A global affair

**W**hile privacy was in the spotlight in 2014—perhaps like never before—it was also a landmark year for international collaboration among privacy enforcement authorities.

It was a year in which relationships and networks carefully cultivated over more than a decade matured into privacy protection action on many global fronts.

More than ever, as Canadians enjoy the unparalleled benefits of the digital age and its increasingly borderless economy, our Office is enhancing our work with international counterparts to minimise the attendant privacy risks.

After years of gradually growing our international networks, relationships and activities, 2014 was a year where

international enforcement action picked up unprecedented steam, establishing itself as the new norm.

Canadians are concerned that there will be weaker privacy protections and less access to recourse to remedy problems when their personal information leaves Canada.

In the face of such concerns, continually increasing international collaboration is essential to build and maintain confidence in today's global, digital economy.

The year included:

- a new, global-scale arrangement which will enable even further collaboration among privacy enforcement agencies world-wide;
- coordinating a global sweep raising awareness about mobile app privacy practices which led to initiatives supporting transparency about privacy practices for app users;
- undertaking an investigation on behalf of Canadians whose personal information tied to court proceedings had been made searchable and fully accessible by a Romanian-based website;
- a tri-country response to a global-scale data breach that affected millions of people; and
- joint efforts that resulted in operators deciding to take down an Eastern Europe-based website that displayed images taken from unsecured webcams including those from Canadian bedrooms.

## INCREASING ENGAGEMENT AND COMING TOGETHER

The foundations supporting these actions in the past year were set in the 10 years that came before. In 2004, we increased our international engagement significantly. That year, we attended our first meeting of the Berlin Group

## Links

### Asia Pacific Privacy Authorities

<http://www.appaforum.org/about/>

### Association francophone des autorités de protection des données personnelles

<http://www.afadp.org/>

### Commission for the Control of INTERPOL's Files

<http://www.interpol.int/About-INTERPOL/Structure-and-governance/CCF/Commission-for-the-Control-of-INTERPOL%27s-Files>

### The International Working Group on Data Protection in Telecommunications (Berlin Group)

<http://www.berlin-group.org/>

## Other international initiatives of note

- **Asia Pacific Privacy Authorities:** This group meets twice a year to exchange ideas and best practices about privacy regulation, new technologies and ways to raise awareness of privacy issues.
- **Association francophone des autorités de protection des données personnelles:** We were instrumental in creating this organization in 2007, representing francophone data protection authorities around the world and supporting developing Francophonie countries in the process of establishing data protection regimes.
- **Commission for the Control of INTERPOL's Files:** The OPC participates in meetings of this body, which serves as an independent watchdog on how INTERPOL lives up to its established standards on the processing of personal information.
- **The International Working Group on Data Protection in Telecommunications (Berlin Group):** This group examines technological developments that raise privacy issues and focuses of personal information on the Internet.

(see sidebar on page 30). In the next two years, we attended our first Organisation for Economic Cooperation and Development (OECD) and Asia-Pacific Economic Cooperation (APEC) meetings.

In June 2007, OECD member countries adopted the Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy. Among other things, this encouraged member countries to change their laws to allow authorities to collaborate and called for an informal network of privacy enforcement authorities.

Following this, we joined with 10 other privacy enforcement authorities to establish the [Global Privacy Enforcement Network](#) (GPEN) in March 2010, to foster cross-border co-operation among privacy authorities.

The same year also saw the launch of the APEC [Cross-border Privacy Enforcement Arrangement](#), under which member countries agreed to cooperate on consumer privacy investigations and enforcement matters.

## IMPORTANT CHANGE LEADING TO ACTION AND RESULTS

Some four years after the OECD's Recommendation, amendments to PIPEDA in 2011 allowed us to enter into formal, written agreements with other privacy enforcement authorities within Canada and abroad. This enables us to share information with other

organizations for enforcement purposes while maintaining confidentiality.

Since then, we have signed memoranda of understanding with our counterparts in Germany, Ireland, the Netherlands, the United Kingdom and Uruguay. In 2013, our agreement with our Dutch counterparts enabled us to complete the world's first joint [privacy investigation](#), into WhatsApp's cross-platform mobile messaging service.

