



Office of the
Privacy Commissioner
of Canada



PRIVACY

privacy

Privacy

privacy

Privacy

privacy

Privacy

privacy

Privacy

Privacy

PRIVACY

Privacy

Privacy

privacy

privacy

privacy

privacy

The drawings on this page and throughout the report are the works of the children of employees at the Office of the Privacy Commissioner of Canada.

Office of the Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

(613) 947-1698, 1-800-282-1376
Fax (613) 947-6850
TDD (613) 992-9190

© Minister of Public Works and Government Services Canada 2012

Cover image: Alin Popescu / Shutterstock.com

Cat. No. IP51-1/2011
1910-0051

This publication is also available on our website at www.priv.gc.ca.

Follow us on Twitter: @privacyprivee



**Privacy Commissioner
of Canada**

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 947-1698
Fax: (613) 947-6850
1-800-282-1376
www.priv.gc.ca

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

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél.: (613) 947-1698
Télééc.: (613) 947-6850
1-800-282-1376
www.priv.gc.ca



June 2012

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

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Personal Information Protection and Electronic Documents Act* for the period from January 1 to December 31, 2011.

Yours sincerely,

Original signed by

Jennifer Stoddart
Privacy Commissioner of Canada

**Privacy Commissioner
of Canada**

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 947-1698
Fax: (613) 947-6850
1-800-282-1376
www.priv.gc.ca

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

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél.: (613) 947-1698
Télééc.: (613) 947-6850
1-800-282-1376
www.priv.gc.ca



June 2012

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, 2011.

Yours sincerely,

Original signed by

Jennifer Stoddart
Privacy Commissioner of Canada

Table of Contents

Message from the Commissioner	1
Privacy by the Numbers in 2011	7
1. Overview of 2011	9
1.1 Serving Canadians	9
1.2 Supporting Parliament	10
1.3 Supporting Organizations	11
1.4 Advancing Knowledge	12
1.5 Global Initiatives.....	13
1.6 Technology Lab	15
2. Key Issue: Children and Youth Privacy.....	17
2.1 Investigations Relating to Children and Youth	20
• Nexopia	20
• Webcam use in a daycare.....	25
2.2 Surveillance of Children.....	26
2.3 Youth Outreach Initiatives	27
2.4 Digital Literacy	28
2.5 Contributions Program - Projects for Youth	30
3. The Privacy Landscape	
Overview of other major issues addressed by the OPC	31
3.1 Financial Privacy	32
• Investigations	32
• Task Force for the Payments System Review.....	36
3.2 Biometrics	37
• Investigation	37
• Biometrics Guidance Document	41
3.3 Online Privacy	42
• Investigations (Facebook, Google).....	42
• Canada's Anti-Spam Legislation	46
• Consumer Privacy Consultations.....	47
• Online Behavioural Advertising Guidance.....	48
• Privacy Poll	49
• Technology Lab	50
3.4 Modernization of Privacy Laws	50
• Implementing Amendments to PIPEDA	50
• Reducing the Risk of Data Breaches	51
• PIPEDA review.....	52

Table of Contents

4. Meeting the Concerns of Canadians	53
4.1 Information Requests	53
4.2 Intake	54
4.3 Complaints Received	54
4.4 Complaints by Industry Sector	55
4.5 Types of Complaints Received	56
4.6 Early Resolution	56
4.7 Complaint Investigations	59
4.8 Snapshot of 2011 Investigations	60
4.9 Data Breaches	67
5. Reaching out to Canadians	71
5.1 Toronto Office	72
5.2 Self-Assessment Tool for Organizations	73
5.3 Small Business Week - Cyber Security	74
5.4 Business Poll	75
5.5 Lawyers' Handbook	75
5.6 Data Privacy Day 2011	76
5.7 Outreach Across Canada	76
5.8 Contributions Program	76
5.9 Speaking Engagements	78
6. In the Courts	79
7. Substantially Similar Provincial and Territorial Legislation	83
8. The Year Ahead	85
Appendix 1	91
Definitions	91
Investigation Process	94
Appendix 2	96
PIPEDA Investigation Statistics for 2011	96

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 to organizations engaged in commercial activities across the country, except in provinces that have substantially similar private sector privacy laws. Quebec, Alberta and British Columbia each have their own law covering the private sector. Even in these provinces, PIPEDA continues to apply to the federally regulated private sector and to personal information in inter-provincial and international transactions.

PIPEDA also protects employee information, but only in the federally regulated sector.

Message from the Commissioner

Teenagers are growing up in a very different world than I did.

Today's youth have an unprecedented ability to communicate. This first wave of what some have called the "Facebook generation" has latched onto the on-line world to stay in touch with friends – sharing new YouTube videos and the latest hit songs, making plans to hang out, and talking about what's happening in their lives.

I did many of the same things with my school friends – except that I did all this in person or over the phone shared with other family members.

The big difference about what I used to do and now is that there is no record of what my friends and I gossiped about back then. That was also the case for my own children – who are still only in their 20s.



But that's clearly not the case for anyone who is now a teenager.

All of that online communication creates a permanent record – and that could carry risks to their privacy and to their reputations. Not just today, but perhaps even more in the future.

Teenagers are expected to make mistakes - it's a natural part of growing up.

The fact that electronic records of many of the mistakes of today's youth will persist for decades to come is cause for deep concern.

Indeed, a host of perils threaten the privacy and personal information of children and youth – one of the reasons that we have made them a key focus of this report.

Not only are the young usually the first to embrace any new kind of digital communication, they are also often unsuspecting about the potential privacy intrusions that can accompany such novel technologies.

And there's another good reason why our efforts to protect the personal information of children and youth warrant their own chapter. They constitute an important example of where my Office is providing leadership on a priority privacy issue.

Providing such leadership is a commitment I made to MPs and Senators when I was reappointed to a three-year term as Privacy Commissioner of Canada. It was one of three areas on which I promised to focus; the other two were supporting informed privacy decision-making and improving service delivery to Canadians.

Now, one year into my renewed mandate, seems an appropriate point to review progress in fulfilling those commitments.

SIGNIFICANT PRIVACY ISSUES

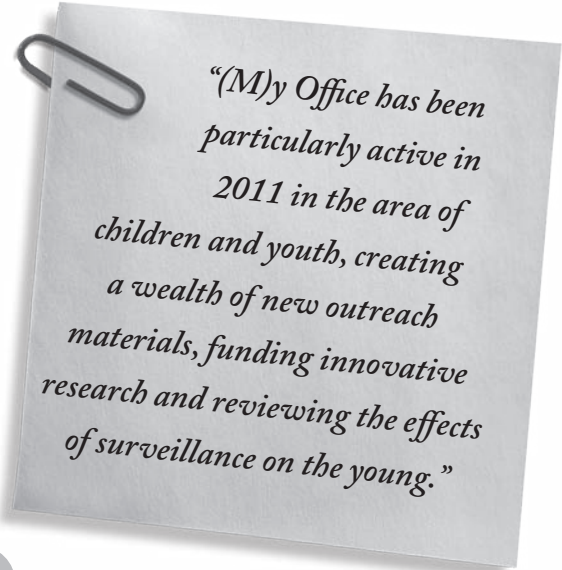
First, leadership on significant privacy issues. As described later in this report, my Office has been particularly active in 2011 in the area of children and youth, creating a wealth of new outreach materials, funding innovative research and reviewing the effects of surveillance on the young.

We also wrapped up a comprehensive investigation into a complaint about privacy concerns related to a

social networking website that specifically targeted young people. This first OPC investigation of a youth-oriented social networking site was highly complex, resulting in a detailed Report of Findings of some 100 pages, with 24 recommendations.

However, many of the problems with the site could have been avoided if only privacy considerations had been taken into account back when the operation was being designed and launched. For that reason, my Office considers that this particular investigation ought to serve as "lessons learned" for everyone engaged in handling the personal information of youth.

Another area in which we also provided privacy leadership was the burgeoning use of online behavioural advertising. While the term itself may be unfamiliar, almost all Canadians who go online will have seen such advertising.



"(M)y Office has been particularly active in 2011 in the area of children and youth, creating a wealth of new outreach materials, funding innovative research and reviewing the effects of surveillance on the young."

Officially, online behavioural advertising is defined as the practice of tracking a consumer's online activities in order to deliver advertising geared to that consumer's inferred interests. What it means in practice is that Internet ad networks follow you around online, watching what you do so they can serve you targeted ads.

Late in 2011, we published guidance about how the parties involved in – or benefiting from – online behavioural advertising can ensure that their practices are fair, transparent and in compliance with the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

We specifically pointed out that organizations engaged in online behavioural advertising should avoid tracking children – or tracking on websites aimed at children – since meaningful consent may be difficult to obtain.

Yet another area of providing leadership on a priority privacy issue during the year was the “lawful access” legislation which had been announced by the Government (and which was eventually introduced as Bill C-30 early in 2012.) This legislation would have obvious impacts on the telecommunications industry. Following up on earlier mutual representations with provincial and territorial commissioners responsible for privacy, in October I sent an open letter to Public Safety Minister Vic Toews outlining my concerns that the expanded surveillance regime proposed in the legislation would have serious repercussions for privacy rights.

INFORMED PRIVACY DECISIONS

The second topic on which I committed to focus in my renewed mandate was supporting informed privacy decision-making by Canadians, organizations and institutions.

In May, my Office laid a solid foundation for this effort by publishing a final report on extensive public consultations the previous year about online tracking, profiling and targeting and cloud computing. From what we learned in those consultations flowed such things as tip sheets about cookies and cloud computing, a speakers series spotlighting frontier privacy challenges, the work on children and youth, the online behavioural advertising guidance and some of the questions in our biennial public opinion survey.

But that was by no means the sum of my Office's efforts to make sure that Canadians develop strong digital literacy skills and better understand privacy rights.

For lawyers, we provided a handbook covering the privacy issues they were most likely to encounter during litigation and the running of a law office. For small businesses, we authored a set of DIY articles on protecting their valuable information – including personal details about customers – from online threats.

Working together, the OPC and its counterparts in Alberta and British Columbia also devised an innovative, online tool which allows organizations to assess the personal information safeguards necessary

in records management, network security, continuity planning and 14 other operational areas.

SERVICE DELIVERY

My third commitment was to focus on improving service delivery to Canadians. This is where the rubber truly hits the road in my Office, led by the day-to-day handling of information requests and complaints.

Streamlined procedures and the benefits of experience continued to yield improvements in our handling of complaints in 2011. The average time to deal with an accepted complaint dropped from more than 15 months in 2010 to just above eight months, significantly below the 12-month requirement in the Act.

A major contribution to this performance improvement can be traced to our greater use of an early resolution process which sidesteps an official investigation for selected complaints. By working with both the complainant and the respondent organization, our early resolution officers were able to successfully clear up more than 90 percent of the cases this process handles - without resorting to a full investigation.

And to continue to meet the needs and expectations of Canadians in the rapidly evolving digital environment, we strengthened our technology laboratory, which provides expert support to our audits and investigations and will also support the OPC's responsibilities under Canada's new anti-spam legislation.



As an Officer of Parliament, I have a special responsibility to Parliamentarians. The Assistant Privacy Commissioner and I, as well as other senior officials from my Office, appear before committees, examine legislation for privacy implications, submit comments and have numerous informal interactions with Parliamentarians and staff.

This 2011 Annual Report contains many more examples of how we have delivered on the commitment to these three focus areas.

MAKING A DIFFERENCE

However, the overarching question must be: Are we making a difference?

The answer is that, 10 years after PIPEDA became law, there is encouraging evidence that the OPC has had a positive impact on the privacy landscape.

According to public opinion surveys commissioned by the OPC, the proportion of Canadians saying they feel they have less protection of their personal privacy in daily life than a decade previously has declined, from 71 percent in 2006 to 61 percent in 2011.

I believe that the Office of the Privacy Commissioner of Canada deserves some of the credit for this change in public attitudes.

Recent years have brought continual challenges to the OPC and the first-class team of professionals here has consistently upped its game. The year 2011 was no exception and I am fortunate to work with such committed, hard-working and imaginative people. These include my indispensable Assistant Commissioner, Chantal Bernier, whose unflinching enthusiasm and intellectual curiosity are a source of constant inspiration.

Despite the welcome change in public attitudes, however, the proportion of Canadians telling the survey that protection of personal privacy will be one of the most important issues facing the country over the next 10 years has remained essentially unchanged from 2006 to 2011, at two-thirds.

To me, the explanation for this apparent paradox is straightforward.

Canadians appreciate that more is being done to protect their privacy and personal information. Yet they also understand that new challenges mean that still more must be done.

Prominent among those challenges is the rise of what is being called Big Data. In essence, this refers to the ability brought about through technological advances to gather more data than would have been conceivable just a few years ago and then sift through it, looking for patterns.

BENEFITS AND DANGERS

There's no denying some potential benefits to society from Big Data. To take a somewhat prosaic example, Google is now able to spot flu outbreaks in North America days faster than national health authorities by flagging clusters of online inquiries about symptoms and remedies.

This undoubted public health benefit was quickly taken up by commercial interests. An article in the *New York Times* described how a large marketing firm devised advertisements for a behind-the-ear thermometer which were sent to smartphones loaded with certain apps that collect basic details about the users, including their gender and whether they are parents. So the thermometer ad was specifically targeted at smartphones used by mothers of young children.

In addition, the ad was sent only to smartphones being used in regions where Google detected a flu spike and where the mothers were within three kilometres of retailers carrying the thermometer. Tapping the onscreen ad took the smartphone user to a product page with an informational video and a list of nearby retailers.

Some may find such personalized tracking by advertisers “creepy,” others might welcome targeted ads as relevant and helpful.

Whatever your view, this is only the beginning of where Big Data is going.

The many new forms of digital communication between individuals – texting, emails, instant messaging and so on – are all very easily computer readable and therefore subject to complex analysis by computers. Sophisticated software can track individuals through their unique identifying device numbers – revealing their location in time and place, their Internet activities and their interactions with other people with whom they form a “community.”

As Leonard Cohen prophetically sang in “The Future” two decades ago, in years to come, “won’t be nothing you can’t measure anymore.”

INFORMATION EXPLOSION

Until recently, the definition of personal information was fairly clear-cut for most people. It was what you’d find on a tombstone, plus traditional things like address, phone number, Social Insurance Number, driver’s licence and passport, and so on. Now people scatter digital crumbs containing personal information as they move through their online existence.

And the volume of those crumbs is mounting at an explosive rate.

My Office has already laid down guidelines for the use of such information in the specific instance of online behavioural advertising. But there will undoubtedly be uses we can’t currently foresee which will have serious implications for privacy.

That’s why, in the end, improving the digital literacy of all Canadians is so crucial.

Jennifer Stoddart
Privacy Commissioner of Canada



Privacy by the Numbers in 2011

PIPEDA information requests received	5,236
PIPEDA formal complaints accepted	281
PIPEDA early resolution cases successfully closed	116
PIPEDA investigations closed	120
Draft bills and legislation raising PIPEDA issues reviewed for privacy implications	11
Policy guidance documents issued	5
Parliamentary committee appearances	5
Other interactions with Parliamentarians or staff (for example, meeting with MPs or Senators)	33
Speeches and presentations delivered	143
Contribution agreements signed	8
Visits to main Office website	1,843,686
Visits to Office blogs and other websites (including OPC blog, youth blog, youth website, deep packet inspection website and YouTube channel)	871,698
Total	2,715,384
"Tweets" sent	416
Publications distributed	11,811
News releases issued	37

Note: Unless otherwise specified, these statistics also include activities under the *Privacy Act*, which are described in a separate annual report.

Overview of 2011

1.1 SERVING CANADIANS

INFORMATION REQUESTS

During 2011, our Office handled more than 5,200 phone calls, emails and letters from Canadians about privacy issues in the private sector covered by PIPEDA. Issues related to the use of Social Insurance Numbers remained a common reason that people contact us for information. As well, we are receiving a growing number of requests related to online issues, particularly with respect to social networking sites. More details appear in section 4.1.

COMPLAINTS

In yet another move to speed up service to Canadians, we created a dedicated Intake Unit, which initially reviews all written complaints received. If necessary, the Unit follows up with the complainant to clarify our understanding of the complaint and gather any additional information or documents necessary so we can launch an investigation as quickly as possible.

This streamlined screening has helped to reduce the average times of an investigation. Combined with other complaint handling improvements such as the increased use of early resolution approaches, the result has been a further drop in the time it takes to handle all formal complaints – now down to an average of 8.2 months – well below the 12-month requirement set out in PIPEDA. (See Appendix 2 for details.)

We accepted a total of 281 formal complaints in 2011, compared to 207 in 2010. Possible explanations for this 35 percent rise include an increased complexity of issues raised, heightened public awareness of privacy rights or more intense interaction with business in the digital economy.

In 2011, we completed 125 early resolution cases and all but nine were satisfactorily resolved without opening a formal investigation.

COMPLAINT INVESTIGATIONS

We completed 120 formal investigations into complaints related to the private sector in 2011. This is a significant decrease from 2010, when we completed 249 investigations, in the culmination of a two-year effort to clear a backlog of complaints.

We have made privacy issues related to children and youth a focus of this year's report and summaries of the relevant complaint investigations are included in Chapter 2.

Investigations related to financial privacy, online privacy and biometrics appear in Chapter 3, a survey of the 2011 privacy landscape. Information on still other complaint investigations is provided in Chapter 4.

1.2 SUPPORTING PARLIAMENT

From a legislative perspective, Parliament and its committees had a reduced sitting schedule during 2011 because of the general election. As well, with Parliamentary priorities focused mainly on public sector concerns such as crime and the federal budget, our Office was called upon for fewer PIPEDA-related appearances.

The general federal election of May 2, 2011 sent new members to the House of Commons for the third time since 2006. The Conservative Party remained in power, increasing their seats from a minority to a majority in the 41st Parliament.

PUBLIC AWARENESS

Our Office uses many different tools to raise awareness of privacy among Canadians – speeches and other public presentations, media interviews, paper and online publications, an ever-changing website, social media such as Twitter and blogs, YouTube videos, contests for young people, educational kits for teachers and even a popular privacy calendar.

Details of our public awareness activities can be found in Chapter 5.

While the government has focused largely on public sector-related bills, it also reintroduced Bill C-12, an *Act to amend the Personal Information Protection and Electronic Documents Act*. When the year ended, it was still at the beginning of the legislative process and had not been referred to a standing committee for review.

The Government also said it would introduce Internet surveillance legislation that did not pass in the previous Parliament. In this regard, we continued to express our concerns related to lawful access legislation.

APPEARANCES BEFORE MPS AND SENATORS

During 2011, our Commissioner and Assistant Commissioner made five Parliamentary committee appearances.

The OPC also examined a total of 11 bills as well as two new committee studies introduced in the 41st Parliament for potential privacy implications. One was the E-Commerce in Canada study of the Standing Committee on Industry, Science and Technology.

Throughout the year, we also had many informal interactions with Parliamentarians, including follow-ups to committee appearances, subject-matter inquiries from Members of Parliament, face-to-face meetings and briefings.

PIPEDA-RELATED PARLIAMENTARY WORK

Given the reduced sitting schedule in 2011, the Standing Committee on Access to Information, Privacy and Ethics postponed a review of our 2010 Annual Report to Parliament on PIPEDA.

1.3 SUPPORTING ORGANIZATIONS

This past year we released a final report on our 2010 Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing. The contributions and analysis associated with the consultations gave rise to several activities in 2011, including:

- guidelines to help organizations involved in online behavioural advertising ensure that their practices are fair, transparent and in compliance with PIPEDA; and
- continuing work to develop cloud computing guidance specifically directed to privacy issues relevant to Small- and Medium-sized Enterprises (SMEs). This guidance will be available early in 2012.

We also offered guidance to legal professionals in the private sector. *PIPEDA and Your Practice — A Privacy Handbook for Lawyers*, launched in August, explains how PIPEDA relates to the everyday practice of Canadian lawyers.