Opportunities for collaboration of this kind also help us increase our capacity in the area of spam-related enforcement. For example, we have increased our engagement with the London Action Plan and the Messaging, Malware and Mobile Anti-Abuse Working Group, two key international networks in the anti-spam sphere that include substantial industry membership. This involvement is allowing us to learn from the experience of authorities enforcing long-established anti-spam legislation and cultivating partners for future enforcement cooperation.

## A LANDMARK YEAR FOR INTERNATIONAL PRIVACY PROTECTION ACTION

On top of signing new collaboration agreements with our counterparts in Dubai and Romania, 2014 included numerous examples of investigations and other enforcement activities based on information sharing and jointly coordinated activities.

### Links

#### Global Privacy Enforcement Network

<https://www.privacyenforcement.net/>

#### Cross-border Privacy Enforcement Arrangement

<http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx>

#### WhatsApp investigation

[https://www.priv.gc.ca/media/nr-c/2013/nr-c\\_130128\\_e.asp](https://www.priv.gc.ca/media/nr-c/2013/nr-c_130128_e.asp)

### *Putting a price on privacy*

Our Office received 27 complaints against the Romania-based website Globe24h.com in 2014, about how it collects and publishes the personal information of Canadians.

Given the similarity of the circumstances, we addressed all of the complaints through a single investigation.

Globe24h.com republishes legal findings from a number of jurisdictions, including a significant focus on Canada. In pre-digital times, including personal information in the written decisions of courts and tribunals had a very limited privacy impact. Simply put, in order to discover sensitive details about individuals contained in decisions, a person would have to go to the trouble of visiting a courthouse or archives and then take the further step of performing meticulous research.

Today, of course, information in digital form is available at our fingertips. And unlike other online legal repositories, Globe24h.com allows search engines to index pages, which dramatically increases the accessibility of the personal information contained in those findings.

For each of the complainants, Globe24h.com had republished a court or tribunal decision that contained sensitive personal about them.

Approximately one-third of the complaints to our Office dealt with family law matters such

as divorce or custody hearings. Others related to bankruptcy, human rights, labour relations and immigration matters—containing highly detailed, highly sensitive personal information, including financial and health information that could have negative reputational impacts.

One complaint, for example, was made on behalf of the complainant's daughter, who was named and described as a "sex worker" in a case in which she had acted as a witness. At the time of the complaint, this decision as republished by Globe24h.com was the first result returned when searching her name online.

In another case, a complainant was concerned that search results for the name of her son included information about an acrimonious custody hearing.

One man filed a complaint because he operated a business under his own name and was concerned that searches for that business also turned up financial and medical information about him that arose during a legal dispute.

Another individual was concerned that the publication of a court finding would make the pardon he had received completely ineffective.

Taking advantage of both the sensitivity of information published, and the resulting demand from many to have it removed, the company put both formal and informal



mechanisms in place for removing data from the site—for a fee. In our view, this amounts to the monetization of personal information by Globe24h.com by essentially extorting payment for its removal.

For example, at the time of the first complaint filed to our Office, individuals were given the option of an “express” removal of their personal information within 72 hours by paying a €19 (approximately \$25) processing fee per document. During our investigation, the paid option was removed as of July 2014. Despite this action by the website, one complainant reported Globe24h.com advised her that her file could “be removed in full” from its server “and Google” for €200 (about \$266).

In almost all instances, our Office was able to have the offending document removed from the site without cost, although concerns persist about the site’s overall operation.

To this end, and given the location of the website, our Office has entered into a cooperation arrangement with the Romanian data protection authority—which has also received complaints about the organization—toward securing an appropriate resolution to this matter. Our Office continues to pursue enforcement of our findings through multiple avenues.

### *Insufficient safeguards against an international breach*

In 2013, media reports revealed that there had been a sophisticated, long-term intrusion of Adobe Inc. computer systems affecting millions of customers around the world. An individual complained to us after he found personal information related to his Adobe account on a public website, after having been told that the breach did not affect him.