Our Office, along with the Offices of the Information and Privacy Commissioners of Alberta and British Columbia, jointly launched a new online tool to help businesses better safeguard the personal information of customers and employees. *Securing Personal Information: A Self-Assessment Tool for Organizations* is a detailed online questionnaire and analysis instrument that helps organizations gauge how well they are protecting personal information, in keeping with the applicable private sector privacy law.

The OPC Toronto office, established in 2010, undertook almost 50 outreach activities in 2011 to organizations and industry associations. These were part of our efforts to increase understanding of PIPEDA and compliance requirements by business.

Chapter 5 contains more details of these various initiatives.

1.4 ADVANCING KNOWLEDGE

ARMCHAIR DISCUSSIONS

An OPC priority is helping Canadians better understand the diverse privacy issues that affect their lives and how they can protect their privacy.

In 2011, we organized a few armchair discussions to spotlight new and provocative voices exploring new perspectives on privacy research. We also asked each speaker for short papers exploring areas that interest them in the field of privacy.

In February 2011, we invited behavioural economist Alessandro Acquisti, associate professor of Information Technology and Public Policy at the Heinz College, Carnegie Mellon University, and sociologist Christena Nippert-Eng, associate professor of sociology in the College of Science and Letters at the Illinois Institute of Technology, to talk about what motivates us to reveal or conceal details of our personal lives, and how we protect the private lives of others around us.

In April, we invited tech innovators Adam Greenfield and Aza Raskin to explore opportunities for privacy ranging from the design of intimate

devices, like smartphones, that we share our lives with every day, to the sensor-rich landscape around us. They discussed opportunities for companies to empower individuals with greater choice and control over how their data are used and the prospects for greater collaboration within and across industry sectors.

In June, we heard from Canada Research Chair David Murakami-Wood, associate professor in the Department of Sociology at Queen's University, and Craig Forcece, associate professor in the Faculty of Law at the University of Ottawa, who both examined the privacy risks in a society that is increasingly placing its citizens under greater surveillance.

In September, we invited two experts on young people's use of social media, Kate Raynes-Goldie, Ph.D. candidate at the Department of Internet Studies at Curtin University of Technology, and Matthew Johnson, director of education with the Media Awareness Network, to talk about what privacy means to youth and how to help youth preserve their privacy by promoting digital literacy skills.

1.5 GLOBAL INITIATIVES

ENFORCEMENT COOPERATION

In 1973, Sweden enacted the world's first national privacy law. Four decades later, there are now roughly 80 national privacy laws, or data protection laws as they are often called, in force globally. Many have been passed since PIPEDA came into force on January 1, 2001.

Although differing significantly in terms of scope and enforcement, most of these laws are based on what are commonly referred to as “fair information principles.” These principles are set out in Schedule 1 of PIPEDA.

Sharing common principles allows privacy commissioners and data protection authorities to pursue common goals even if the wording of their legislation differs – PIPEDA's “limiting collection” is “data minimization” in European law.

Not only do privacy enforcement authorities share the similar objectives of promoting the protection of personal information and furthering the rights of individuals, but they also face similar challenges.

Privacy issues are becoming global. Increasingly, individuals throughout the world rely on common information and communication technologies; they share information, videos and photos using a few highly popular social networking platforms; they play online games using the same platforms and they

conduct searches using the same search engines. As a result, when one of these global companies changes its privacy practices, or worse, when it experiences a privacy breach (as we witnessed with Sony's PlayStation Network in 2011), millions of people worldwide can be affected.

Global issues demand a global response. As a result of amendments to PIPEDA that came into force in 2011, our Office is in a much better position to cooperate with our foreign counterparts on issues that affect individuals in other jurisdictions.

We can now collaborate and share information with persons or bodies in a foreign state that have similar legislated functions and duties or with persons or bodies who have legislated responsibilities relating to conduct that would be a contravention of PIPEDA. By sharing our expertise and the information we obtain during our investigations, we can use our resources more effectively and conduct more thorough and efficient investigations.

Our ability to share information is subject to certain conditions, most notably a requirement for a written arrangement with the other party, which must contain confidentiality provisions limiting the use of any information we share or receive. Arrangements with both the Dutch and the Irish data privacy commissioners were being finalized at the end of 2011.

Our Office has also played a leadership role in encouraging cooperation more generally.

At the 33rd International Conference of Data Protection and Privacy Commissioners, held in Mexico City in November 2011, commissioners passed a resolution on increasing international enforcement coordination. Our Office is one of the co-chairs of a working group that was created to develop a framework and processes for possible coordinated enforcement actions.

The working group will build on the success of the Global Privacy Enforcement Network (GPEN) and the Cross-border Privacy Enforcement Arrangement (CPEA) of Asia-Pacific Economic Cooperation (APEC), which we described in our 2010 Annual Report.

Our Office was one of the founding members of GPEN, which now has more than 20 members.

We are also a member of the CPEA, which is limited to enforcement authorities in the Asia-Pacific region and now has members from six APEC economies.

As well, our Office is a member of the Asia Pacific Privacy Authorities (APPA) forum, made up of privacy authorities in the Asia Pacific region. APPA holds two meetings annually where we exchange ideas and best practices about privacy regulation, new technologies and ways to raise awareness of privacy issues.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD)

The Organisation for Economic Co-operation and Development's *Guidelines on the Protection of Privacy and Transborder Data Flows* were developed more than 30 years ago. Although the guidelines have proven remarkably resilient, the world has changed dramatically since then.

Recognizing this, the OECD has launched a review of the guidelines to assess whether they are still relevant considering the "changing technologies, markets and user behaviour and the growing importance of digital identities." The review is being conducted by the OECD's Working Party on Information Security and Privacy (WPISP) and it is being advised and supported by a multi-stakeholder volunteer group chaired by Commissioner Stoddart.

The volunteer group will be expected to make preliminary recommendations to the WPISP. The range of possible recommendations is wide. The WPISP could conclude that the technology-neutral guidelines are still as relevant as ever or it could conclude that parts of the guidelines need to be updated or revised.

FRANCOPHONIE

Our Office was instrumental in the creation in 2007 of the organization representing francophone data protection authorities around the world, the *Association francophone des autorités de protection des données personnelles* (AFAPDP). We are committed to helping the AFAPDP provide increased support to developing countries in the Francophonie as they establish new legislative frameworks to protect the privacy rights of their citizens.

In 2011, Assistant Commissioner Chantal Bernier attended the association's first training seminar to take place on the African continent, in Dakar, Senegal. In her presentations, she discussed how privacy principles apply in various legal regimes and gave an overview of the historical importance of the OECD guidelines. In a second AFAPDP seminar before the International Conference of Data Protection and Privacy Commissioners in Mexico, she focused on the accountability principle and its practical application.

1.6 TECHNOLOGY LAB

Our technology lab and its small staff keep the OPC up-to-date with developing technologies and provide expert support for audits and investigations where technology is a major component. The technologies run the gamut from apps through smartphones to gaming consoles. Lab technologists can scrutinize such apps or devices to learn what personal information is being stored, what is being exchanged on the web and how it is being protected.

As an example of current privacy concerns, the lab has the ability to analyze the tracking techniques used by online behavioural advertisers and also the effectiveness of privacy controls on social networking sites.

Key Issue: Children and Youth Privacy



INTRODUCTION

In the battle to preserve the value of privacy in an online world, children and youth increasingly find themselves in the front lines.

Young Canadians are the most open to adopting new communications technologies which can, in some cases, invade their privacy. This holds true, not surprisingly, for those aged 18 to 34, as confirmed by a national opinion survey carried out this year for the OPC. (See section 3.3)

But the true adoption age for digital media is much, much younger.

We know, for example, that thousands of apps targeted at babies and toddlers are now available to teach little ones the alphabet and to entertain them with nursery rhymes.

The evidence may still be mostly anecdotal, but one recent study found that a third of North American Gen-Y moms (those aged 18 to 27) have let their children use a laptop by age two.

By the time the kids are three, those laptops and tablets are connected to the Internet daily for about a quarter of U.S. kids, according to the Joan Ganz Center in New York. By age five, the proportion online has soared to half.

We are giving our children unprecedented access to the Internet, but what are we doing to teach them about how to protect their privacy in the online environment?

We often hear the claim that young people growing up in this digital era do not care about privacy. This is not true.

While concepts of privacy are evolving, and young people tend to think about privacy differently than their parents, study after study shows that young people *do* care about their privacy.

What we hear when we go out to speak in schools, is that young people *want* to protect their online reputations, but many of them just don't know *how*. They ask us how to control who sees what is in their online profiles. They want to know how to block unwanted contact on social networking sites, and how to learn what others are posting about them.

There are a number of reasons why we see many younger Canadians running into privacy pitfalls online.

Part of the explanation is that they are such enthusiastic users of online technologies that they sometimes try new applications before all the privacy kinks have been identified and ironed out.

As well, young people tend to think that their online space is private and only their friends will see the content. They live in the moment and often don't think about how the messages they send or post today could turn up to haunt them years in the future.

Teenagers growing up in an online world are being watched and analyzed like no other previous generation.

Many online players are trying to capture the eyeballs and keystrokes of the young, with a view to commercializing their personal information. Below,

we relate the tale of a website which draws revenue from ads that target the 13-to-18-year-olds who make up one-third of its users.

Yet, while a lot of effort is going into exploiting the personal information of children and youth for profit, far fewer resources are being expended in helping children and youth recognize the value of privacy protection and develop the skills necessary to protect their personal information.

Children and youth face particular privacy perils because they lack the knowledge and experience to judge risk appropriately and mitigate it effectively.

As a result, our Office has substantially stepped up its efforts aimed at helping this vulnerable portion of Canadian society.

During the past year, we developed two new graphic-rich privacy packages for school and community use, a teen-oriented video and a tip sheet for parents. We continued a popular contest where teens produce short videos about privacy concerns. We continued to add resources to our youth website and blogs.

In addition, the OPC's Contributions Program has recently funded three innovative research and public education initiatives that explored the relationship between youth and privacy and promoted the protection of personal information among youth.

But a much greater effort is needed.

A five-nation study of digital literacy by the Media Awareness Network (MNet) for the OPC concluded that, in Canada, online privacy does not receive the attention it deserves within digital literacy. And existing educational efforts are also hampered by a lack of coordinated strategy.

MNet's nine specific recommendations, detailed in Chapter 2, include the idea of digital competencies for all Canadians, such as a knowledge of privacy rights and recourse mechanisms.

Here's an idea: Why not award badges to young people who master such digital competencies, much like Girl Guides and Boy Scouts win badges?

Innovative thinking like that would also help parents struggling to improve their own digital literacy skills, while simultaneously trying to impart a whole new set of life skills to their children.

Understandably, some parents want to use new technologies to make sure their children are safe. But this can lead to video surveillance and GPS tracking which include little or no consideration for the privacy rights of children and youth.

That matters because, first and foremost, kids learn about the concept of privacy from how they see privacy practised at home.

Our survey of relevant research suggests that if children are brought up in a surveillance environment where privacy is not valued, then they could in turn learn to not value privacy. These children may also fail

to learn how to establish their own privacy boundaries and be less likely to respect the boundaries of others.

Perhaps worse, constant surveillance can introduce the notion of distrust and dishonesty into family life, encouraging children to become secretive. If Mom might be watching the front door through an online video cam that's part of a home security system, then her daughter could be tempted to sneak her boyfriend in by the back door.

At first blush, such speculation may seem far-fetched, even alarmist.

But privacy guru danah boyd of New York University and Microsoft has pointed out that teens have already evolved defences against parental monitoring of semi-public fora like Facebook.

The teens hide their candid messages to their friends in plain sight, says boyd, by using language and cultural references which carry special meanings for their friends but seem innocuous to adults.

Boyd gives an example of a teenage girl despondent over a romantic breakup. To hide her true feelings from her mother, the girl posted to Facebook the lyrics from Monty Python's "Always Look on the Bright Side of Life." Her mother responded with a note that she seemed to be happy.

But her friends knew differently since the song features in a movie where the characters are about to be killed. They immediately got in touch to ask how the girl was coping.

2.1 INVESTIGATIONS RELATING TO CHILDREN AND YOUTH

NEXOPIA INVESTIGATION: WEBSITE AIMED AT YOUTH TACKLES SOME PRIVACY PROBLEMS BUT NOT ALL

Significant privacy flaws uncovered during the OPC's first investigation of a youth-oriented social networking site could serve as a lesson of what to avoid for websites that encourage the collection and publishing of personal information about youth.

The in-depth investigation of Nexopia identified several areas where the organization was in breach of PIPEDA and resulted in 24 recommendations. Many of the concerns could have been avoided if privacy issues had been more carefully considered when the website was developed.

Nexopia was open and cooperative during the investigation and the Commissioner was satisfied with the organization's response to 20 recommendations. However, four recommendations related to the indefinite retention of the personal information remained unresolved at the end of 2011.

BACKGROUND

Founded in 2003, Edmonton-based Nexopia predates many other popular social media websites. It claims more than 1.6 million registered users, with more than a third between the ages of 13 and 18.

Roughly half the users are from Alberta and British Columbia.

Nexopia considers itself an "open community" website differing from sites like Facebook. Although 90 percent of its users are also Facebook users, Nexopia argues that on Facebook "they communicate and share with their real life friends," while on Nexopia "they communicate with their online friends and 'show off' to the world."



Commissioner Stoddart commented: "The fact that the site is targeted at younger people strongly influenced our approach in this investigation.

Given that so many of Nexopia's users are young, extra care is needed to ensure that they understand the site's privacy practices."

"Other websites targeted at younger people also need to take note of this investigation and ensure they've adequately considered the privacy considerations particular to a youth context."

WHAT WE FOUND

Our investigation was prompted by a complaint by the Public Interest Advocacy Centre based in Ottawa. The key areas where Nexopia did not comply with PIPEDA included:

- default settings inappropriate for its target youth audience and a lack of clarity about available privacy settings;
- a lack of meaningful consent for the collection, use and disclosure of personal information collected at registration;
- the sharing of personal information with advertisers and other third parties without proper consent; and
- the indefinite retention of personal information.

ISSUES

1. Disclosure of user profiles to the public and default privacy settings

At the beginning of our investigation, Nexopia’s default privacy settings were “visible to all” – meaning visible to the whole Internet.

Given the special circumstances surrounding youth users and privacy, the OPC found that a reasonable person would not consider it appropriate for Nexopia to pre-select settings that push users towards disclosing their personal information, in some cases very sensitive personal information, for potentially everyone on the Internet to see.

The investigation also revealed that Nexopia does not adequately notify its users of default settings, or explain the difference between various settings.

Our Office found more could be done to inform users about the available privacy settings to ensure that users can make informed decisions about how they can control access to their personal information.

Nexopia users should be expected to opt-in to the “visible to all” setting – and with a full understanding of the implications of that choice.

Our Office found that more restrictive default settings, coupled with increased information for users in a format appropriate for a youth audience, would strike an appropriate balance between ensuring young people can enjoy the benefits of social networking, while protecting their privacy.

The OPC was satisfied that Nexopia’s proposed corrective measures, which include changing defaults and providing better information to users, will meet our recommendations.

2. Lack of meaningful consent for the collection, use and disclosure of personal information collected at registration

Our investigation found that Nexopia failed to adequately identify and inform users of its purposes for the collection, use and disclosure of the personal information it requires users to provide at registration.

For example, it was not clear which “core” profile information and profile pictures would be visible to users within the Nexopia community and anyone on the Internet, by default.

Nexopia acknowledged that the current version of its Privacy Policy was not necessarily written with the needs of youth in mind.

Nexopia was passively relying on users to read and agree to the terms of its lengthy and formal Privacy Policy as a means of obtaining consent. Our Office found that a mere link to the policy at the bottom of the registration page was not sufficient to obtain appropriate consent from the site’s target youth audience.

The OPC was pleased that Nexopia has agreed to update its Privacy Policy to add information and also use language appropriate to its user base. It will also require users to review its Privacy Policy as part of the registration process – although our Office has encouraged Nexopia to explore ways to present privacy information in more innovative ways.

3. Sharing of personal information with advertisers without proper consent

The information Nexopia provides to users about its advertising practices, particularly regarding the sharing of personal information with advertisers was incomplete. In some cases, they were sharing personal information without telling users clearly.

For example, Nexopia did not fully explain what targeted advertising is and how such advertising works. As well, its Privacy Policy did not explain that Nexopia allows third parties, such as advertising networks, to place cookies in the browsers of users

and visitors to its site in order to collect information about web usage.

The OPC was of the view that Nexopia’s own use of personal information for advertising purposes and its serving of behaviourally targeted advertisements to users *is* acceptable as a condition of service, provided individuals are made fully aware of how this practice works.

However, our Office was also of the opinion that individuals should be able to opt-out of being tracked by third parties – which are typically unknown to them.

Nexopia agreed to provide more information in its Privacy Policy and on its website about targeted advertising and the presence of third-party served advertising and tracking cookies. These changes were to include links to information about advertising and cookies on the site – and also about how cookies work and how they can be removed.

The OPC was satisfied with Nexopia’s response to our concerns.

4. Sharing of personal information with other third parties without proper consent

Nexopia regularly disclosed users’ unique user IDs to a payment processor when users make purchases on the site. As well, it disclosed a user’s age, gender and unique user ID to a rewards company each time a user participates in what the site calls “Earn Plus” offers.

The site did not explain to users the potential disclosure of their personal information to the rewards company, nor that such disclosures may be provided over and above any information the user provides directly to the rewards company as a condition of a particular “Earn Plus” offer. Nexopia admitted that their online statements and actual disclosure practices had become misleading.

Nexopia asserted that the information provided to the payment processor and the rewards company could not be used to identify and obtain more information about individual users. However, our testing revealed that a user’s unique ID can be used to link to the user’s profile and potentially permit access to all the personal information displayed there.

In our view, Nexopia could use another unique code or identifying number that limits the amount of personal information that passes between the parties and yet still allows efficient billing and payment processing.

Nexopia agreed to stop providing unique user IDs to the payment processor and has made the decision to completely remove the “Earn Plus” service from the site, and, therefore, will stop sharing users’ personal information with the rewards company.

The OPC was satisfied with Nexopia’s response.

5. Retention of personal information

Nexopia collected non-users’ email addresses through invitations to join the site initiated by users. Users

were *not* required to confirm to Nexopia that they had their friend’s consent for the purposes of sending an invitation to join the website, prior to providing the friend’s email address to the company.

A non-user who didn’t want to receive further invitations could click on a link to a page entitled “Opt out of Nexopia.com invites”.

However, the non-user was not informed on this page that their email address would be retained by Nexopia. For the unsubscribe feature to be effective, Nexopia said it must retain for an indefinite period a list of email addresses to which no further messages would be sent.

In our view, it was important for the user who provides the email address in the first place to ensure that they have obtained prior consent from the email address owner, their friend, for the invitation email to be issued by Nexopia.

As well, our Office recommended that Nexopia offer non-users a clear choice between a) unsubscribing from join-the-site invitation emails, or b) permanent deletion of their email address.

The OPC was satisfied with Nexopia’s response to our concerns about this issue.

Nexopia agreed to add text to its “Find and Add Friends” feature to emphasize that users should have non-users’ permission to give the website their email addresses.

The organization also agreed that, in the future, non-users who receive invitation emails will be able to request the permanent deletion of their email address from Nexopia's database.

Our Office also considered the issue of deletion of accounts.

When users clicked on an option called "Delete Account" they were advised: *This will delete your account, including your profile, your pictures, friends list, messages, etc. Your forum posts, comments and messages in other users' inboxes will remain.*

In fact, Nexopia advised us that the only information deleted is the user's "shouts".

Other information was *stored indefinitely*. (For example, username; user ID; email address; IP address and log-in information; friends list; gallery pictures; profile contents; messages and comments; and profile photos.)