Following this, a joint investigation between our Office and Ireland’s Data Protection Commissioner in coordination with the Australian Data Protection Authority concluded that the safeguards Adobe had in place at the time of the breach were not appropriate given the sensitivity of the information involved (which included usernames, passwords, names and addresses, and encrypted payment card numbers). We were satisfied that Adobe conducted a thorough investigation of the breach and made changes to protect customer data, such as enhancing its user-password management process and decommissioning a server affected by the breach.

Since the effects of this breach were global in scale, it was incumbent on us to work with international partners to protect the privacy interests of individuals at home and abroad.

### *Sounding a warning on web cams*

In addition to extending the reach of any one data protection agency, collaboration and coordination brings the strength of numbers to enforcement activities, as well as speed when circumstances demand. In one instance in 2014, we were quickly able to engage numerous counterparts from around the world and address a significant invasion of privacy happening on a global scale.

In mid-November, our Office became aware of a website based in Eastern Europe that posted links to images from unsecured webcams in use around the world, including in Canada. The stated motive for this action was to highlight the hazards of not changing the username and password from the manufacturer's defaults. The net result was images of homes, workplaces and commercial spaces being broadcast for all to see, in many cases along with the exact geographic location of the camera.

Upon learning of the website, we promptly reached out to other privacy authorities, who were equally concerned. Our Office, along with the heads of the data protection authorities of the United Kingdom, Australia and Macao, as well as the Commissioners of Quebec, Alberta and British Columbia, sent the operators of the website a joint letter urging them to take down their feeds.

We were pleased that the website operators heeded our concerns and took down the site

following our joint letter. Since then, the website has been re-established in a more limited form with links primarily to webcams in public locations.

Building from this result, we also worked with our counterparts to prepare **information letters** sent to manufacturers, urging them to ensure the appropriate security measures are in place to protect their customers' privacy and provide further guidance to customers about ensuring the security of their webcams.

### *A not-so-clean sweep*

As the coordinator for the second **GPEN Privacy Sweep**, we built on the success of the inaugural 2013 event, bringing together data protection agencies from around the world to focus on a specific privacy-related issue. A total of 26 privacy enforcement authorities participated in the 2014 Sweep, up from 19 in 2013.

The 2014 theme was mobile privacy. In all, participating agencies assessed more than 1,200 of the world's most popular mobile apps—including 151 assessed by our Office—looking at the types of permissions an app was seeking, whether those permissions exceeded what would be expected based on the app's functionality, and most importantly, how the app explained to consumers why it wanted the personal information and what it planned to do with it.

## Links

### **Information letters**

[https://www.priv.gc.ca/media/nr-c/2015/let\\_150212\\_e.asp](https://www.priv.gc.ca/media/nr-c/2015/let_150212_e.asp)

### **GPEN Privacy Sweep**

[https://www.priv.gc.ca/media/nr-c/2014/nr-c\\_140910\\_e.asp](https://www.priv.gc.ca/media/nr-c/2014/nr-c_140910_e.asp)

### OPC continues lead role in global enforcement network

In addition to coordinating GPEN's annual Privacy Sweep, we are also an active member of the five-country GPEN Management Committee, along with the U.K., New Zealand, Israel and the U.S.

Our Office provides technical support to the GPEN website, which is hosted by the OECD. In 2014, among other changes, we added a joint enforcement contact facility for the OECD, APEC and the Council of Europe, and enhanced the platform for public communications on GPEN activities.

Overall, GPEN had an extremely successful year in 2014, promoting and supporting cooperation in cross-border enforcement of laws protecting privacy. In addition to the number of member authorities rising by 50 percent to reach 51 members, communication between authorities on the secure website is also increasing.

Overall, while the **sweep found** that many popular apps are building user trust by providing clear, easy-to-read and timely explanations about what information they collect and how it is used, many others are failing to provide even the most basic privacy information. For example, 85 percent of apps left users questioning how their personal information might be collected, used or disclosed.

Following the sweep, we took the lessons learned and developed practical advice for app developers in the form of **Ten Tips for Communicating Privacy Practices to Your App's Users**.

Following up on specific concerns about particular apps, we issued letters that led to improved privacy practices for over 100 apps, based both in Canada and abroad.

### *Clarifying what's in store when visiting an app marketplace*

On the heels of the Sweep, we joined with the Privacy Commissioner for Personal Data of Hong Kong in encouraging app marketplaces, such as those operated by Apple and Google, to improve transparency by requiring developers to post links to privacy policies. Together with 23 international counterparts, we **published** an open letter to this effect in early December.

### Links

#### **Sweep results**

[https://www.priv.gc.ca/media/nr-c/2014/nr-c\\_140910\\_e.asp](https://www.priv.gc.ca/media/nr-c/2014/nr-c_140910_e.asp)

#### **Ten Tips for Communicating Privacy Practices to Your App's Users**

[https://www.priv.gc.ca/resource/fs-fi/02\\_05\\_d\\_61\\_tips\\_e.asp](https://www.priv.gc.ca/resource/fs-fi/02_05_d_61_tips_e.asp)

#### **Open letter**

[https://www.priv.gc.ca/media/nr-c/2014/let\\_141210\\_e.asp](https://www.priv.gc.ca/media/nr-c/2014/let_141210_e.asp)

### *A new, broader, multilateral approach*

Bilateral arrangements and regional initiatives to promote cooperation have, undoubtedly, been useful in our ongoing efforts to enforce data protection legislation. However, the paths that information takes in this technology-driven era dictate that information sharing and enforcement efforts happen on a broader scale to allow authorities to cover more ground, more quickly.

Toward that end, in 2014, privacy authorities around the globe took the next important step.

The Global Cross Border Enforcement Cooperation Arrangement is the fruit of collaborative thinking and planning by the members of the International Conference of Data Protection and Privacy Commissioners. Announced at the 2014 Conference in Mauritius, this arrangement will provide a common foundation for expedited multilateral information sharing and enforcement cooperation by privacy authorities around the world.

The new arrangement sets out ground rules for the sharing of confidential information related to enforcement work. For example, it could enable several data protection authorities to work together to respond to a major data breach. The ability to share this type of information is critical to coordinating enforcement efforts. For us, this multi-lateral

**The Global Cross Border Enforcement Cooperation Arrangement was not the only collaborative initiative to be announced in Mauritius. Data protection agencies from the Commonwealth agreed in Mauritius to create the Common Thread Network. The aim of this group is to facilitate the sharing of experiences, knowledge and expertise, and promote cross-border cooperation among Commonwealth jurisdictions. The founding members also acknowledged the important role that robust data protection can have in fostering growth in the field of information and communications technologies and, as a result, promoting socio-economic development.**

mechanism is an important addition to our existing bilateral memoranda of understanding.

We are proud to have joined our counterpart in the U.K. in leading the drafting of the documents underpinning this new approach to privacy law enforcement.

## LOOKING AHEAD

The Global Cross Border Enforcement Cooperation Arrangement, slated to come into effect in October 2015, has the potential to be the broadest privacy enforcement arrangement of its kind in the world—providing a more effective and efficient way for data protection agencies to reap the benefits of each other's enforcement work and to strengthen overall privacy protection activities.

In turn, our combined work can result in stronger and clearer messages aimed at international companies that need to comply with a variety of different privacy laws around the world to encourage and compel improved privacy protection practices.

Global support for this new arrangement from international privacy and data protection commissioners, as well as the growing participation in GPEN, the annual Privacy Sweep—planning for the 2015 edition is well under way—and other international endeavours highlight the importance the privacy enforcement community places on cooperation to advance the case for personal information protection.

More and more, when it comes to privacy protection, international cooperation is clearly the new normal. Our Office has taken the necessity for international enforcement collaboration to heart, and can say with confidence that Canadians will see benefits from our work to protect their personal information wherever it may travel.

Greater collaboration among privacy protection authorities can help build citizen trust, enabling individuals to partake in the global, digital economy with confidence and to embrace new, innovative products and services with trust rather than trepidation.

Ultimately, this end result will be beneficial to everyone's bottom line.