Another concern related to account deactivation and the freezing of accounts, either by Nexopia or upon request by a user. The personal information contained in frozen user accounts remained inactive on Nexopia's servers indefinitely and was not subject to any periodic review.

Nexopia admitted it had not deleted account information since 2004, either from "deleted" or frozen accounts.

It was clearly misleading to provide a "Delete Account" option. The OPC recommended that

Nexopia provide a true delete option for the accounts and personal information of users.

Unfortunately, Nexopia said it would not implement this recommendation because the cost of doing so would be prohibitively high. It also argued that the information stored in the archives was only accessible to system administrators and recovered in the event that they received a warrant from a law enforcement authority.

The OPC understood the technical challenges presented in permanently deleting users' personal information. However, Nexopia's practice of storing indefinitely all of an individual's personal information was in contravention of PIPEDA.

It's clear that law enforcement authorities sometimes require access to information. Such requests or warrants may justify a longer retention period in specific cases, but they do not justify wholesale and indefinite retention of *all* records just in case there may be a request at some point in time.

Nexopia's practice of storing personal information in its archives indefinitely, on the small possibility it may be the subject of a warrant from a law enforcement agency, was therefore not acceptable.

Moreover, there are security risks inherent in retaining vast amounts of former users' personal information, long after it has served its original purpose. As well, our Office is concerned that Nexopia's users are being misled into thinking they

can delete their personal information at some point, if they want to.

This issue remained unresolved at the end of our investigation. The OPC is proceeding to address these unresolved issues in accordance with our authorities under PIPEDA, which include the option of going to Federal Court to seek to have the recommendations enforced.

The full investigation report is available on our website.

DAYCARE CENTRE MODIFIED WEBCAM MONITORING TO INCREASE PRIVACY PROTECTION

BACKGROUND

The complainant enrolled his son at a private daycare centre and was told that parents could pay a fee for its webcam service to let them see their child's daycare room in real time. Parents viewed the webcam feed via the Internet after entering a unique password.

The daycare centre stated that it had instituted the webcam service for two reasons: first, so it could monitor the daycare environment for security purposes; and, second, to provide parents with assurances regarding the daycare environment.

The centre told the OPC that approximately 60 percent of the parents of registered children had enrolled in the webcam service.

The complainant subsequently learned that the webcam feed was being recorded. He notified the

daycare centre that he objected to the recording and that he felt appropriate privacy safeguards were not in place.

Following notification of the investigation, the centre deleted its saved video files and modified its systems to no longer record the video stream captured by its webcam. The centre also implemented a privacy policy requiring all parents to sign a form consenting to the webcam monitoring, regardless of whether a parent wished to enrol in the service.

The daycare centre acknowledged that a parent would be able to record and send out the webcam feed as viewed on a personal computer. Upon our Office's suggestion, the centre required parents using the webcam service to sign a contract agreeing to not record the webcam feed and promising to keep the assigned password confidential.

WHAT WE FOUND

At issue was whether the daycare centre collected the complainant's son's personal information without consent and failed to adequately safeguard his son's personal information.

Initially, the OPC was of the view that the daycare centre was not in compliance with PIPEDA Principles 4.7 (security) and 4.3 (consent) and subsection 5(3) (appropriate purposes) and recommended the centre cease the webcam monitoring program.

During the investigation, however, the centre improved its organizational and technological

security measures by ceasing to record the video stream, implementing a privacy policy and enhancing password protection features. Nonetheless, our Office recommended that the daycare centre further enhance its technological security measures and implement additional contractual terms in order to prevent inappropriate use of the information collected by the webcam.

Consultation with the Ministry of Children and Youth Services in Ontario at the time revealed that of the 4,784 licensed child care programs operating

in Ontario, only 61 offered live video streaming – and several daycares without webcam monitoring operated close to the complainant’s home. Because individuals appear to have alternative child care options, there was no evidence that parental consent was not voluntary.

CONCLUSION

The daycare centre indicated that it implemented all of our Office’s recommendations and we concluded that the complaint was resolved.

2.2 SURVEILLANCE OF CHILDREN



After the OPC dealt with the above complaint, our Office determined it would be helpful to explore related issues further and conducted research about the effects of surveillance on children.

We conducted a literature review to identify and analyze research which addressed the effects that current surveillance practices have on children, including video surveillance, online monitoring and the use of biometrics.

We focused on surveillance in Canada and in societies similar to ours. Despite the paucity of pertinent research, there was consensus among the work that does exist that constant surveillance in the long term affects how children view and interact with the world.

All of the research noted the prevalence of surveillance in children’s lives today. There are parents using video baby monitors and “nanny cams,” and later Internet and cell phone monitoring software and GPS. Schools have security cameras, RFID tracking, and palm scanners. Corporations track kids online for marketing purposes.

Surveillance has become the new norm for several reasons. Parents are frightened by over-blown stories of “stranger danger” (which statistics do not support), and surveillance is affordable, available and easy to use.

As well, they see that the state uses surveillance to detect and deter anti-social behaviour, while business uses online surveillance for commercial profit.

According to the available research, indiscriminate surveillance on children without proper boundaries and explanations may potentially affect:

- **Autonomy and social development**
Without the freedom to experiment with making critical and ethical choices, children could instead make decisions based on fear and risk of punishment. They could become less likely to learn to regulate and direct their own behaviour.
- **Trust, fear and learning to assess risk**
Surveillance could create an artificial, risk-free

environment where children might not be given opportunities to develop self confidence and risk management skills.

- **Digital literacy**
Monitoring software could hamper children's development of digital literacy skills needed to navigate the online world effectively.
- **Understanding privacy**
If children are brought up in a surveillance environment where privacy is not valued, they in turn may not value privacy. These children may also not learn how to establish their own privacy boundaries and could be less likely to respect the boundaries of others.

2.3 YOUTH OUTREACH INITIATIVES

We have successfully launched two youth presentation packages intended to be used with students in Grades 7-8 and Grades 9-12¹.

The goal is to show young people how technology can affect their privacy, and how they can build secure online identities while keeping their personal information safe.



Resources for
parents and teachers

Each package includes a set of vibrant PowerPoint slides with accompanying speaking notes to assist teachers or other adults in providing effective and engaging presentations in schools or the community. Presentations take about 30 minutes, but extra time for group discussion is encouraged.

Presenters are invited to provide feedback to the OPC so the package can be continually improved.

We have also developed a four-and-a-half-minute video, *What Can YOU Do to Protect Your Online Rep*, which



What Can YOU Do
to Protect Your
Online Rep - Video

¹ Secondary I to II and III to V in Quebec.

speaks to teens directly and covers the key privacy concepts that young people need to consider when sharing information online. The video – launched in January 2012 – can be viewed online or downloaded for discussing privacy issues with teens.

The Office also developed a tip sheet geared to parents who want to talk to their kids about privacy in the online world. The tips urge parents to try out the online spaces their kids are using, keep up with the technology, emphasize the importance of password protection and tell their kids to “think before they click.”



Our third annual *my privacy & me* national video contest again proved popular, with more than 100 entries. The winning videos were submitted by students from across Canada.



Students aged 12 to 18 enter by producing video public service announcements from one to two minutes long on timely privacy issues.

A fourth contest was launched in September, with winning entries expected to be announced in March 2012.

Further details on all these initiatives can be found on our special youth website, www.youthprivacy.ca.

2.4 DIGITAL LITERACY

Digital literacy includes the abilities to use, understand and create with computers and the Internet. Unlike Australia and the U.K., Canada does not have a national strategy for digital literacy.

The development of digital literacy skills was included in the federal government’s Digital Economy Strategy Consultation process in May 2010, but it has not received attention in the follow-up.

To better understand the state of play, we contracted the Media Awareness Network (MNet) to identify

leading digital literacy initiatives in Canada and abroad; evaluate their privacy component; and identify opportunities within digital literacy initiatives for our Office to raise the online privacy awareness and skills of Canadians.

MNet found that although the importance of digital literacy is recognized in Canada, online privacy as a specific topic within digital literacy does not receive the attention it deserves and existing efforts are hampered by a lack of coordinated strategy.

In its paper, MNet compared Canadian digital literacy programs with efforts from the U.K., the U.S., Australia and Brazil. It found the following trends:


- Youth are a prime target for digital literacy interventions, including privacy skills. Although adults are also vulnerable to privacy risks, they are made a lower priority for digital literacy skills development.
- Current digital literacy interventions do not anticipate future risks but rather scramble to keep up with the present.
- Outside of broadly defined groups such as youth, adults and seniors, existing programs display little sensitivity to other factors which may affect digital literacy, such as immigrant status or gender.
- Despite the possibility of delivering digital literacy education exclusively online, all the countries studied prefer face-to-face instruction, especially for seniors.
- Promote these privacy competencies as an entitlement for Canadians.
- Integrate issues of data protection and democracy in educational modules.
- Focus more on adults.
- Support continuing digital literacy education for all elementary and secondary students.
- Prepare privacy resources which can be adapted to many audiences.
- Support Community Access Program sites as venues for privacy education.
- Promote and support existing, high-quality resources.
- Promote a national focus on digital literacy.


Based on its review, MNet made the following recommendations:


- Define privacy competencies that Canadians need to manage their personal information online. The suggested competencies range from awareness that personal information is increasingly treated as a commodity to a knowledge of privacy rights and recourse mechanisms.

2.5 CONTRIBUTIONS PROGRAM - PROJECTS FOR YOUTH

Over the past few years, the OPC's Contributions Program has funded innovative research and public education initiatives that explored the relationship between youth and privacy and promoted the protection of personal information among youth. For instance:

 The Media Awareness Network was awarded funding in 2011-12 for its project *Young Canadians in a Wired World - Phase III*. This project is one of the most comprehensive and wide-ranging studies of Internet use by children and teens in Canada. *Phase III* of the project covers completion of qualitative research previously undertaken by MNet using parent and youth focus groups in Calgary, Toronto and Montreal, writing of the qualitative research final report, and developing and implementing a communications strategy.

 Also in 2011-12, Atmosphere Industries was awarded funding for its project *Gaming Privacy: Creating a Privacy Game with Canadian Children*. This project proposes to work with Canadian children to create, deploy and research a cross-media game that engages children ages eight and up in the development of privacy literacy skills. Cross-media games mix physical with digital spaces and technologies to create unique experiences that get people working together in public spaces to solve puzzles and accomplish game goals.

 In 2009-10, OPC funded a project carried out by the University of Guelph, titled *Privacy and Disclosure on Facebook: Youth & Adults' Information Disclosure and Perceptions of Privacy Risks*. It aimed to advance the understanding of information sharing on Facebook by high school students and working adults through a literature review and a survey of 600 Canadians. The research focused on factors that motivated disclosure of information and the use of privacy settings as well as examining Facebook users' perception of privacy risks and knowledge of privacy settings. The final report includes recommendations to help the OPC develop strategies for making the public aware of the privacy risks of social networking sites and the need to make more informed decisions about information sharing.

The OPC looks forward to the results of this research being applied and put to good use by interested end-users focusing on the identification and privacy needs of youth as they navigate the modern challenges of the online world.

privacy

Privacy

Privacy

CHAPTER 3

The Privacy Landscape

AN OVERVIEW OF SOME OF THE OTHER MAJOR ISSUES ADDRESSED BY
THE OFFICE OF THE PRIVACY COMMISSIONER OF CANADA DURING THE YEAR

The privacy landscape in 2011 featured both gradual evolutions and abrupt shifts, akin to the steady creep of the Earth's crust punctuated with rare tectonic upheavals.

Once again, the principle-based structure of PIPEDA proved flexible and forceful enough to deal with the bulk of these privacy challenges. Yet the legislation itself is also evolving and further legislative changes may be needed to respond to emerging privacy challenges that differ in scope or nature from anything encountered in the 10-year life of the legislation.

During the year, the Commissioner suggested that the prospect of large penalties appeared necessary to convince companies to get serious about preventing data breaches. She also released an open letter calling on the federal government to justify its proposed "lawful access" legislation which had "serious repercussions for privacy rights."

Canadians appear to recognize these emerging challenges. A public opinion poll commissioned by

our Office found significantly more privacy concerns about new communications technologies than just two years ago.

Four in 10 of the 2,000 randomly polled Canadians said that computers and the Internet pose a risk to their privacy, up from one-quarter in a 2009 survey. Privacy concern also rose over online social networking sites, cell phones and online financial services.

As demonstrated by summaries of some of our investigations in this chapter, such concerns are often well founded.

In the field of financial privacy, for example, we found PIPEDA violations by an insurance company, a credit bureau, a car manufacturer and a credit union.

New concerns also surfaced regarding social networking giant Facebook, which has been featured in past reports. And we continue to monitor Google's implementation of privacy improvements which we recommended after the company's inappropriate collection of personal information.

To keep pace with the rapidly evolving privacy landscape, our Office issued guidance documents about biometrics and online behavioural advertising – two developments spawned by new technology. We also strengthened our technological expertise, partly to support OPC’s role in Canada’s new anti-spam legislation, which is expected to go into effect this year.

All these developments are detailed on the following pages, which examine some of the major issues we addressed during 2011.

3.1 FINANCIAL PRIVACY



Most people guard the details of their finances as zealously as they guard their PINs at the sales register or ATM. A nightmare shared by everyone would be learning that some crook is running amok with your credit card.

Because of such sensitivity and the huge number of transactions with Canadians, the financial sector has regularly accounted for the largest proportion of formal complaints accepted by the OPC. In 2012, it also gave rise to several noteworthy investigations, which are summarized here.

INVESTIGATIONS

CREDIT BUREAU PURGES LOAN HISTORY FROM INDIVIDUAL’S CREDIT REPORT WITHOUT HIS KNOWLEDGE

BACKGROUND

An individual financed the purchase of a used vehicle through a third-party financing company. In financing the purchase of his vehicle, the complainant sought a lender that reported to a national credit bureau. He did so in the belief that a positive repayment history might help augment his overall credit standing.

The complainant began repaying his car loan in July 2004. By June 2008, the complainant’s loan was paid in full.

In 2008, following the repayment of his car loan, the complainant sought to take advantage of a provincial program which provided grants to qualified applicants towards the purchase of a home. The complainant appeared to have obtained a mortgage

pre-approval from a mortgage broker conditional upon qualification for the grant.

According to the complainant, after receiving notice of acceptance for the grant, he returned to the mortgage broker with whom he had been conditionally pre-approved, only to be advised that he no longer qualified for the loan.

Although the reasons supporting the complainant's denial of credit could not be determined with certainty – lenders and financial institutions having a right to their own criteria for loan approval – the mortgage broker in question informed our Office that credit information relating to the complainant's car loan with the financier was not listed on the complainant's credit history.

It was the mortgage broker's belief that the absence of the car loan history may have harmed the complainant's credit score. In the broker's view, the complainant's loan with the financier, which showed a generally positive repayment history, might have helped in part to re-establish the complainant's credit rating. It was his understanding that the complainant's credit score had dropped significantly from the time when the complainant had been pre-approved for a mortgage, to the time when the complainant had qualified for the grant.

WHAT WE FOUND

While we were unable to estimate how much the complainant's credit score may have been altered by the loss of car loan information, our investigation corroborated the fact that car loan information

related to the financier, once listed on the complainant's credit report, was later missing.

Investigation revealed that the financier had previously been reporting the complainant's payment history to a credit bureau on a monthly basis. But some time before settlement of the complainant's loan, the financier ceased reporting to that credit bureau.

According to the credit bureau, it was the company's policy to stop reporting any information from a data source with which it did not have an ongoing relationship (i.e., "a severed data source") approximately 60 days after its relationship with a data source ended. This policy effectively purged all information associated with a severed data source – whether positive or negative – leaving no trace of that particular credit history on an individual's file. The credit bureau asserts this policy was necessary to ensure that information provided in its credit reports remained accurate, complete and up-to-date.

Our investigation focused primarily on the credit bureau's obligations to ensure the accuracy and completeness of the complainant's credit file. We also considered matters relating to openness. To this end, we closely reviewed the credit bureau's policies and practices surrounding severed data sources, taking into account the company's obligations under provincial credit reporting and consumer protection acts.

Despite our initial misgivings about the deletion of the complainant's credit history, over the course

of our investigation the credit bureau produced sufficient evidence to demonstrate how reporting information from a severed data source might adversely affect the integrity of its credit reports. Although the effects in this case of the purging of loan information from the complainant's credit report were such that it rendered his credit history incomplete, we could envision just as many other scenarios in which *not* purging information from a severed data source might have led to an equally inaccurate or incomplete credit picture.

Without continuity in the reporting relationship with a data source, the credit bureau was unable to ensure that the information in its credit reports was recent, reliable and up-to-date. Not only would the credit bureau have been unable to report on subsequent changes to an individual's credit report, the company would also have been unable to verify and investigate inaccuracies in data reporting.

Despite the above, we were still concerned that credit information was entirely purged from the complainant's credit file, without his knowledge. In this case, not only was the complainant completely unaware that his personal information was to be deleted, but third parties who might have relied on the company's credit reports for lending appeared to have been similarly unaware of the company's policies and practices.

At the time of our investigation, the credit bureau did not publicly disclose its 60-day retention policy for information from severed data sources. The company's data retention policy stated only that: "A

credit transaction will automatically purge from the system six years from the date of last activity."

Had the complainant been aware of the credit bureau's 60-day policy, he may have been in a better position to monitor his file and to consider placing a narrative on his credit report. He might also have thought to take action to obtain information directly from the severed data source in a timely manner in order to supplement his credit record.

CONCLUSION

As PIPEDA requires that an organization make readily available to individuals specific information about its policies and practices relating to the management of personal information, and so far as the credit bureau failed to be open with the complainant about its policy on severed data sources, we found the complaint to be well founded. The credit bureau agreed to implement our Office's recommendations to address this issue.

BANK PROPERLY REDACTED INFORMATION RELATED TO CREDIT CARD FRAUD PROBE

The complainant alleged that a bank denied her access to her personal information relating to the bank's investigation into the alleged fraudulent use of her credit card.

The respondent bank had informed the complainant that her credit card would be cancelled because of potential fraudulent use of the card. After more than six months dealing with the customer care centre and ombudsman's office of the bank, the complainant

made an access request to the bank's privacy officer asking for all documents pertaining to the fraudulent use of her credit card and the ensuing cancellation. She specifically requested the name of the merchant where the alleged fraud occurred.

The bank provided five pages of documents about the credit card account but blacked out the names of some individuals and some of the computer commands used at the bank. Dissatisfied with this information, the individual filed an access complaint under PIPEDA against the bank.

Our Office found that the respondent bank properly redacted the personal information of other individuals, the computer system commands used during the investigation, and the information generated by the investigation into the alleged fraud.

We also found that the information redacted could be described as confidential commercial information. We agree that if the information redacted were to be released, the commercial interests of the respondent would suffer irreparable harm. The disclosure would be a breach of the respondent's contractual obligations of confidentiality and, further, it could put at risk merchants with which the bank had contractual confidentiality obligations.

Our Office concluded that the complaint was not well founded.

CREDIT UNION SHOULD HAVE OBTAINED CONSENT FOR CREDIT CHECK ON SPOUSE

An individual complained that a credit union had collected his personal information during what he alleged was a misleading credit application process. He also alleged that his personal information was kept without consent and that the credit union refused to destroy that information. Finally, he complained that the organization had conducted a credit check on his spouse without consent and had improperly used and disclosed the information acquired.

Our Office found that the respondent did make it clear to the complainant what personal information was required for the application process. We also took in consideration the legal obligation cited by the credit union to retain the complainant's personal information.

However, the investigation raised concerns about the collection of information about the complainant's spouse. Although the complainant's spouse was named on the application form, she had not provided consent for a credit check.

Our Office recommended that the credit union revise its processes to ensure that consent is obtained from each customer applying for credit before obtaining a joint credit bureau report. The credit union confirmed that it had reinforced the procedure manual to make obtaining consent from both consumers a mandatory requirement before a joint credit bureau report is obtained.

Our Office concluded the complaints relating to both collection and consent with regard to the complainant's personal information were not well founded.

Regarding the retention issue, we were satisfied that the legal obligation cited by the credit union for the retention of the complainant's personal information for a period of seven years was reasonable. Accordingly, we concluded that the complaint was not well founded.

The complaints relating to consent to the collection of his spouse's personal information and the use and disclosure of her information were well founded and resolved.

TASK FORCE FOR THE PAYMENTS SYSTEM REVIEW

The modern payments system extends all the way from cash purchases at a convenience store to multi-million dollar transfers between businesses. It includes all the institutions, instruments and services that support the transfer of value between parties, including money, financial instruments, and even the exchange of information.

That landscape is being dramatically altered by advances in the digital economy, which have facilitated an online marketplace where payments are being made in new and innovative ways.

In June 2010, the Minister of Finance announced the launch of the Task Force for the Payments System

Review. In the summer of 2011, the Task Force asked for submissions related to the transformation of the Canadian payments system. Our Office made a submission on privacy and security issues which we considered relevant for the Task Force, for stakeholders in the payments system environment, and for individuals.

Since payments often involve very sensitive information such as details of personal finances, the OPC submission stressed that the payments industry needs to be aware of the challenges of defining personal information in the digital age, challenges associated with new technologies, and the potential to re-identify individuals. We urged a diligent effort to implement the strongest measures of privacy protection throughout the payments system process.

We were encouraged that the Task Force has acknowledged privacy as a guiding principle associated with the transformation of the payments system and also has incorporated privacy into its governance framework. Keeping this issue in mind, we recommended that all references to privacy in the payments system not only recognize this principle, but also that the payments system be designed to meet privacy obligations required by statute.

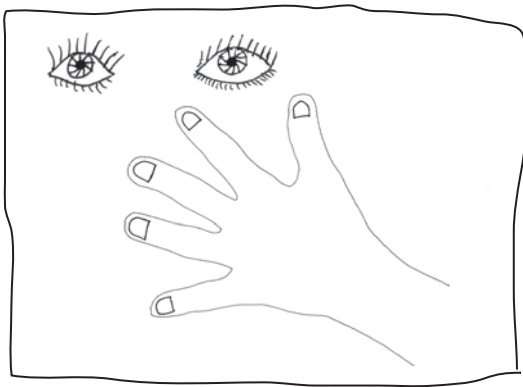
The OPC recognizes that innovation in the payments system helps encourage economic growth. New and dynamic business practices and technologies are introduced to enhance business and consumer experiences. Yet these business and technological innovations increasingly collect, use and disclose vast amounts of consumer personal information at the

point of payment, making it essential to fully address privacy and security issues.

To support innovation and build a strong digital economy, consumers must adopt the new practices and technologies. That adoption depends on consumer trust. Meeting obligations related to

information and privacy rights serves as a catalyst to build such trust and, as a result, encourages economic participation.

3.2 BIOMETRICS



There is something new under the privacy sun – the emerging field of biometrics. A word unfamiliar to many just five years ago is increasingly becoming part of daily life, as machines scan irises, faces, fingertips, palms and even the way people walk to confirm or authenticate identities.

With this new technology come new privacy concerns, which is why the OPC produced a biometrics guidance document this year. As well, an investigation recounted below demonstrates how biometrics and privacy can intersect in practice.

INVESTIGATION

TEST-TAKER OBJECTS TO PALM-VEIN SCANNING

BACKGROUND

A woman objected to having her palm scanned before writing a test in 2009 and to this information being disclosed to an American organization.

The owner and administrator of the test is a U.S.-based organization. Personal information is collected and used in Canada for the test by Canadian staff at Canadian test centres, where more than 8,000 tests were delivered in 2008.

The test administrator authenticates test-takers with palm-vein scanning technology by identifying the vein patterns beneath the skin of the individual's hand and then retaining the pattern in an encrypted numerical (binary) template (a “numerical key”). The test administrator uses this technology to detect fraud and/or impersonation during tests.

The process cannot be reversed. No actual biometric data is retained in a record that could be deciphered. Forging a vein-pattern identity would be very difficult since veins are inside the body and have many detectable and differentiating features. The test administrator maintained that mere visual identification and verification against ID cards are not fully reliable since fraudsters will go to considerable lengths to physically resemble and impersonate others.

Every time test-takers leave or return to the examination room, only their palm-vein template is used to re-authenticate them. As well, the individual's palm-vein template is matched against any others the test administrator has collected at past exams and locations, even if they had been collected under different names.

WHAT WE FOUND

Our Office determined that a reasonable person would consider appropriate the test administrator's use of palm-vein scanning for purposes of identifying individuals and ensuring the integrity of the test. We also found it acceptable that the test administrator collects and uses digital photos alongside the palm-vein scan template since, in a few past cases, the photo has protected certain candidates from the repercussions of a false-positive match of their palm-vein scan.

The test administrator stated two main reasons for collecting personal information from test-takers, including biometric data: 1) to verify the identity of the candidate taking the test; 2) to ensure that

the test scores sent to schools accurately reflect the students' abilities.

We arrived at our finding after studying three factors: risk of fraud, the degree of privacy sensitivity of the test administrator's current palm-vein scanning technology, and security standards for the storage and treatment of palm-vein templates.

FRAUD

The test administrator demonstrated that attempted illegal activity and fraud has occurred at test sessions.

The test administrator provided evidence of professional test-takers and reported that, in 2003-2004, five individuals located in Montreal and New York were found to have taken the test on behalf of 185 individuals from the U.S. The fraudsters were eventually prosecuted, convicted and imprisoned in a U.S. federal penitentiary. One of the individuals convicted publically claimed to have written the test more than 300 times. As a result, many of the schools which used the exam as part of their admission process asked the test administrator to take a far more rigorous approach to exam security.

The test administrator asserted that biometric technology is effective as a deterrent. For example, after introducing its biometrics program, attempted test fraud decreased substantially. And, in two cases, individuals fled a test centre - before a palm-vein scan could be taken - after they were questioned about a mismatch between the photographs and signatures collected under the same names at a previous exam session.

As for preventing instances of impersonation, the test administrator reported that the company's first forays into palm-vein scanning detected a person who had taken the test five times using five different identities. It also identified 23 people who had hired the same imposter to take the test on their behalf. In both cases, the imposters had used counterfeit government-issued ID.

A Canadian test-taker tried to register at a test centre in 2009 to write the exam for the fourth time but was refused because the individual's palm template did not match that from the previous exam sitting. The individual has never contacted the test administrator since.

PRIVACY SENSITIVE

In light of the test administrator's recent history with authentication methods and the various alternatives that it has adopted over the years, its current use of palm-vein scanning does not appear to be overly privacy invasive. The test administrator began looking for an alternative to its digital fingerprint identification system in 2006, after concerns were voiced about fingerprinting, by students, data-protection authorities and some test centre personnel.

Our Office sees all biometrics as privacy invasive to a certain extent because they involve the collection of an individual's physical characteristics. But not all biometrics are highly privacy invasive in and of themselves. In our view, the binary representation of a candidate's palm-vein scan, given the test administrator's current use of the technology, is not overly sensitive personal information.

For example, we note that the palm-vein scans are immediately transformed into an encrypted binary template, the binary code is non-reversible and no raw biometric image is retained. As well, the binary code information retained from the scan cannot easily be interpreted by other parties or applied to other purposes, and the binary template is stored separately from any other personal information about the test taker. Palm-vein scanning is also considered a "non-trace" biometric, since latent images cannot be left on objects, including the system used for the scan.

DATA STORAGE SECURITY STANDARDS AND RETENTION

With respect to personal information transmission, retention and storage, we did not find that the test administrator was in contravention of its obligations under the Act.

After a site visit to a test centre, we were satisfied that biometric, identification and test information is encrypted for transmission and storage, and that data access is restricted. The encryption algorithm that the test administrator's third-party contractor uses is a recognized encryption standard with good security levels for sensitive data. Further, the data is protected by numerous high-level safeguards at the data storage centre. Security policies were found to be documented and written agreements for data protection procedures exist between the test administrator and the third-party contractor. The accountability called for in PIPEDA Principle 4.1.3 was thus upheld.

The complainant also expressed concern about her personal information being transmitted to, as well as retained and stored in, the U.S. In this regard, we noted that in the test administrator's *Information Bulletin*, the reader is clearly advised that their information will be transmitted to the United States. We thus deemed the test administrator's actions to be concurrent with PIPEDA Principle 4.8 ("openness").

In 2009, this Office issued its *Guidelines for Transferring Personal Information Across Borders*, which distilled key findings from investigations over the years. One such finding is: "PIPEDA does not prohibit organizations in Canada from transferring personal information to an organization in another jurisdiction for processing."

We also deemed reasonable the test administrator's set retention period of five years for biometric data and test scores collected, and noted the existence of an automated, scheduled clean-up process of this data after the five years. Thus, the need to limit use, disclosure and retention described in PIPEDA Principle 4.5 was respected.

CONSENT

When we retraced the steps necessary to register for the test, we found that individuals were adequately informed that their personal information will be collected and that they were notified of the purposes for the collection.

Ninety-five percent of registrations for the test are online, which requires checking a box to agree to specific terms and conditions, as well as to the

privacy policy (all web links provided). On the site, test-takers are specifically referred to the test administrator's *Information Bulletin*, a key online document (also available by mail) that explains the identification requirements to be met on the test day and the reasons for those requirements.

The *Bulletin* provides test policies and procedures, and also the privacy policy, where more information can be found. It informs individuals of the specific types of personal information to be collected, retained and transmitted to the U.S., data encryption, and the test administrator's designated uses of this information. It also forewarns test-takers that, on the day of their exam and upon signing the rules and agreement document, they will be providing their consent to palm-vein scanning for fraud-detection purposes. Also on its website, the test administrator posts other detailed information about its use of test-day biometrics and also links to FAQs specifically about the test administrator's use of palm-vein recognition. The website clearly advises that providing a palm-vein scan to the test administrator is mandatory for all exam-takers.

CONCLUSION

Our Office concluded that the complaint was not well founded.

Note: Please see Chapter 6 (In the Courts) for another case involving the use of biometrics.

BIOMETRICS GUIDANCE DOCUMENT

Your face, your fingertips, your irises, the way you walk: All of these “biometric characteristics” can be used by machines in various ways to automatically recognize individuals and confirm or authenticate their identities.

Noting the growing interest among organizations and companies in adopting biometric systems, the OPC prepared detailed guidance that explains the technologies and their impact on privacy.

The guidance document, called *Data at Your Fingertips: Biometrics and the Challenges to Privacy*, explores the benefits and drawbacks of biometrics. On one hand, the technology can contribute to highly reliable and robust identification systems — more reliable, for instance, than paper-based systems. On the other hand, there can also be significant privacy challenges, such as:

- covert collection and use of biometric data, with iris-based systems able to surreptitiously gather images of people’s eyes from two metres away or fingerprints gathered from latent prints left when people touch surfaces;

- cross-matching, where a biometric trait collected for one purpose is used for a different purpose without a person’s knowledge and consent;
- the unwanted disclosure of secondary information embedded in DNA or other biometric information about an individual.

Canada does not have a policy on the use of biometrics either by the government or by the private sector. However, the guidance document stresses that many of the approaches already used to strengthen privacy protections in other fields should also be applied to initiatives that use biometrics.

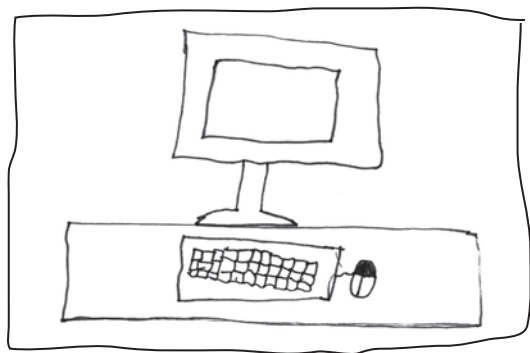
These include taking privacy considerations into account from the start and also applying a Privacy Impact Assessment. As well, our Office encourages organizations to apply a well-established four-part test, which is detailed in the guidance document.

These considerations are now being used when evaluating specific cases where biometric systems are deployed in the private sector.



Data at Your
Fingertips: Biometrics
and the Challenges
to Privacy

3.3 ONLINE PRIVACY



Canadians are the heaviest users of the Internet on the planet, spending about 45 hours on average online every month. We are also among the world's most enthusiastic online social networkers. Roughly one in two Canadians are on Facebook.

Not surprisingly, given these statistics, online privacy is a continuing concern for the Canadian public and for the OPC. This year, we published fact sheets focusing on the privacy implications of cloud computing, cookies and online behavioural advertising. We also investigated complaints about new features introduced by Facebook, which are detailed below.

INVESTIGATIONS

FACEBOOK DEMONSTRATES BETTER BUT NOT YET BEST PRIVACY PRACTICES

Over the course of 2011, we investigated a number of privacy complaints against Facebook. While the

nature of complaints varied in seriousness and in scope, most stemmed from the introduction of new features to its social networking platform. Two of our most recent investigations of this company related to complaints about:

- A “Friend Suggestion” feature, which is designed to entice non-users to join the social networking site by giving these invitees a list of “friends” and photos of existing users; and
- Social plug-ins, which allow a user to obtain personalized content on third-party sites.

We were satisfied with the end results of our investigations in these cases.

On balance, Facebook appears to be giving more consideration to privacy than when we first began investigating it. Yet the company could still do a better job of considering the privacy impacts of new features before their public introduction.

Notwithstanding general improvements to the company's privacy practices (and its platform's detailed privacy settings), we were disappointed that the company hadn't anticipated the widespread privacy concerns that followed the launch of its Friend Suggestion feature. In our view, privacy should have been built in at the front end of that feature – not added after the fact in response to negative reactions from individual users and data protection authorities.

FRIEND SUGGESTIONS

Three individuals filed complaints with our Office after receiving emails inviting them to join the social networking site. The invitations included so-called Friend Suggestions – a list of users which, in most cases, were people the complainants knew. Lacking any explanation about how the company had generated these suggestions, the complainants were concerned that the company may have inappropriately accessed their electronic address books.

The investigation did not find any evidence to suggest that the company was accessing the complainants' personal address books or those of their suggested friends. Friend Suggestions were instead generated by a complex algorithm which matched common sets of data uploaded by users.

At the time the complaints were filed, the invitations from the social networking site provided very little information about how the company's Friend Suggestion feature worked. During our investigation, however, the company agreed to make changes. In particular, the company removed all Friend Suggestions from its initial invitation and only provided these in subsequent reminders, allowing a non-user to either learn more about the service or to opt out of receiving Friend Suggestions and any further messages from the company.

SOCIAL PLUG-INS

In the case of the social plug-ins, the company introduced a feature that would allow its users to see content drawn from their user profiles on third-party websites. Buttons such as "Like" and "Recommend" appeared on third-party websites and allowed the site users to suggest and recommend content to other site friends. For example, a logged-in site member visiting a news website using the company's social plug-ins would be able to see a list of the articles recommended by his or her friends.

The complainant in this case was concerned about the potential exchange of information between the company and the two-million-plus websites which host the company's social plug-ins.

While the investigation confirmed that the company was not sharing personal information with third-party websites through the social plug-ins, how that feature operated was unclear to many Canadians. Once again, we felt that the company could have done a better job of educating the public and its users on the operation of the new feature, and of ensuring that sufficient privacy protections were being built into new product designs.

IDENTITY VERIFICATION

A further complaint raised the issue of whether Facebook collected more personal information from the complainant than necessary as a condition for obtaining services. It also questioned whether the company had provided the complainant with the opportunity to raise a challenge to the organization's compliance with PIPEDA with the designated

individual(s) accountable for the organization's compliance.

The complainant created a personal social networking site account in September 2010. She alleged that she was able to use her account for a few days, but was then required to provide her mobile phone number to confirm her identity to be able to access her account again.

Since she did not have a mobile phone number, the complainant stated that she was unable to confirm her identity.

The complainant also alleged that Facebook did not allow her to address a challenge concerning compliance with the principles of PIPEDA to the designated individual(s) accountable for the organization's compliance. The complainant stated that she sent several emails to the company's customer services and to other services regarding the verification of her identity, but only received automated messages from the company directing her to use the company's Help button.

Facebook informed our Office that it used mobile phone numbers as part of its account verification process when an account is flagged due to suspicious botnet or spam-related activity. The company stated that the complainant's account was flagged.

The company stated that verification by mobile phone was only one option for verification of an account. The user could also confirm the names of their site friends by identifying those tagged

in photographs posted on the company's social networking site. As well, the user could verify his/her account by providing his/her full name on the account, date of birth, login email address and uploading a government-issued ID and ensuring that his/her full name, date of birth and photos were clear. Facebook noted that it encourages users to sever (i.e. mask) any personal information on the government-issued ID that is not needed to verify their identity. The company stated that it provided the complainant with the option of using an alternative method to verify her account, but did not identify which alternative was presented.

With regard to the complaint about challenging compliance, the company submitted that it had various contact forms for privacy questions and comments. For example, the company's Privacy Policy noted that an individual can submit a privacy complaint against the company via TRUSTe's Watchdog Dispute Resolution Process.

Our Office found Facebook clearly informed its users of the purpose of the collection, namely that the collection of personal information is a security measure used to ensure that the user is a real person with one account. Further, the Office found that the company offered its users a choice of authentication, with each option corresponding to a different level of privacy invasiveness. In this context, our Office did not find that asking users to upload government-issued ID for authentication purposes (with personal information other than the name, date of birth and photo masked) violated PIPEDA.

On the issue of challenging compliance, the Office found that Facebook provided a web form at the start of its Privacy Policy that allowed users to complain to the company regarding a privacy issue. As such, the Office found that the company had privacy complaint procedures in place that were accessible and easy to use.

The Office concluded that the allegations were not well founded.

GOOGLE REQUIRED TO ADDRESS PRIVACY DEFICIENCIES

In June 2011, our Office announced results of our follow-up work stemming from an investigation into Google Inc's collection of highly sensitive data from unsecured wireless networks.

We reported that Google had committed to implement remedial measures that will reduce the risk of future privacy violations but that Commissioner Stoddart had also taken the unprecedented step of requesting the company undergo an independent, third-party audit of its privacy programs within a year and share the results with her Office.

The incident involved Google Street View cars inappropriately collecting personal information such as emails, usernames, passwords, phone numbers and addresses during 13 months tracing roadways across Canada. Thousands of Canadians were likely affected.

In a preliminary report published in October 2010, we noted that Google had advised our Office that the incident stemmed from an engineer's initiative and Google's lack of controls over processes to ensure that necessary privacy protections were followed.

We concluded that the collection was a serious violation of the privacy rights of Canadians and unlawful because it did not follow core principles of PIPEDA – user knowledge and consent to the collection of personal information. Details of that investigation were published in our 2010 Annual Report and are available on the OPC website.

The remedial measures that Google agreed to implement included:

- significantly augmenting privacy and security training provided to all employees;
- implementing a system for tracking all projects that collect, use or store personal information and for holding the engineers and managers responsible for those projects accountable for privacy;
- requiring engineering project leaders to draft, maintain, submit and update Privacy Design Documents for all projects to help ensure that engineering and product teams assess the privacy impact of their products and services from inception through launch;

- assigning an internal audit team to conduct periodic audits to verify the completion of selected Privacy Design Documents and their review by the appropriate managers; and
- piloting a review process under which members of Google's Privacy Engineering, Product Counsel and Privacy Counsel teams review proposals involving location-based data, as well as the software programs used for the collection of data.

Google also undertook to delete the data collected in Canada. This process has been complicated by various rules and regulations to which the company is subject under Canadian and U.S. laws. The company stated that, until such time as the data can be destroyed, it will remain secured and will not be used.

We will follow up with Google in 2012 to gauge the full implementation of our recommendations.

Our Office was one of several international data protection authorities that investigated the Google WiFi debacle. The French data protection authority imposed a fine of 100,000 Euros (more than \$140,000 Canadian at the time) against Google.

CANADA'S ANTI-SPAM LEGISLATION

Canada now has anti-spam legislation, although it is not yet in force.

Canada's anti-spam legislation, or CASL for short, is intended to deter unwanted electronic

communications by regulating the sending of commercial electronic messages (CEMs), including emails and text messages. With limited exceptions, senders of CEMs will need to obtain consent from the recipient before sending the message, include information that identifies the sender; and provide a means for the recipient to withdraw consent.

The legislation is also designed to curb other harmful practices such as electronic address harvesting and installing malware (malicious software) on computers.

When the law comes into force, our Office will share the responsibility for enforcing it with the Canadian Radio-television and Telecommunications Commission (CRTC) and the Competition Bureau.

The CRTC will be responsible for investigations regarding the sending of unsolicited commercial electronic messages, the unauthorized alteration of transmission data and the installation of software without consent.

The Competition Bureau will address false or misleading representations and deceptive marketing practices in the electronic marketplace.

We will focus on the unauthorized collection of personal information, specifically:

- electronic address harvesting, including the compiling of email lists through the use of computer programs to automatically mine the Internet for addresses; and

- the collection of personal information through access to computer systems contrary to an Act of Parliament.

The Act allows our Office to share information and cooperate with the CRTC and the Competition Bureau to ensure the effective enforcement of the legislation. During 2011, we worked closely with these two organizations and with Industry Canada to prepare for the implementation of the legislation by – among other activities – producing communications tools to raise public awareness and developing procedures to work together.

The new Act is expected to come into force in 2012.

CONSUMER PRIVACY CONSULTATIONS

In May 2011, the OPC released its final *Report on the 2010 Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing*. These consultations were intended to inform and frame our policy and research work in addressing emerging issues. Following up on the report's commitment to action, we launched new efforts in 2011 to promote privacy literacy to all Canadians, Canadian business and Canadian technology developers.



Report on the 2010 Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing



Cookies - Following the Crumbs



Cloud Computing



Every Move You Make... Advertisers are tracking your online behaviour

We published fact sheets on cookies, cloud computing as well as online behavioural advertising. Aimed primarily at the public, these fact sheets provide general information. We also updated our Interpretation Bulletin on the definition of personal information.

In December 2011, we published a guidance document on online behavioural advertising (OBA), which is the online, third-party tracking of individuals across web sites over time to target advertisements based on the inferred interests of those individuals. This document outlines how the parties involved in – or benefitting from – OBA can ensure that their practices are fair, transparent and comply with PIPEDA.

A great deal of activity and discussion about consent and transparency has been under way in this area among data protection authorities in the U.S. and Europe, advertisers, and the technical

community (web browser developers). We took the opportunity to weigh into the discussion and provide a framework, grounded in PIPEDA, for these practices.

ONLINE BEHAVIOURAL ADVERTISING GUIDANCE

In our Privacy and Online Behavioural Advertising (OBA) Guidelines, we take the position that the information involved in OBA will generally be considered personal information. We view the purposes for OBA as reasonable in the circumstances, but we think that OBA should not be considered a condition of service to access the Internet. We note that individuals need to be properly informed of the practice and must provide consent. That consent can be implied, providing that:

- Individuals are made aware of the purposes for the practice in a manner that is clear and understandable – the purposes must be made obvious and cannot be buried in a privacy policy. Organizations should be transparent about their practices and consider how to effectively inform individuals of their online behavioural advertising practices, by using a variety of communication methods, such as online banners, layered approaches, and interactive tools;



- Individuals are informed of these purposes at or before the time of collection and provided with information about the various parties involved in online behavioural advertising;
- Individuals are able to easily opt out of the practice – ideally at or before the time the information is collected;
- The opt-out takes effect immediately and is persistent;
- The information collected and used is limited, to the extent practicable, to non-sensitive information (avoiding sensitive information such as medical or health information); and
- Information collected and used is destroyed as soon as possible or effectively de-identified.

The guidelines also singled out a couple of practices that we feel are problematic.

Certain types of technology have recently been used for OBA (for example, “zombie” cookies) that individuals cannot delete or prevent from tracking their web browsing. The guidelines are clear that if individuals cannot decline the tracking and targeting because there is no viable way for them to exert control over the technology used, or if doing so renders the service unusable, then organizations should not be employing that type of technology for OBA purposes.

The guidelines also note that, given the difficulty of ensuring meaningful consent from children to OBA practices, organizations should avoid tracking children and tracking on websites aimed at children.

PRIVACY POLL

Privacy concerns about a range of new communications technologies have risen sharply among Canadians over the past two years, according to a public opinion survey commissioned by our Office.

Yet many people using these new technologies are still not taking even rudimentary steps to protect their privacy, the same survey reported.

The telephone survey of 2,000 randomly selected adults found that four in 10 said that computers and the Internet pose a risk to their privacy, up from one-quarter (26 percent) in a similar survey just two years ago.

Another 15 percent specifically mentioned online social networking sites – something barely on the radar in 2009 (two percent). As well, privacy concerns about cell phones and other telecommunications nearly quadrupled (from three percent to 11 percent) and unease also increased concerning credit/debit cards and banking/online banking.

Surveying in late February and early March, Harris/Decima found that three-quarters (74 percent) of respondents said they owned at least one mobile

communications device, such as a cell phone, smartphone or tablet.

However, only four in 10 used password locks for the devices, or adjusted their settings to limit the sharing of personal information that may be stored on the devices.

The 2011 Canadians and Privacy Survey also found that one-third of Canadians use public WiFi sites, such as those located at coffee shops and airports, where online communication may not always be protected by encryption. Of those, fully 85 percent admitted to some concern about possible risks to the security of their personal information.

An overwhelming majority favour tough sanctions against organizations that fail to properly protect the privacy of individuals. More than eight in 10 respondents wanted to see measures such as publicly naming offending organizations, fining them, or taking legal action against them.

While younger Canadians aged 18 to 34 are the most enthusiastic users of the new technology, the survey showed they are also the most likely to use available mechanisms to protect their privacy, suggesting that, while young people are eager to embrace new technology, they also care about privacy and are willing to take steps to protect it.



The complete survey is available on our website at www.priv.gc.ca.

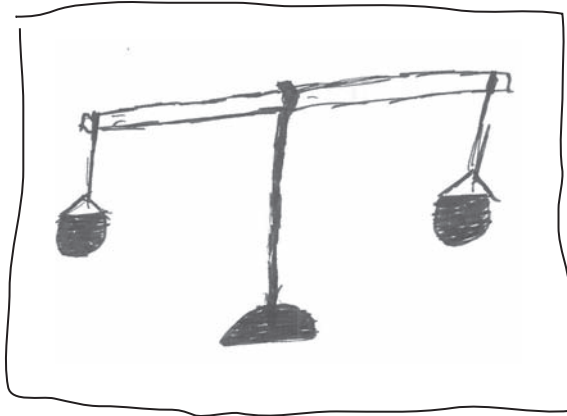
TECHNOLOGY LAB

Defending online privacy can sometimes be a high-tech task and that's where the OPC's technology lab comes to the fore. The lab keeps our Office up-to-date with developing technologies and provides expert support for audits and investigations where technology is a major component.

The lab's controlled environment allows technologists to check what personal information is being stored on a wide range of devices or applications and how it is protected.

For example, the lab can analyze the tracking techniques used by online behavioural advertisers and also the effectiveness of privacy controls on social networking sites.

3.4 MODERNIZATION OF PRIVACY LAWS



IMPLEMENTING AMENDMENTS TO PIPEDA

In April 2011, amendments to PIPEDA came into effect which gave the Commissioner enhanced discretion regarding the conduct of investigations and the sharing of information with provincial and international counterparts.

The Commissioner can now decline to investigate complaints and discontinue investigations in certain defined circumstances, such as where the complaint could be more appropriately dealt with through procedures under other laws or where the complaint was not filed within a reasonable period of time. These amendments will help concentrate resources on complaints that raise serious privacy issues or problems of a systemic nature and also help balance service to all Canadians with the concerns of individual complainants.

Under these new discretionary powers, the Commissioner in 2011 decided to discontinue two complaint investigations and declined to begin an investigation of a third. In all three cases we decided the matters were more appropriately dealt with through procedures under other laws.

With respect to information sharing, the amendments allow the Commissioner to enter into arrangements with both provincial and international counterparts to share information, including information otherwise confidential under PIPEDA, subject to certain safeguards.

At the provincial level, our Office has long worked with the provincial privacy commissioners to ensure a harmonized and coordinated approach to the application of private sector privacy laws. The enhanced ability to share information will allow the OPC to work even more closely with the provincial commissioners.

In this regard, in November, we entered into a revised Memorandum of Understanding with the Commissioners in British Columbia and Alberta that provides for cooperation and collaboration in private sector privacy policy, enforcement, and public education. As part of this collaboration, we review the cases being investigated by provincial colleagues to identify any common issues.

Internationally, the ability to cooperate with foreign counterparts is becoming a necessity considering increasing transborder data flows and privacy breaches with impacts in multiple jurisdictions. Our Office initiated discussions about information sharing and cooperation arrangements with several foreign data protection authorities and was nearing agreement with the Dutch and Irish as the year ended.

REDUCING THE RISK OF DATA BREACHES

In the fall of 2011, the federal government reintroduced legislative amendments that would make it mandatory to report certain breaches to our Office and to the affected individuals.

Under Bill C-12, organizations would be required to report any material breach of security safeguards to our Office. They would assess whether the breach is “material” by considering factors such as the sensitivity of the information involved, the number of individuals affected and the systemic nature of the breach.

Organizations would also be required to notify individuals “where it is reasonable to consider in the circumstances that there exists a real risk of significant harm to affected individuals,” depending on the sensitivity of the information and the probability of it being misused.

While a mandatory reporting scheme would give us a clearer picture of how many breaches are occurring, why they are occurring, and what steps should be undertaken to reduce the risk of future incidents, we believe the data breach reporting provisions contained in Bill C-12 have become out of date.

It is noteworthy that the proposed changes before Parliament at the end of 2011 stem from recommendations that were made back in 2006 and which still have not been implemented.

Much has changed as the years have passed. Data breach reporting provisions contained in the proposed legislation were a good first step for promoting accountability and transparency, but more is clearly needed now.

In recent years, we have seen very serious, large-scale data breaches. Data breach notification, in itself, may not be sufficient to create the kind of incentives necessary to ensure that organizations take security issues more seriously in the current environment.

Many other countries are taking a harder line on breaches. For example, the United States has been a leader in this area and virtually all states have data breach laws. Meanwhile, a European Commission Regulation proposed in early 2012 included data breach provisions and very significant fining powers for European data protection authorities.

Commissioner Stoddart has encouraged the federal government to explore strengthened enforcement options that would create stronger incentives for organizations to ensure personal information is adequately protected.

PIPEDA REVIEW

PIPEDA, which was designed to be a principle-based and technologically neutral legislation, became law in 2001 and requires a Parliamentary review every five years.

The first review began in 2006. Bill C-12, which proposes amendments to PIPEDA resulting from that first review, was introduced in the House of Commons in September 2011. It replaced the earlier Bill C-29, which died on the Order Paper following the dissolution of Parliament on March 26, 2011.

Parliament had not issued a formal call for a second review by the end of 2011. Nonetheless, we are currently examining how the law and current practices should evolve to best serve Canadians in the face of modern privacy challenges.

The next review will be an opportunity to examine whether PIPEDA remains sufficiently flexible and effective in responding to privacy challenges created by rapidly evolving technology.

Our position on whether and how PIPEDA needs to evolve to address these new and emerging challenges will be informed by our reflections on three key themes: 1) appropriate enforcement mechanisms and incentives to ensure compliance with the Act; 2) gateway concepts, such as “personal information” and “commercial activity,” which directly influence the scope of application of PIPEDA; and 3) innovative approaches for organizations to assume and demonstrate accountability for their personal information management practices.

Meeting the Concerns of Canadians

Responding to questions and complaints constitutes the bread-and-butter work of our Office. This is where we have direct contact with Canadians, either by answering questions about privacy issues or by addressing and investigating complaints about problems encountered when dealing with organizations.

This year, the Office has continued refining our processes for handling questions and complaints to better serve Canadians.

4.1 INFORMATION REQUESTS

Our revamped Information Centre fielded 5,236 information requests about private-sector privacy issues in 2011, a slight increase over 2010. The bulk of the requests (4,518) were made by phone, as in previous years.

Social networking sites accounted for the largest single category of calls, with our tracking system showing surges whenever the media reported on controversies related to Facebook and Google. Particular concerns to callers included the possible disclosure of personal information without consent, the adequacy of privacy settings, the collection of personal identifiers when reinstating an account, as well as the misuse of personal information already posted online.

New technologies to monitor the workplace were also a recurring theme, as employees voiced concern about their own personal information being collected at work, without the ability to opt out.

Calls also increased whenever there was a well-publicized data breach, such as that involving Sony PlayStation Network accounts. Callers didn't necessarily inquire about the specific breach but often asked about the security of personal information in general.

Our Office continued to receive calls almost daily regarding concerns about the collection of personal information such as the Social Insurance Number,

date of birth and bank account information for the purposes of a rental agreement, to obtain a credit report or to return a product at a retail outlet. This collection of personal information raises concerns about the subsequent safeguarding and retention practices of the various organizations.

Other concerns raised by callers included what they characterized as over-collection of medical information by insurance companies, the accuracy of the personal information held by banks and credit reporting agencies and difficulties in accessing information held by telecommunications companies to ensure accuracy.

4.2 INTAKE

In 2011, as part of our work to improve our front-end service, we created a dedicated Intake Unit.

All written complaints about privacy matters are forwarded to this Unit. The Intake Unit reviews the complaint, and, if necessary, quickly follows up with the complainant to clarify our understanding of the complaint and to gather any additional information or documents necessary to begin an investigation.

If the complainant has not already raised his or her concerns with the person responsible for privacy within the relevant organization, an officer in the Intake Unit will ask the complainant to try to resolve the issue with the organization directly, and come back to us if that is unsuccessful.

In addition, as is often the case when people call our Information Officers, our Intake team is sometimes able to satisfactorily address the issue immediately, eliminating the need for our Office to accept the matter as a formal complaint.

For instance, if previous investigation has shown that the activities being complained about are actually compliant with PIPEDA, an Intake Officer would explain this to the individual.

Or, if we have previously determined that we don't have jurisdiction over the organization or type of activity, an Officer will explain and try to direct the individual to other resources or assistance.

4.3 COMPLAINTS RECEIVED

Overall in 2011, our Office accepted 281 formal complaints under PIPEDA, a 35 percent increase from 207 in 2010. This increase could be linked to a variety of factors, such as an increasing complexity of issues that Canadians raise (leading to more becoming formal

complaints), possible heightened awareness among Canadians of their privacy rights, or changes in how all of us interact with businesses in the increasingly digital economy.

4.4 COMPLAINTS BY INDUSTRY SECTOR

Complaints related to the financial sector continued to account for the largest proportion of formal complaints we accepted, roughly one in five.

Our experience is that financial institutions have among the best-developed privacy policies and practices, although we continue to identify some areas of concern through our investigations. The explanation for the consistent high placement appears to lie in the size of the financial sector and the huge number of transactions conducted with individual Canadians.

Complaints in the transportation sector jumped this year compared to previous years, doubling historical

norms to become the second largest sector. Just over half of these complaints related to access issues. It isn't clear why we have seen this increase, which has been noted across all transportation sub sectors. We intend to observe this potential trend closely over the next year for possible implications.

Meanwhile, complaints in the insurance sector (previously one of the top three sectors) have declined over the last two years.

This could be because in the last couple of years we have seen an increase in clarity and awareness of privacy rules in the insurance sector.

Major Sectors Targeted in Complaints

Sector	2011	2010	2009
Financial	22%	22%	24%
Transportation	12%	6%	6%
Telecommunications	11%	9%	18%*
Services	10%	17%	4%
Insurance	9%	13%	18%

*Prior to 2010, Telecommunications included Internet complaints, which are now a separate category.

Note: Statistics and definitions for all industry sectors can be found in Appendix 2.

4.5 TYPES OF COMPLAINTS RECEIVED

The use and disclosure of personal information, access to personal information, and collection of personal information were once again the top three issues raised in complaints to our Office.

In addition, we noticed that the proportion of complaints about corrections to, or notations on,

personal information rose significantly this year to five percent of all formal complaints accepted (compared to one percent or less in previous years). This could be linked to increased awareness by Canadians of how their personal information is collected and used and awareness of their rights to see and correct these records.

Top 3 Types of Complaints Received in the last 3 years

Type of complaint	2011	2010	2009
Use and disclosure: Complaints involving allegations that personal information was inappropriately used or disclosed, without consent, for purposes other than those for which it was collected.	32%	27%	26%
Access: Complaints about difficulties gaining access to personal information.	26%	24%	28%
Collection: Complaints involving the unnecessary collection of personal information or personal information collected unfairly or unlawfully, such as without proper consent.	20%	16%	14%

4.6 EARLY RESOLUTION

We have an early resolution process with designated Early Resolution Officers. This allows us to better serve Canadians by addressing complaints quickly, with a less formal approach than our official complaint investigation process.

When we receive a written complaint where there is a high likelihood that the issue could be resolved quickly, the Intake Unit refers the case to an Early Resolution Officer.

The Early Resolution Officer works with both the complainant and the respondent organization to resolve a complaint.

The early resolution process has been very successful. In some cases, an issue that would have taken months to resolve through the official complaint investigation process is now concluded in days. We have received very positive feedback on the early resolution process from both complainants and organizations.

EARLY RESOLUTION COMPLAINTS

In 2011, we completed 125 early resolution cases. As illustrated in the detailed statistics in Appendix 2, we were able to reach a satisfactory conclusion in 116 of these cases. The remaining nine cases were transferred for formal investigation.

To continue to improve the timeliness and effectiveness of our service to Canadians, we have significantly increased the number of complaints handled through this process – almost half of formal complaints, up from about a quarter in 2010.

Despite this increase in volume, we are still maintaining last year's improvements in timeliness of resolution of these complaints. In 2011, complaints resolved through early resolution were completed in an average of two months from complaint acceptance, compared with 14 months for full investigations.

In addition, we are also maintaining an extremely high rate of successful resolution – more than 90 percent.

The early resolution process will continue to be an important tool for quickly and effectively addressing concerns that Canadians bring to our Office.

We are also encouraging all investigators to use early resolution approaches where they see an opportunity to do so. For instance, the first success story in the following section is a case assigned to an investigator. In the early stages of the investigation, the investigator realized there was an opportunity to use early resolution approaches, and quickly resolved the complaint.

Of course, not all complaints are good candidates for early resolution. Complaints that raise complex, new or potentially systemic issues will continue to be addressed through our formal investigation process.

PIPEDA Early Resolution Activity in 2011

Total number of early resolution interventions completed	Number transferred for further investigation	Number successfully resolved
125	9	116

Note: Further statistics on the sector, type, and dispositions for successful early resolution interventions can be found in Appendix 2.

EARLY RESOLUTION SUCCESS STORIES

CONCERN OVER SAFEGUARDS ON CLIENT PASSWORDS

After registering for a company's loyalty membership program online, the complainant received a confirmation email containing his secure password. At the request of one of our investigators, the company looked into the practice of sending the password in the confirmation email. It decided that this was not necessary, and took steps to discontinue the practice. Company officials apologized to the complainant and thanked him for bringing it to their attention. The company's quick and effective response satisfied our Office and the complainant.

COMPLAINANT'S EX-BOYFRIEND USED CREDIT REPORT TO FIND HER

While checking her credit report, an individual noticed a credit inquiry on her by a retailer who employed her former boyfriend, from whom she had fled. The individual contacted our Office because she was concerned that her ex-boyfriend had used the information in her credit report to locate her.

An Early Resolution Officer contacted the retailer, who confirmed that an employee had broken company policies. The retailer took disciplinary action and also restricted access to the credit check system to senior management. The company apologized to the complainant.

The individual was satisfied with the response by the retailer, but was still concerned that a credit check could be used again to locate her. An Early Resolution Officer contacted the Privacy Officer of the credit reporting agency, who agreed to work with the individual to prevent this incident from reoccurring.

DRIVER'S LICENCE INFORMATION UNNECESSARILY COLLECTED

While purchasing tickets for a go-kart rental, an individual was asked to provide his driver's licence. When the individual questioned the request, the owner explained that his date of birth and driver's licence number was recorded for marketing purposes and that they would not honour the tickets if this information wasn't provided. An Early Resolution Officer contacted the owner of the company and provided him with our Office's publications about the use of driver's licences and a past decision regarding this issue.

The owner and his staff reviewed the material and became aware of the sensitivity of the information they were recording. This small business immediately took key steps to meet its privacy obligations: a) modifying its data collection software, b) creating and providing training for staff on a new privacy policy, and c) posting its collection policy for customers in a public area. The owner appreciated the information we provided, and the complainant was satisfied with the steps taken to address his complaint.

DIFFICULTY ACCESSING PERSONAL INFORMATION

An individual complained to this Office that a telecommunications company had failed to respond to his request to access his personal information. The Early Resolution Officer contacted the telecommunications company to find out why the individual's request had not been fulfilled. The company investigated and determined that two departments within the organization were aware of the request, but neither responded, thinking that the other department had already done so. The company immediately responded to the request after determining what happened and implemented changes to ensure this would not be repeated. The complainant received the document he requested and was satisfied with the response of the company.

REMOVAL OF PERSONAL INFORMATION FROM A UK-BASED WEBSITE

An individual contacted us to complain that a social networking website based out of the U.K. had failed to respond to his repeated requests to have his profile deleted, and he was still receiving messages from the website.

The Early Resolution Officer contacted the website's U.K. head office. The company's privacy official reviewed the company's policies and procedures for deleting a profile and could not offer an explanation as to why the complainant's profile had not been deleted. However, the company immediately responded to our telephone request to remove the complainant's profile and ensure that the action was permanent. The complainant was satisfied with the company's actions.

4.7 COMPLAINT INVESTIGATIONS

In 2011, we completed 120 complaint investigations. These formal investigations were done in cases where complaints raised complex, new or potentially systemic issues.

The number of investigations concluded is significantly lower than in 2010, when we completed 249 investigations, as part of our two-year effort to clear a backlog of complaints.

In 2011, with the backlog effectively eliminated and with an increased use of early resolution, we were

able to return to our 2008 staffing levels and still improve the timeliness of our investigations.

The average formal complaint investigation time dropped to 14 months – down several months from previous years. When combined with early resolution complaints, these improvements have led to a significant reduction in average complaint treatment time for accepted complaints.

The overall average is now down to slightly more than eight months.

We are also pleased that, in a majority of investigations, we were able to find a satisfactory conclusion to issues. Only 11 percent of investigations resulted in complaints being deemed well founded (but not resolved), meaning we were not able to reach a conclusion that we found acceptable. (See below for more details.)

In 2011, we saw a jump in the number of investigations where we concluded that PIPEDA did not apply to the organization or activity that was the subject of the complaint – up to 15 percent from three percent the previous year.

This jump is in part due to a 2010 Federal Court decision on the scope of application of PIPEDA where personal information is collected for the purpose of defending an insured individual against a tort claim arising from a motor vehicle accident. This led to a few complaints being closed because they had been received before this jurisdictional decision yet concerned activities over which the Court ruled PIPEDA does not apply.

We also saw a significant decrease in the proportion of cases deemed either resolved, or well founded and resolved. These dropped by two-thirds, from 33 percent of all cases in 2010 to just 11 percent in 2011.

This decrease was almost exactly offset by the increase in the proportion of cases settled through early resolution, which nearly doubled from 24 percent in 2010 to 49 percent in 2011.

These two shifts demonstrate how cases that were previously resolved through the more time-consuming investigation process are now being settled more rapidly through the early resolution process. It dramatically illustrates the efficiency gains achieved for all Canadians through the early resolution approach.

4.8 SNAPSHOT OF 2011 INVESTIGATIONS

Number of investigations completed	Number deemed well-founded (and unresolved)	Number satisfactorily concluded
120	13	107

Note: Further statistics on the sector, type, and dispositions for completed investigations can be found in Appendix 2.

INVESTIGATION SUMMARIES

The following is a look at some of the investigations completed during 2011. Additional details about some of the cases are available on our website.

We have named the organizations that are the subject of complaints only where the Commissioner has determined that it is in the public interest to do so.

Investigations dealing with cases relating to young Canadians are included in Chapter 2, our special feature section on children and youth privacy. Cases dealing with financial privacy, biometrics, and online privacy can be found in Chapter 3, on the privacy landscape in 2011.

This section highlights some of the risks to personal information we have identified in the course of our investigations.

RISK: NOT PROPERLY DISCLOSING PURPOSE OF COLLECTING PERSONAL INFORMATION

JOB SEEKER NOT ADEQUATELY INFORMED ABOUT PURPOSE OF PERSONAL INFORMATION COLLECTION

The complainant was contacted via email by an industry associate of a Toronto-based company operating under the name of “Job Success”. Having obtained a copy of the complainant’s resume from an online job search site, and with a view to ostensibly offering job search and career management services, the associate informed the complainant he could be invited to attend an “interview”.

When the company called to arrange a meeting, the complainant asked for more details, particularly whether it was about a specific job. The staff member organizing the meeting responded that she did not have that information available but that further details would be provided in person.

Having accepted the company’s invitation to meet, the complainant visited the respondent’s office and was introduced to a senior director. Following personal introductions, the senior director began asking the complainant where he was from and where he went to school. He also asked the complainant to elaborate on the professional experiences noted in his resume and to provide information on his career aspirations.

Nearing the end of the meeting, which lasted approximately 45 minutes, the senior director turned to the company’s “selection process” and the purported advantages of working with Job Success (namely, assistance in marketing oneself to prospective employers, obtaining quality interviews, and learning how to conduct oneself in interviews).

Up until this point in the meeting, the complainant was of the impression that the company was conducting a job interview. In this regard, the complainant maintained that he was misled as to the purposes for which his personal information had been collected.

Our investigation focused on the obligation of Job Success to identify the purposes for which personal information was to be collected at or before the

time of collection. Under PIPEDA, an organization must document the purposes for which personal information is collected, and specify those purposes to the individual to whom the information belongs.

At the time our investigation was initiated, details of the company's information management practices were difficult to find. Initially, the company's website did not have a privacy policy and the purposes for which it was collecting personal information was nowhere to be found.

Not only was the company's website short on information, Job Success also failed to specify the purposes for which it was collecting personal information prior to its meeting with the complainant.

Over the course of our investigation, we asked the respondent about the lack of information it made publicly available about the company's services. The company responded that its website was "not informative on purpose" so as to generate curiosity about the company's affairs, thus encouraging individuals to "come in and sit down."

In our view, Job Success failed to clearly identify the purposes for which individuals' personal information was being collected at or before the time of collection.

Furthermore, in so much as the company did not make sufficient efforts to ensure that the complainant was advised of the purposes for which his information was to be used, in a manner that

he could reasonably understand, it failed to obtain the meaningful consent of the complainant for the collection and use of his personal information.

In the course of our investigation, Job Success agreed to take corrective action within 90 days of the issuance of our final report. We found the complaint to be well founded and conditionally resolved.

RISK: USING SENSITIVE PERSONAL INFORMATION FOR THE PURPOSE OF AUTHENTICATION

CABLE AND COMMUNICATIONS COMPANIES USE SENSITIVE PERSONAL INFORMATION FOR AUTHENTICATION

During the year, we investigated a number of complaints against cable and communications companies trying to collect sensitive personal information from individuals for the purposes of online or telephone authentication.

Almost all of these complaints involved individuals who were looking to open new service accounts, or seeking information and/or assistance in relation to existing accounts.

In most cases, individuals registering for new services (by telephone or online), were asked to provide one of several pieces of personal information for identification purposes. The pieces of information typically collected included the Social Insurance Number (SIN), provincial driver's licence number, or Canadian passport number. Individuals were also

asked for standard tombstone information, including dates of birth.

Our Office has previously held that the collection of sensitive information may be justifiable when an organization needs to ensure the creditworthiness of a new customer. Reducing the credit risks assumed by organizations in accepting new customers – whose only interaction with the service provider is often online or by telephone – is, in our view, a legitimate business purpose. As invariably stated by the communications industry, the use of personal information to ensure an appropriate and accurate credit match can, at times, help minimize credit exposure.

We also note in the cases we investigated that, although the collection of the SIN, driver's licence or passport number was an acknowledged condition of the supply of service, it was not an absolute condition. During our investigations, we noted that respondents, as a matter of policy, allowed their customers alternatives to the collection of personal information for the purpose of a credit check. Customers who did not require credit could opt to provide companies with a valid credit card number or a cash deposit as payment security.

Notwithstanding the above, while it may be reasonable for a company to request sensitive personal information *for the purpose of facilitating a credit check*, that same information collected with a view to customer authentication (often following the creation of a service account) may be unnecessary. In the cases we examined, complainants repeatedly

expressed concern over industry practices which require a customer to self-authenticate using potentially sensitive personal information.

In our view, the collection of a SIN, driver's licence or passport number for purposes of authentication may, in some circumstances, be a violation of PIPEDA. Not only are such pieces of personal information unnecessary in the provision of cellular, cable or Internet services, most companies providing such services have demonstrated the ability to authenticate their customers (following a credit check and the creation of an account) without such collection.

In the cases we investigated, respondent organizations demonstrated the ability to authenticate their existing customers in a more privacy sensitive manner. In most cases, companies did so by way of a customer created personal identification number (PIN) or pass-code.

Of course, the provision of the SIN, driver's licence or passport number by an individual for authentication purposes may remain optional. Indeed, we recognize industry concerns that individuals often forget pass-codes, and that a requirement to use a pass-code as a default for authentication can lead to unwanted frustration on behalf of customers.

But the ability to provide other identification or less sensitive personal information instead should be disclosed to potential customers upfront and be clearly posted in a company's privacy policy.

Where provided, sensitive personal information must at all times be appropriately safeguarded by an organization.

RISK: FAILURE TO DISCLOSE SURVEILLANCE VIDEO

PERSONAL INFORMATION COLLECTED IN COMPANY'S LEGAL DEFENCE FALLS UNDER PIPEDA

The complainant claimed she was injured after stepping in a puddle of water in a Sobeys store in November 2008. She discussed the incident with the store manager and subsequently retained a lawyer.

In a letter to Sobeys, the lawyer requested various records including any surveillance tapes of the incident. He indicated that his client said the store's roof had been leaking. The customer submitted a further request to Sobeys for access to her personal information, citing PIPEDA.

In her later complaint to our Office, the customer claimed that she was unaware that her personal information was being collected in a videotaped record of the incident. She said that, when she initially reported her fall, the manager had neglected to disclose the existence of the videotape.

Her complaint alleged that Sobeys had collected, used and disclosed her personal information without her knowledge and consent. It also alleged that the store had improperly withheld personal information to which she was entitled under PIPEDA.

PIPEDA requires the knowledge and consent of individuals for the collection of their personal information. Our 2009 *Guidelines on Overt Video Surveillance in the Private Sector* are also clear that the public must be informed of such surveillance.

However, Sobeys' privacy policy makes no mention of the use of video surveillance, or any collection of personal information by such means.

Sobeys also confirmed that there were no signs posted at the store to advise shoppers that the premises were under video surveillance. However, there is a monitor that shows people entering and leaving the store, and cameras are suspended from the ceiling, in plain view of customers. Sobeys' privacy officer argued that it would be obvious to anyone in the store that video cameras were in use.

In our view, a monitor at an entranceway and cameras hanging high overhead, by themselves, do not provide clear and sufficient notice to patrons that a video surveillance system is in use.

Moreover, people must be made aware of the surveillance while still outside the store, so that they can choose whether to enter. According to our guidelines, a sign should be posted at the front entrance to alert prospective customers. It should briefly describe the purpose of the video surveillance,



Guidelines on Overt
Video Surveillance
in the Private
Sector

and offer a telephone number for further information or to let patrons request access to their personal information.

In a preliminary report provided to Sobeys in December 2010, we recommended that all of the chain's stores provide proper notice about the collection of personal information through the use of video surveillance. We also called on Sobeys to include a description of its practice of collecting personal information via video surveillance in its privacy policy.

In response to our recommendations, Sobeys has now placed a sticker at the entrance of the store in question, where customers can also see a live monitor along with a camera hanging down beside it, as well as in another area of the store, indicating that closed-circuit television cameras are in use.

Sobeys is also encouraging its other corporate stores to affix such decals and has since advised us that decals are in place at all its New Brunswick stores.

At the conclusion of our investigation, we determined that the collection portion of the complaint was well founded.

However, we also concurred that the decals, along with the viewing monitor at the store's entrance and the camera hanging down beside the viewing monitor, constituted sufficient notice that the store is under video surveillance. Accordingly, we also deemed the issue to be resolved.

In addition to the collection issue, the complainant also alleged that she was being denied access to her personal information.

Sobeys' privacy officer initially told us that the only personal information the store collected about the complainant in the course of its commercial activities was the security video footage.

When pressed, however, the privacy officer stated that the store had gathered further personal information about the complainant, but that it was generated to defend itself against an anticipated claim for damages by the complainant.

Because the videotape had been turned over to the complainant two days after her PIPEDA request, we dismissed that portion of the access complaint as not well founded.

Concerning the reports and letters created after the injury occurred, we took the view that Sobeys' activity of defending itself against a customer's claim in tort for an incident that occurred on its premises was sufficiently related to its regular course of business that it constituted a commercial activity under the Act. It was therefore covered by PIPEDA.

But we also found the documents in question to be subject to litigation privilege, a component of solicitor-client privilege, which protects materials brought into existence for the dominant purpose of litigation, or reasonably anticipated litigation.

In our view, Sobeys was therefore entitled to deny the complainant access to the personal information contained in those documents.

Accordingly, we determined that the portion of the access complaint related to the letters and reports was not well founded.

UNRESOLVED COMPLAINTS

Most of the time, we are able to reach a satisfactory resolution to issues through our investigations process. The vast majority of organizations respond positively to our recommendations.

However, if a company refuses to follow our recommendations, we can go to Federal Court to seek an order to enforce compliance and to provide for damages where appropriate. The Commissioner also has the option of naming companies we have investigated if she deems that doing so is in the public interest in the particular circumstances of the case.

The following case summary describes an investigation where we were unable to reach a satisfactory conclusion.

RISK: INTERNATIONAL ORGANIZATIONS AND PIPEDA COMPLIANCE

KLM WEBSITE IN CANADA DOES NOT MEET PIPEDA OBLIGATIONS

The complainant alleged that KLM Royal Dutch Airlines (KLM) denied him access to his personal

information and that of his family members, collected and used for KLM flights. In addition, he alleged that KLM failed to provide him with information about its policies and practices relating to the management of his personal information.

Despite the fact that KLM is an international airline company headquartered in Amstelveen, the Netherlands, the OPC determined that it had jurisdiction in the case because there was a real and substantial connection between the subject matter and the parties to Canada – a test determined by the Federal Court.

The complainant claimed that he asked KLM in a letter dated January 10, 2009, for access to 13 types of passenger information relating to two flights he and his family had taken in 2005. KLM claimed it received a letter from the complainant only on March 17, 2009 asking for this information.

In a letter dated May 6, 2009, KLM informed the complainant that the only identifiable passenger information available so long after the flights was the check-in information for one of the flights, which it supplied. Not satisfied with that response, the individual filed a complaint with this Office on June 10, 2009.

We were satisfied with KLM's response that no information still existed was acceptable, as three-and-a-half years had elapsed since the date of the flights and the complainant's first request. PIPEDA states that organizations should not retain personal information longer than required to fulfill

identified purposes. Unless there were extenuating circumstances, it is not clear why KLM would be expected to retain the complainant's personal information for longer.

However, by failing to meet the 30-day response deadline specified in the Act, KLM had initially denied the complainant access to his personal information.

As well, our investigation's review of KLM's online privacy policy for its Canadian website concluded that the policy is incomplete, is not compliant with PIPEDA, and does not include comprehensive information on its practices and policies relative to KLM's personal information management practices.

Our investigation report recommended that KLM ensure the privacy policy for the Canadian version of its website complies with the Act, and that this online privacy policy either includes information relating to the management of personal information

by the company, or at the very least indicates that this type of information can be obtained from KLM on request.

KLM originally appeared quite willing to implement our recommendation by updating its Canadian website's privacy policy to meet its obligations under the Act. However, an email from KLM dated February 17, 2011 indicated that its planned updating of KLM's privacy policy had been postponed due to technical difficulties. We were disappointed by KLM's lack of commitment to any particular timelines in implementing the recommendation.

We were left with no alternative but to close our investigation with an unsatisfactory result. Accordingly, we concluded that the matter was well founded.

A full Report of Findings from this investigation is available on our website.

4.9 DATA BREACHES

Our Office encourages organizations to voluntarily report personal information data breaches. These breaches fall into three broad types:

Accidental disclosure: Incidents where an organization discloses personal information to unintended recipients by accident. For example, bank statements sent to the wrong address through mechanical or human error, or personal information

made publicly available on an organization's website through a technical error.

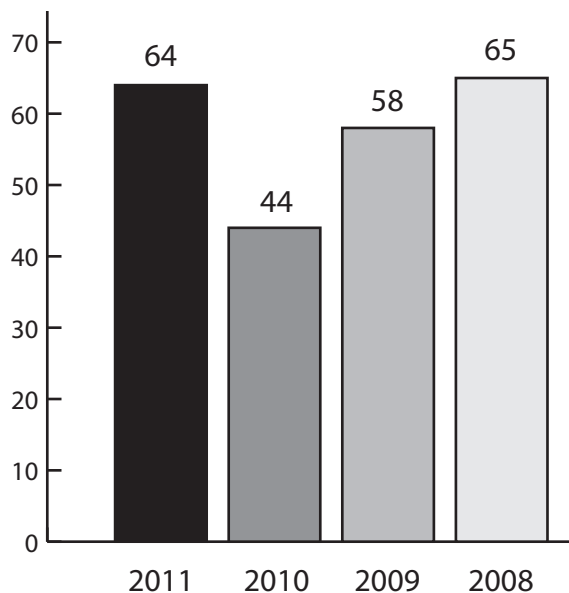
Loss: Incidents where personal information is lost by an organization, usually through the loss of a laptop, CD or paper documents.

Unauthorized access, use or disclosure: Incidents where personal information is accessed, used or

disclosed by someone without an organization's authorization. For example, a stolen laptop, an online hack of an organization's database, or an employee accessing or using personal information for unauthorized purposes.

In 2011, 64 private-sector data breach incidents were voluntarily reported to us.

Voluntary Breach Notifications



While this is a 45 percent increase over the number of incidents reported to us in 2010, it is within the range of the last few years.

Breach notifications from the financial industry – the leading sector in routinely reporting breaches to us – remained steady at 29 incidents. By contrast,

breach notifications from all other sectors more than doubled from 15 in 2010 to 35 in 2011.

We are pleased with this indication that awareness about breach notification and its benefits has spread substantially beyond the financial sector to the broader Canadian private sector.

The profile of breach notification became greater in late 2010 and 2011 thanks to Alberta's introduction of mandatory breach notification and to the draft federal legislation to make breach notification to the Privacy Commissioner mandatory.

Privacy officers in the private sector say they are making conscious decisions to proactively report breaches, even though the federal legislation requiring them to do so has not yet been passed into law. We commend them for doing so.

When we receive a breach report, our Office works with the organization's privacy officer to ensure that the necessary steps are taken and that affected individuals are provided with consistent information and have their concerns addressed. Such cooperation can reduce the prospect of complaints to the Privacy Commissioner.

EXAMPLES OF BREACH INCIDENTS REPORTED TO THE OPC

WEBSITE HACKED

A small retailer observed that credit card numbers and shipping addresses of some customers of its

e-commerce website had been compromised by a website hack. The organization immediately shut down the website and notified our Office and the police. In addition, it asked its payment provider to notify all affected credit card companies about the compromised data. The organization also undertook a forensic audit, and e-commerce sales were not resumed until all audit recommendations to improve security were implemented.

DATA CDs LOST

Unencrypted data CDs containing personal information about a significant number of customers were accidentally lost internally by a financial institution. While nothing suggested the data had fallen into unauthorized hands, the financial institution quickly notified our Office and took measures to address the matter. These measures covered three critical aspects of responding to a breach: a) mitigating the impact by searching for the lost CDs and instituting enhanced monitoring of affected customer accounts; b) notifying all affected customers of the incident; and c) investigating and changing procedures to ensure that in future, the organization's privacy policy (including encryption) would be followed.

EMAIL ADDRESSES DISCLOSED

A retailer reported to us that two of its stores had accidentally sent bulk email messages to a group of customers without concealing individual customer email addresses. In one case, a customer's name and phone number were also included in the bulk email to a number of other customers. The retailer responded quickly, notifying and apologizing to affected customers within days of the incident. The company's Privacy Officer also directed regional management to investigate to ensure that similar bulk emails were not sent by other stores without concealing email addresses. Employees of the two stores involved were re-trained by regional management in the company's protocol for protecting and concealing the personal information of customers when communicating by email.

Reaching Out to Canadians

The concept of privacy is undeniably changing, as it has through time.

Once privacy may have been primarily equated with seclusion – the right to shut oneself off from the world. Yet many in the generation that has grown up in the age of social media have never known real physical seclusion. For them, privacy is more likely to mean controlling the access which others have to information about them.

That’s because protecting privacy has become much more complicated than simply shutting a physical door or withdrawing to some rural Walden.

Nowadays, electronic tentacles poke and prod even into the most remote retreat. For too many people, these tentacles are invisible, gathering personal information from cars rolling down quiet neighbourhood streets or



from malicious software surreptitiously deposited inside their computers.

Because privacy is more important than ever and protecting personal information more complicated than ever, our Office invests a great deal of effort in raising public awareness.

We speak to individuals about their privacy rights, how those rights are being tested and sometimes undermined, and what they can do about it.

We also talk to businesses about their obligations under PIPEDA, and how best to safeguard the personal information of Canadians.

Making presentations at conferences and other events is a central pillar of our public outreach program. In 2011, the Commissioner, Assistant Commissioner and other OPC staff delivered more

than 140 speeches and presentations. As well, our Office had exhibits at high-profile events.

Media interest in privacy issues continues to be high, particularly concerning the online world. Our Office tries to advance our public education mandate through the traditional mass media by accepting as many media interview requests as possible. In 2011, we issued 37 news releases.

Digital literacy is our focus online. Our efforts are aimed at helping individuals develop and improve the skills and knowledge needed to protect their personal information. As well, we work to make sure that businesses give customers the information and tools needed to make informed privacy choices.

Overall visits to our websites were 2,715,384. We added nearly 500 subscribers to our electronic newsletter.

The OPC created a Twitter account in 2010 and used it last year to send roughly 500 “tweets.”

We also cross-promoted our online and social media presences and added QR Codes (squares containing ink blobs that can be read by smartphones) to printed

materials, to make it even easier and faster for people to access our guidance.

The Office distributed approximately 12,000 paper publications in 2011. These included some of the publications published during the year, including annual reports under PIPEDA and the *Privacy Act*, three audits and two publications further described in this chapter – *PIPEDA and Your Practice: A Privacy Handbook for Lawyers* and the *2011 Canadians and Privacy Survey*.

Fact sheets are an effective means of informing Canadians about emerging privacy concerns. The topics of new or revised PIPEDA fact sheets made available this year included cloud computing, cookies, protecting personal information on mobile devices and online behavioural advertising.

Cartoons confer a lighter touch upon serious privacy messages and we continued to make use of cartoons, created exclusively for us, in presentations and on posters, postcards and our popular calendar.

This Chapter provides a summary of some of our major outreach activities in 2011. Note that details of our outreach to children and youth are included in Chapter 2.

5.1 TORONTO OFFICE

The first full year of operation of the OPC Toronto office has bolstered our engagement with businesses, industry associations, academics and other stakeholders.

The office was opened in the fall of 2010, following the maxim of going where the action is. An analysis of two years of PIPEDA complaints had found that 45 percent of respondent organizations were located,

or had their headquarters, in the Greater Toronto Area.

Because so many industry associations and organizations are also headquartered in the GTA, we can leverage the established networks of these organizations – through presentations at their events, and periodic face-to-face meetings.

For instance, in 2011, the OPC Toronto office undertook 48 outreach activities to organizations and industry associations.

In addition, the OPC Toronto office held information sessions with stakeholders designed to promote greater discourse on emerging privacy

issues. The growth of the digital economy has seen businesses leveraging advances in technology to find new ways to reach customers.

Against this backdrop, these sessions let the OPC and businesses exchange information about these innovations. With a better grasp of the underlying legislative issues, businesses will be in a position to make more informed choices to support responsible innovation practices and protect the personal information of their customers.

Finally, since many of our respondents are located in the GTA, we have conducted investigations from the Toronto office as a way of improving efficient and timely service to Canadians.

5.2 SELF-ASSESSMENT TOOL FOR ORGANIZATIONS

In May 2011, continuing collaborative efforts to promote harmonized and consistent privacy practices, the OPC and the Offices of the Information and Privacy Commissioners of Alberta and British Columbia together launched a vehicle to help organizations understand and assess how to protect the personal information they hold.

Securing Personal Information: A Self-Assessment Tool for Organizations is an online, interactive instrument with 17 areas that organizations can assess. These areas include policies, records management, network security, access control, incident management and continuity planning.



Securing Personal Information: A Self-Assessment Tool for Organizations

The tool helps organizations discover where they may need to focus their efforts to ensure that reasonable security safeguards are in place and that they are appropriate for the amount and sensitivity of the personal information they hold.

It will also help organizations to ensure that the safeguards take into account the possible risks to that information and the potential fallout if something happened to it. We think privacy officers will find this tool helpful in promoting the message throughout their organizations that personal information is a vital asset that should be protected.

5.3 SMALL BUSINESS WEEK - CYBER SECURITY

More and more small businesses are going online to reach new customers around the world and provide greater convenience for those closer to home. Our Office seized the opportunity presented by Small Business Week, October 16-22, 2011, to provide a wealth of practical advice about securing customer and client information from cyber threats.

Trust is a major asset for small businesses and that trust is imperiled when customer, client or employee information is stolen or tampered with. Contrary to popular belief, most computer systems aren't compromised or "hacked" by daring acts of genius against which average Joes are defenseless.

Like a burglar who checks first to see if he can enter a home through an unlocked door or window before picking a lock or breaking a window, successful hackers often meet their objective by exploiting common vulnerabilities or "known holes."

The OPC produced a series of articles about these common vulnerabilities and the steps that small businesses could take to protect their valuable information. That advice included:

- regularly updating anti-virus programs and other software and changing passwords every few weeks for online services;
 - encrypting all data, whether on hard drives, databases or USB keys, possibly using the free encryption options bundled with some common operating systems;
 - being vigilant against online impersonation, including making telephone calls to confirm the origin of suspicious emails; and
 - implementing an IT security policy across the entire business.
- Not only are such steps savvy commercial practice, we reminded small businesses, but it is also an organization's legal responsibility to protect the personal information it collects.
- In addition to activities specifically geared to Small Business Week, our Office also exhibited to small- and medium-sized enterprises at 10 events, posted a series of SME-targeted entries to our blog and created a presentation on PIPEDA compliance geared specifically to SMEs.
- securing a business WIFI network by omitting the business name or address, turning on wireless encryption and choosing a long, complicated password;

5.4 BUSINESS POLL

It's essential that our Office understands how familiar businesses are with privacy issues, what types of privacy policies and practices they have in place and how aware they are about emerging privacy issues.

To gain better insight into this business-privacy interface, the OPC in 2011 commissioned a telephone survey of approximately 1,000 businesses

that are subject to PIPEDA. The random sample included small, medium and large enterprises.

Interviews were conducted with representatives who knew the privacy policies and practices of their companies, such as owners, CEOs or chief privacy officers. A report summarizing the survey results will be published in 2012.

5.5 LAWYER'S HANDBOOK

Because lawyers face many issues about the handling of personal information, our Office prepared a guidance document entitled *PIPEDA and Your Practice: A Privacy Handbook for Lawyers*. The handbook was launched in August 2011 at the Canadian Bar Association's annual Canadian Legal Conference and Expo in Halifax, Nova Scotia.

Our handbook aims to help lawyers meet their legal obligations under PIPEDA, where applicable, and covers practical privacy matters that can arise while managing a law firm and conducting litigation.

Dealing with the potential application of PIPEDA to day-to-day legal work, it sets out best practices

in managing the collection, use and disclosure of personal information, and in responding to requests for access to personal information.

The first part of the handbook is dedicated to privacy issues potentially encountered while managing a law practice, and the latter part canvasses privacy issues that can arise during civil litigation.

Our hope is that the handbook will help lawyers think of protecting privacy not only as a matter of legal obligation, but also as a matter of ethical and respectful conduct on behalf of the profession and the clients they serve.



PIPEDA and Your Practice: A Privacy Handbook for Lawyers

5.6 DATA PRIVACY DAY 2011

On January 28, 2011, Canada joined many other countries in celebrating Data Privacy Day. Recognized by privacy professionals, corporations, government officials, academics and students around the world, Data Privacy Day helps to raise awareness about the impact that technology is having on privacy rights and to promote the protection of personal privacy.

In 2011, our Office developed the slogan: *The Net never forgets. Remember to protect personal information.* Used in a variety of materials, the slogan reminded

Canadians that whenever they go online, they are building an identity through their activities and the words and images they post.

This message was highlighted in our Data Privacy Day news release, which generated coverage in Canadian media. In addition, our Office ran an online draw for prizes and shared Data Privacy Day resources, such as posters and fact sheets, with other privacy regulators and organizations.

5.7 OUTREACH ACROSS CANADA

Federal, provincial and territorial officials responsible for privacy agreed during a fall gathering in Quebec City to meet regularly to discuss their respective outreach initiatives.

Materials developed for Data Privacy Day were sent to the offices of provincial and territorial privacy

commissioners, who further distributed them to places such as schools and regional health authorities.

OPC staff travelling outside Ottawa in 2011 made greater efforts to meet with provincial and territorial privacy offices. At events such as meetings with boards of trade we strive to involve our counterparts.

5.8 CONTRIBUTIONS PROGRAM

Established in 2004, the Contributions Program has been very successful in providing funds to cutting-edge research and public education projects dealing with privacy. With an annual budget of \$500,000, the program awards up to \$50,000 per project.

In addition to advancing knowledge, the program aims to increase awareness and understanding among individuals and organizations of their privacy rights and obligations and facilitate practical application of research results by relevant end-users.

In 2011, we funded a wide range of projects of interest to Canadians, including:

- a study of how private security firms operate surveillance camera systems that can be set up for specific events or at temporary hot spots (called re-deployable systems). The research will focus on the interaction between private sector data gatherers and law enforcement authorities;
- the creation of a cross-media game that will use physical and digital spaces to teach Canadian children about privacy;
- the creation of an interactive and educational package about protecting personal information for teachers; and
- a study of the privacy expectations of online social network users, looking at how “private” they believe online social networking spaces truly are.

Research funded through the Contributions Program is conducted independently and at arm’s length from the OPC.

We recently adopted a new five-year strategy for the program to increase its impact among our stakeholders and in Canada generally. The strategy is founded on the following six points:

1) Leveraging impact through partnerships

The OPC will invite several government funding agencies to partner with it to leverage financial resources available and increase the impact of

funding. These partnerships will expand the scope of potential applicants across diverse disciplines.

2) Enabling knowledge translation and application

Funding applicants will be encouraged to plan and provide for knowledge translation initiatives as part of their research proposals. The OPC also plans to organize knowledge translation symposiums over the next few years featuring the research generated under the program.

3) Strengthening peer review

A more robust peer review system supplemented by external reviewers will be established to help ensure higher quality assessments of research proposals and ultimately, higher quality research funded through the program.

4) Facilitating access through technical enhancements

Technical improvements such as an online application system and a searchable research database will help applicants and users to more easily apply for funding or access the knowledge generated under the program.

5) Evaluating the success of the program

A systematic evaluation process will be established to help ascertain the relevance and uptake of research results among researchers, media and other stakeholders.

6) Renewing our public communications strategy

A renewed public communications strategy

for the Contributions Program will be drafted to help further the success of the research and knowledge generated under the program.

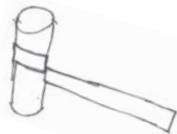
By implementing this strategy, we hope to ensure that the program continues to be responsive to the needs of the OPC and Canadians for cutting-edge research in the area of privacy promotion and protection.

5.9 SPEAKING ENGAGEMENTS

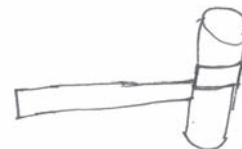
Speaking engagements are a key component in raising public awareness. These give the OPC the opportunity to directly address the specific interests of industry groups, privacy professionals, policy-makers, students and other segments of the Canadian public. Just as important, the speeches allow the Commissioner, Assistant Commissioner and staff to directly respond to the questions that concern these audiences.

In 2011, we took part in 143 events. These included the International Association of Privacy Professionals Canadian Privacy Summit 2011, Canada 3.0, organized by the Canadian Digital Media Network, the Canadian Bar Association Legal Conference and Expo and the Marketing and Law Conference, organized by the Association of Canadian Advertisers. As well, we spoke to a number of business groups and events aimed at small-and medium-sized enterprises.

A number of speeches are available on our website.



In the Courts



In 2011, our Office continued to be involved in a number of long-standing cases before the courts.

Under section 14 of PIPEDA, a complainant who has received a report from our Office may apply to the Federal Court for a hearing with respect to any matter referred to in his or her complaint or referred to in the Commissioner's report, subject to certain limitations.

With the consent of the complainant, the Privacy Commissioner may appear on behalf of the complainant or apply directly to the Federal Court herself with respect to the same matters (section 15 of PIPEDA). The Commissioner may also apply to the Federal Court to appear as a party in a hearing initiated by a complainant.

This year, our Office reached settlements in two Commissioner-initiated applications filed in past years. Another application filed under section 15 in a previous year continued to proceed before the Federal Court.

The Privacy Commissioner regularly initiates judicial action in well-founded cases that remain

unresolved in order to seek court enforcement of her recommendations. We have found this has helped establish a high level of compliance with recommendations.

In keeping with the spirit of our mandate, we have respected the privacy of individual complainants by not including their names in this report.

COMMISSIONER-INITIATED COURT APPLICATIONS (SECTION 15 OF PIPEDA)

Federal Court File No. T-1275-10

Privacy Commissioner of Canada v. Association of American Medical Colleges

This Federal Court application, initiated by the Commissioner, relates to the refusal by the Association of American Medical Colleges (AAMC) to cease collecting sensitive biometric information, such as digital fingerprints, a digital photograph and the driver's licence information of candidates taking the Medical College Admissions Test (MCAT).

The AAMC collects this information to ensure the integrity of the MCAT and because of alleged

fraud related to the MCAT in the United States and Canada. The AAMC, through a third-party contractor, collects digital fingerprints and other personal information from MCAT candidates at exam centres. Although the fingerprints are converted into a digital template, the actual fingerprint images are retained in case the template becomes corrupted.

Our investigation into the matter related to notification of purposes, collection, retention and safeguards. Based on the information provided in the course of the investigation, the Commissioner was of the view that there were less privacy-invasive means to meet the AAMC's purposes in the circumstances.

In response to the Office's Preliminary Report of Finding, the AAMC stated that it would revise its notice and consent language to reflect forthcoming changes as to how personal information would be used. However, it stated that it would continue to collect fingerprints from candidates, as well as a scan of the candidate's driver's licence, and the candidate's photograph.

Our Office, therefore, concluded that the matter was well founded and resolved with respect to the notification issue, but well founded with respect to the collection issue.

In August 2010, the Commissioner filed her Notice of Application in Federal Court, requesting as relief an Order directing the AAMC to find less privacy-intrusive means to achieve its purposes of ensuring the integrity of this high-stakes examination. The

parties filed their affidavits and documentary exhibits in Court in the Fall/Winter of 2010.

At the time of writing this Annual Report, the matter was still before the Federal Court.

Note: This case was previously reported in the 2010 Annual Report.

Federal Court File No. T-1885-10
Privacy Commissioner of Canada v. Greater Toronto Airports Authority

Initiated by the Commissioner, this application concerns the inappropriate collection of personal information by an employee of the Greater Toronto Airports Authority (GTAA), and the GTAA's failure to provide the complainant access to all of his personal information under its control.

One of the allegations that the complainant made was that his ex-wife, an employee of the GTAA, inappropriately used GTAA equipment to collect photographs of him and his family while at Toronto's Pearson Airport. The individual contacted the GTAA with his privacy concerns and the GTAA conducted its own internal investigation. The individual also sought access to his personal information from the GTAA. Being unsatisfied with the manner in which the GTAA handled the investigation and his access request, the individual filed a complaint with our Office. Our Office ultimately found his complaints to be well founded and filed an application under section 15 of PIPEDA.

The Court application raised, among other matters, the issue of whether the GTAA failed to meet its obligations under PIPEDA when an employee collected and used the complainant's personal information without his knowledge and consent. As well, it raised the issue of whether the GTAA provided the complainant with access to all of his personal information under its control.

In November of 2011, we reached a settlement with the GTAA. As part of the settlement, the GTAA provided all of the personal information requested by the complainant to him. In addition, the GTAA implemented an internal camera operating procedure, as well as a written manual on internal camera operation.

Our Office is pleased that the GTAA has agreed to take steps to ensure that the privacy rights of airport passengers are respected.

The complainant in this case has filed a separate Notice of Application for a hearing before the Federal Court, under section 14(1) of PIPEDA regarding this matter. The complainant was seeking various forms of redress, including damages. That separate matter remained unresolved as of the time of writing this Annual Report.

Note: This case was previously reported in the 2010 Annual Report.

Federal Court File No. T-243-10

Privacy Commissioner of Canada v. Sobeys

This Federal Court application, initiated by the Commissioner, stems from a complaint about Sobeys' practice of asking all customers who purchase tobacco products to show identification, regardless of their apparent age.

During the complaint investigation, Sobeys indicated that it has adopted an Ontario-wide policy of asking all purchasers of tobacco products for identification, in order to comply with the requirements of the *Smoke Free Ontario Act*. The legislation prohibits tobacco sales to persons under 19 years of age and requires sellers of tobacco to ask persons who appear to be under the age of 25 for identification.

The Privacy Commissioner's Office recommended that Sobeys develop alternative procedures that do not involve requiring customers to show identification where customers seeking to purchase tobacco products are clearly over the age of 25. The Office subsequently filed an application in Federal Court seeking an order requiring Sobeys to comply with its recommendation.

Following discussions between the parties, Sobeys has amended its policy regarding sales of tobacco in Ontario so that individuals who are clearly of legal age to purchase tobacco products will, in appropriate circumstances, be exempt from the requirement to show identification. Sobeys will be advising its

Ontario customers on its public website that if they have concerns about Sobeys' policy requiring identification then they may address those concerns to the store manager.

The Privacy Commissioner filed its notice of discontinuance on May 31, 2011.

Note: This case was previously reported in the 2010 Annual Report.

JUDICIAL REVIEW APPLICATIONS (SECTION 18.1 OF THE *FEDERAL COURTS ACT*)

Federal Court File No. T-1587-11 and T-1588-11
X v. Privacy Commissioner of Canada

On September 27, 2011, the applicant brought two applications for judicial review, seeking a review of two Reports of Findings issued by our Office with respect to the applicant's complaints.

The applicant had complained to our Office that his former employer's counselling service provider disclosed information to his employer, who in turn disclosed the information to other employees, the applicant's physician, and an independent medical examiner.

Our Office's investigation found that the complaints were not well founded. Our Office concluded that the disclosure by the counselling service provider to the employer was authorized pursuant to a Statement of Understanding that had been signed by the applicant. With respect to the disclosures by the employer, the investigation found that the applicant had provided either express or implied consent.

The applicant alleges that the Commissioner failed to observe principles of procedural fairness, based her decision on an erroneous finding of fact, and acted, or failed to act, by reason of fraud or perjured evidence.

At the time of writing this Annual Report, the matter was still before the Federal Court.

Substantially Similar Provincial and Territorial Legislation

Under paragraph 26(2)(b) of PIPEDA, the Governor in Council can issue an Order exempting an organization, a class of organizations, an activity or a class of activities from the application of PIPEDA with respect to the collection, use or disclosure of personal information that occurs within a province that has passed legislation that is substantially similar to PIPEDA.

Section 25(1) of PIPEDA requires our Office to report annually to Parliament on the “extent to which the provinces have enacted legislation that is substantially similar” to the Act.

In past annual reports, we have reported on legislation in Quebec, Ontario (for personal health information), Alberta and British Columbia that has been declared substantially similar.

Industry Canada has stated that to be substantially similar, provincial or territorial laws will:

- incorporate the 10 principles in Schedule 1 of PIPEDA;

- provide for an independent and effective oversight and redress mechanism with powers to investigate; and
- restrict the collection, use and disclosure of personal information to purposes that are appropriate or legitimate.

On November 17, 2011, New Brunswick’s *Personal Health Information Privacy and Access Act* (PHIPAA) was declared substantially similar to PIPEDA. As a result, personal health information custodians to which PHIPAA applies are exempt from the application of Part 1 of PIPEDA in respect of the collection, use and disclosure of personal health information in New Brunswick.

PHIPAA received Royal Assent on June 19, 2009 and it came into force on September 1, 2010.

Newfoundland and Labrador’s *Personal Health Information Act* (PHIA), which came into force on April 1, 2011, had not been declared substantially similar as of the end of 2011.

The Year Ahead

“It takes all the running you can do, to keep in the same place.” So complains the Red Queen in Lewis Carroll’s *Through the Looking-Glass*.

Science has appropriated this whimsical image into the more formal Red Queen hypothesis in the field of evolution, which states that continuing adaptation is needed for a species to maintain its fitness relative to the systems evolving along with it.

The OPC might be considered an example of the Red Queen hypothesis in action.

Our Office has to keep running as fast as it can just to keep pace with the rapid evolution of communications technologies and societal practices that give rise to new challenges to privacy and the protection of personal information.

In the year ahead, we will continue strengthening our grasp of privacy issues in the online digital world, where more and more Canadians are living their lives. We will apply that hard-won expertise to help Canadians hone strong digital literacy skills. We will expand our use of online tools and other means

of communication to raise public awareness about privacy rights.

Here are a few specific examples of our continuing evolution in 2012:

YOUTH OUTREACH INITIATIVES

GRAPHIC NOVEL

During our 2010 consultations, we heard that young people need special attention because they are using the Internet at younger ages and providing personal information without a clear idea of how and why it will be used. In response, the OPC agreed to develop innovative and creative ways to reach out to young people, leading to the idea of a graphic novel.

The graphic novel will be 12 to 16 pages in both French and English, covering a few privacy subjects through single illustrated pages and





multi-page spreads. The overarching theme will be broader than simple digital privacy; it will introduce concepts and ideas necessary for understanding how present-day digital interfaces work, and how these can present technological challenges to online privacy.

The OPC has engaged a writer and a graphic designer/illustrator to jointly produce the novel, which is slated for release in 2012, both online and in print.

Feedback on a preliminary version of the novel will be provided by focus groups of youth aged 12 to 17 in sessions organized by a public opinion research firm. Youth will also be canvassed for their views on the OPC youth website and, more generally, their opinions about privacy.

MORE FOR YOUTH

Following up on the successful launch of our two youth presentation packages intended to be used with students in Grades 7-8 and Grades 9-12², we will be releasing a third package geared to students in Grades 4-6.

Like the earlier packages, this will contain the tools needed for teachers or other adults to provide effective and engaging presentations in schools or the community. The goal is to show young people in all three age groups how technology can affect their privacy, and how they can build secure online identities while keeping their personal information safe.

2 Secondary I to II and III to V in Quebec.

In January 2012, our Office also launched a video version of the package, targeted to students in Grades 8 to 12 and available for viewing on our main website, youth website and YouTube channel.

Privacy videos of a different nature will be in the spotlight in March, when students in the Encounters with Canada program from schools across the country vote to decide the winners of our fourth annual *my privacy & me* national video contest for youth. Students aged 12 to 18 enter by producing video public service announcements from one to two minutes long on privacy issues associated with social networking, mobile devices, online gaming or cybersecurity.

Prizes go to the top videos in each of the four themes.

CANADA'S ANTI-SPAM LEGISLATION

We will continue to work with Industry Canada and our enforcement partners to prepare for the coming into force of the legislation. As well, we will be enhancing our in-house technical and investigative capability to deal with the challenges of enforcing the legislation.

TECHNOLOGY LAB

In 2012, the technology lab will boost its capabilities by adding equipment and personnel, primarily to deal with the challenges posed by implementing Canada's new anti-spam legislation. Under the law, the OPC is responsible for investigating the unauthorized

collection of personal information, particularly electronic address harvesting, and collection of personal information through unlawful access to computer systems.

DATA PRIVACY DAY

Building on the success of our campaign in 2011, OPC messaging for Data Privacy Day in 2012 will focus on the importance of limiting the amount of personal information shared online. In the week leading up to January 28, we will be engaging in various activities, which will include the launch of new tools, and presentations to youth, public servants, businesses and staff. Our Office will also develop new resources, such as posters and graphics, which can be used to raise privacy awareness in any organization.

PRIVACY AND LEGISLATION

The second Parliamentary review of PIPEDA is expected to be launched in 2012. Amendments could help ensure the law remains an effective tool for protecting the privacy rights of Canadians.

INVESTIGATIONS

Handling complaints under PIPEDA is where the rubber hits the road at the OPC. We have already substantially sped up our handling of the hundreds of formal complaints received annually.

Now, beginning in January 2012, we are adopting amended dispositions with updated definitions. These new dispositions better reflect the responsibilities of

organizations to demonstrate accountability under the Act, while the new definitions provide clear language about what each disposition means.

The key change is a revised approach to identifying a matter as “resolved.” As of January 1, 2012, we will only use a “well founded and resolved” finding in cases where the complaint was well founded and the organization has, by the time a finding is issued, actually taken the necessary corrective action.

The stand-alone finding of “resolved” will be eliminated to avoid confusion between this finding and the dispositions of “settled” and “early resolved.”

In tandem, a new finding of “well founded and conditionally resolved” will now be applied to cases where an organization has made an express commitment to demonstrate its implementation of corrective measures within a specified time period after the Office’s findings are issued. This wording reflects that, in some cases, an organization commits to addressing the issues identified by our Office, but that not all needed changes can be made immediately.

When we use this finding, we will ask the respondent to keep us informed on a predetermined schedule after the investigation, to assess whether necessary corrective action has been taken.

Additionally, we will be asking companies to demonstrate compliance with our recommendations. This could be through an independent third-party audit at their own expense within a given time frame.

Here are the new dispositions and their definitions:

Not well founded: The investigation uncovered no or insufficient evidence to conclude that 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.

Early resolved: The OPC helped negotiate a solution that satisfied all involved parties, without a formal investigation being undertaken. The Commissioner does not issue a report.

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.

MOVING DAY 2013

Over the next 18 months the OPC will be preparing for the summer of 2013, which will see its operations move from downtown Ottawa to Gatineau, across the river in Quebec. Our Ottawa office currently houses 95 percent of our employees. The move provides the opportunity to trade up to a new building boasting the latest technology as well as being environmentally certified.

Appendix I

DEFINITIONS

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.

DEFINITIONS OF FINDINGS AND OTHER DISPOSITIONS

The Office has developed a series of definitions of findings and dispositions to explain the outcome of its investigations under PIPEDA. Below are the definitions that were in place up to the end of 2011.

Beginning in January 2012, we are adopting amended dispositions with updated definitions. These new dispositions better reflect the responsibilities of organizations to demonstrate accountability under the Act, while the new definitions provide clear language about what each disposition means. For a description of the new set of dispositions and definitions, please see the “Year Ahead” Chapter.

Not well founded. The investigation uncovered no or insufficient evidence to conclude that an organization violated PIPEDA.

Well founded. An organization failed to respect a provision of PIPEDA.

Resolved. The investigation substantiated the allegations but, prior to the conclusion of the investigation, the organization took or committed to take corrective action to remedy the situation, to the satisfaction of the OPC.

Well founded and resolved. The Commissioner, being of the view at the conclusion of the investigation that the allegations were likely supported by the evidence, before making a finding made a recommendation to the organization for corrective action to remedy the situation, which the organization took or committed to take.

Settled. The OPC helped negotiate a solution that satisfies all involved parties during the course of the investigation. No finding is issued.

Discontinued. The investigation was discontinued before the allegations were fully investigated. An investigation may be discontinued as a result of a request by the complainant, or where the complaint has been abandoned. **In addition**, as of April 1, 2011, when changes to PIPEDA came into effect, an investigation may be discontinued at the

Commissioner's discretion for the reasons set out in subsection 12.2(1) of PIPEDA.

No jurisdiction. The investigation led to a conclusion that PIPEDA did not apply to the organization or activity that was the subject of the complaint.

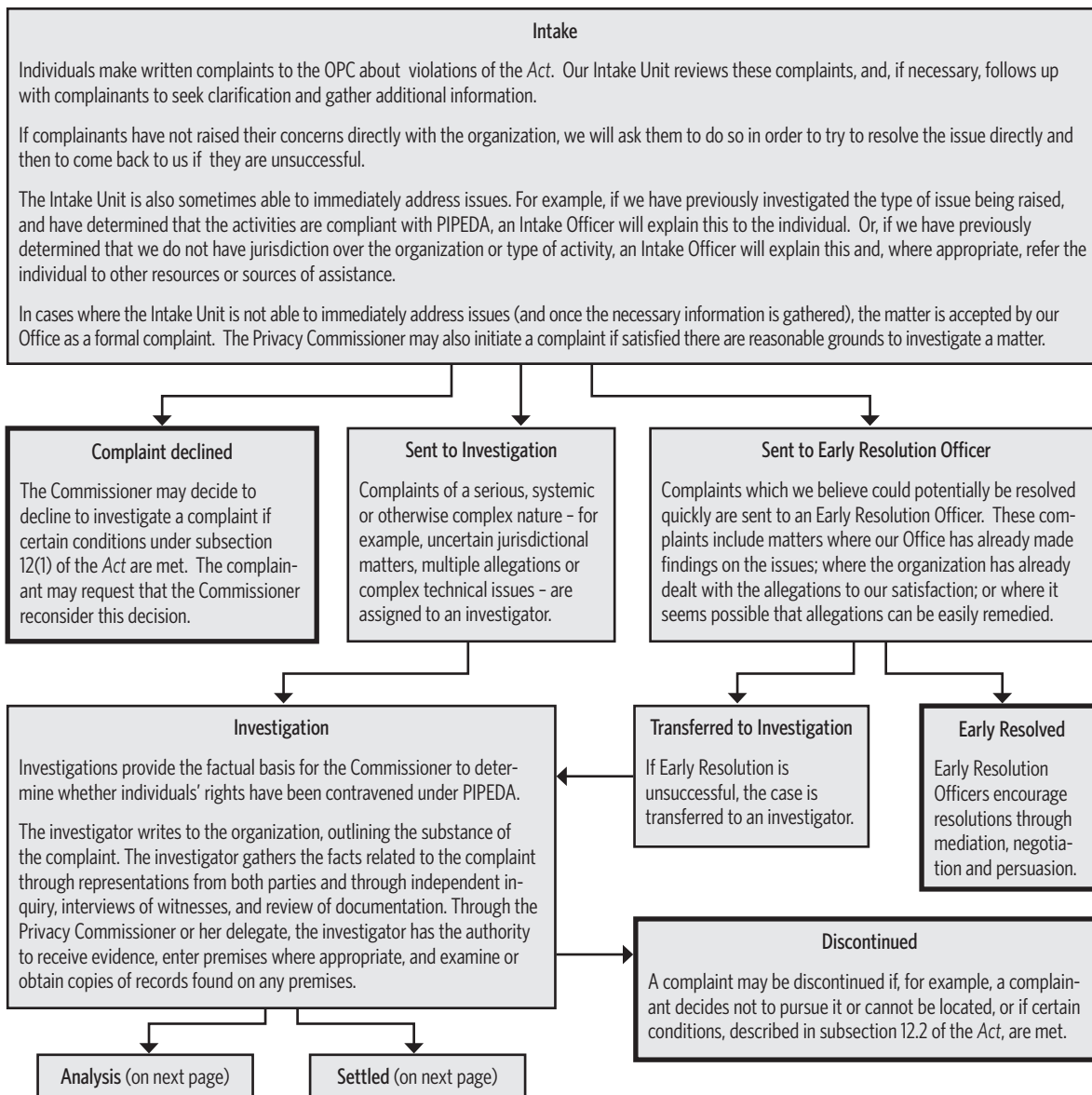
Early resolution. This applies to situations where the issue was dealt with before a formal investigation occurred. For example, if an individual filed a complaint about a type of issue that the OPC had already investigated and found to comply with PIPEDA, we would explain this to the individual. "Early resolution" would also describe a situation where an organization, on learning of allegations against it, addressed them immediately to the satisfaction of the complainant and the OPC.

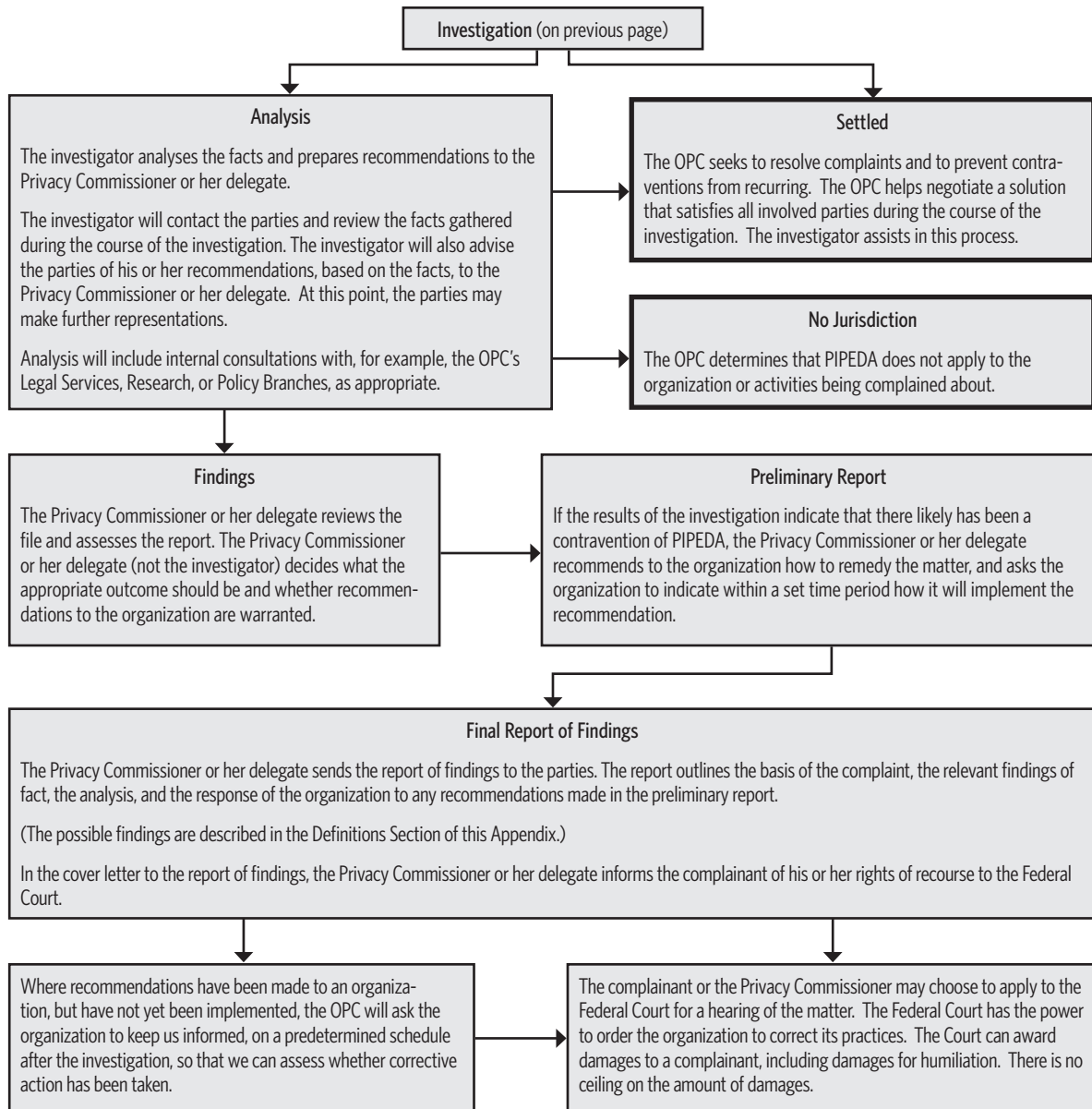
No report prepared pursuant to subsection 13(2). *Note: This disposition was used only for investigations ended prior to April 1, 2011, when subsection 13(2) of PIPEDA was repealed.* The Commissioner is not required to prepare a report if certain conditions are met: (a) the complainant ought first to exhaust grievance or review procedures otherwise reasonably available; (b) the complaint could more appropriately

be dealt with, initially or completely, by means of a procedure provided for under the laws of Canada or the laws of a province; (c) the length of time that has elapsed between the date when the subject-matter of the complaint arose and the date when the complaint was filed is such that a report would not serve a useful purpose; or (d) the complaint is trivial, frivolous or vexatious or is made in bad faith. If she does not prepare a report, the Commissioner informs the complainant and the organization and gives reasons.

Declined to investigate. *Note: This disposition was used only for complaints received after April 1, 2011, when the revised subsection 12(1) of PIPEDA came into effect.* The Commissioner declined to commence an investigation in respect of a complaint because she 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.

INVESTIGATION PROCESS





Appendix 2

PIPEDA INVESTIGATION STATISTICS FOR 2011

Note: Percentages in statistical charts do not always total 100 due to rounding.

Overall in 2011, our Office accepted 281 formal complaints, a 35 percent increase from 207 in 2010. This increase is likely linked to a variety of factors,

such as the increasing complexity of privacy issues faced by Canadians (leading to more becoming formal complaints), possible heightened awareness among Canadians of their privacy rights, or changes in how people interact with businesses in the increasingly digital economy.

Complaints Received by Industry