# Investigation Statistics

## PIPEDA 2014 - COMPLAINTS 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	50	4			8	3	2	1	9		<b>77</b>
Use and Disclosure	35	5		7	14		6		6		<b>73</b>
Collection	29	1		5	9	1	14	1		1	<b>61</b>
Appropriate purposes	1	2	56							1	<b>60</b>
Safeguards	24	1			11	1	1		2		<b>40</b>
Consent	16				5	2	2		1	3	<b>29</b>
Time Limits	11								1		<b>12</b>
Accuracy	5				2				2		<b>9</b>
Retention	7								1		<b>8</b>
Accountability	2								1		<b>3</b>
Correction/Notation	0								1		<b>1</b>
Identifying Purposes	0									1	<b>1</b>
Openness										1	<b>1</b>
<b>Total</b>	<b>180</b>	<b>13</b>	<b>56</b>	<b>12</b>	<b>49</b>	<b>7</b>	<b>25</b>	<b>2</b>	<b>24</b>	<b>7</b>	<b>375</b>

PIPEDA 2014 - **AVERAGE TREATMENT TIMES BY DISPOSITION**

<b>Disposition</b>	<b>Number</b>	<b>Average Treatment Time in Months</b>
Early Resolution-Resolved	180	2.4
Settled	7	6.8
Discontinued (under 12.2)	13	5.7
Withdrawn	49	6.0
No Jurisdiction	12	7.8
Not well-founded	25	12.4
Well-founded conditionally resolved	7	27.4
Well-founded resolved	24	11.5
Well-founded	2	15.5
Declined to investigate	56	0.6
<b>Total cases</b>	<b>375</b>	
<b>Overall weighted average</b>		<b>4.8</b>



PIPEDA 2014 - **PIPEDA TREATMENT TIMES** - Average Treatment Times by Complaint and Resolution Types

Complaint Type	Early Resolution		All Other Resolutions (not ER)	
	Number of cases	Average Treatment Time in Month	Number of cases	Average Treatment Time in Month
Access	50	2.7	27	10.4
Accountability	2	7.4	1	15.8
Accuracy	5	3.0	4	8.9
Appropriate purposes	1	3.4	59	1.0
Collection	29	2.8	32	10.3
Consent	16	2.3	13	13.5
Correction/Notation			1	10.6
Identifying Purposes			1	30.9
Openness			1	30.9
Retention	7	2.1	1	15.1
Safeguards	24	2.5	16	6.9
Time Limits	11	1.5	1	3.4
Use and Disclosure	35	1.8	38	6.9
<b>Grand Total</b>	<b>180</b>	<b>2.4</b>	<b>195</b>	<b>7.0</b>

PIPEDA 2014 - **PIPEDA VOLUNTARY BREACH NOTIFICATIONS** - By Industry Sector and Type of Incident

Sector	Incident type			Total incidents per sector	Proportion of all incidents
	Accidental Disclosure	Loss	Theft and Unauthorized access		
Accommodations			1	1	2%
Financial	9	2	5	16	36%
Insurance	2		4	6	14%
Internet	1		6	7	16%
Other Sectors	1			1	2%
Professionals			1	1	2%
Sales/Retail	2		3	5	11%
Services	1	1	1	3	7%
Telecommunications	1		2	3	7%
Transportation	1			1	2%
<b>Grand Total</b>	<b>18</b>	<b>3</b>	<b>23</b>	<b>44</b>	<b>100%</b>

### PIPEDA 2014 - COMPLAINTS ACCEPTED BY INDUSTRY SECTOR

Sector Category	Number	Proportion of all complaints accepted
Accommodations	19	5%
Entertainment	4	1%
Financial	81	20%
Insurance	21	5%
Internet	72	18%
Other Sectors	24	6%
Professionals	9	2%
Sales/Retail	25	6%
Services	23	6%
Telecommunications	52	13%
Transportation	72	18%
<b>Total</b>	<b>402</b>	<b>100%</b>

PIPEDA 2014 - **COMPLAINTS ACCEPTED BY COMPLAINT TYPE**

<b>Complaint Type</b>	<b>Number</b>	<b>Proportion of all complaints accepted</b>
Access	77	19%
Accountability	3	0%
Accuracy	8	2%
Appropriate purposes	60	15%
Collection	65	16%
Consent	47	11%
Retention	7	1%
Safeguards	33	7%
Time Limits	12	7%
Use and Disclosure	90	22%
<b>Grand Total</b>	<b>402</b>	<b>100%</b>

## PIPEDA 2014 - COMPLAINTS 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	31		4	1	20	1	15		7		48	79
Transportation	12	56	1		3	1				1	62	74
Telecommunications	34		2		1	1	4		2		10	44
Services	19			2	4	1			6		13	32
Internet	16		2	2	3		2		1	5	15	31
Other Sectors	15		1	3	6	1		1	1		13	28
Insurance	14		1	2	4	1	1		4		13	27
Sales/Retail	16		1		1	1		1	1	1	6	22
Accommodations	16				1		2				3	19
Professionals	4		1	2	5						8	12
Entertainment	3				1		1		2		4	7
<b>Total</b>	<b>180</b>	<b>56</b>	<b>13</b>	<b>12</b>	<b>49</b>	<b>7</b>	<b>25</b>	<b>2</b>	<b>24</b>	<b>7</b>	<b>195</b>	<b>375</b>

# Appendix 1

## Definitions of Complaint Types under PIPEDA

Complaints received by the OPC are categorized according to the principles and provisions of PIPEDA that are alleged to have been contravened:

**Access.** An individual has been denied access to his or her personal information by an organization, or has not received all the personal information, either because some documents or information are missing or because the organization has applied exemptions to withhold information.

**Accountability.** 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*.

**Accuracy.** An organization has failed to ensure that the personal information it uses is accurate, complete, and up-to-date.

**Challenging compliance.** 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.

**Collection.** An organization has collected personal information that is not necessary, or has collected it by unfair or unlawful means.

**Consent.** An organization has collected, used or disclosed personal information without meaningful consent, or has made the provision of a good or service conditional on individuals consenting to an unreasonable collection, use, or disclosure.

**Correction/Notation.** The organization has failed to correct personal information as requested by an individual, or, where it disagrees with the requested correction, has not placed a notation on the information indicating the substance of the disagreement.

**Fee.** An organization has required more than a minimal fee for providing individuals with access to their personal information.

**Openness.** An organization has failed to make readily available to individuals specific information about its policies and practices relating to the management of personal information.

**Retention.** Personal information is retained longer than necessary for the fulfillment of the purposes that an organization stated when it collected the information, or, if it has been used to make a decision about an individual, has not been retained long enough to allow the individual access to the information.

**Safeguards.** An organization has failed to protect personal information with appropriate security safeguards.

**Time limits.** An organization has failed to provide an individual with access to his or her personal information within the time limits set out in the *Act*.

**Use and disclosure.** Personal information is used or disclosed for purposes other than those for which it was collected, without the consent of the individual, and the use or disclosure without consent is not one of the permitted exceptions in the *Act*.

## Appendix 2

### Definitions of Findings and Other Dispositions

At the beginning of 2012, our Office altered some of the definitions of findings and dispositions in order to better convey the outcomes of our investigations under PIPEDA, and to better reflect the responsibilities of organizations to demonstrate accountability under the *Act*.

The definitions below explain what each disposition means.

**Not well-founded:** The investigation uncovered no or insufficient evidence to conclude an organization contravened PIPEDA.

**Well-founded and conditionally resolved:** The Commissioner determined that an organization contravened a provision of PIPEDA. The organization committed to implementing the recommendations made by the Commissioner and demonstrating their implementation within the time frame specified.

**Well-founded and resolved:** The Commissioner determined that an organization contravened a provision of PIPEDA. The organization demonstrated it had taken satisfactory corrective action to remedy the situation, either proactively or in response to recommendations made by the Commissioner, by the time the finding was issued.

**Well-founded:** The Commissioner determined that an organization contravened a provision of PIPEDA.

**Settled:** The OPC helped negotiate a solution that satisfied all involved parties during the course of the investigation. The Commissioner does not issue a report.



**Discontinued:** The investigation was discontinued before the allegations were fully investigated. An investigation may be discontinued at the Commissioner's discretion for the reasons set out in subsection 12.2(1) of PIPEDA, as a result of a request by the complainant, or where the complaint has been abandoned.

**Declined to Investigate:** 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.

**No jurisdiction:** Based on the preliminary information gathered, it was determined that PIPEDA did not apply to the organization or activity that was the subject of the complaint. The Commissioner does not issue a report.

## Appendix 3 Investigation Process

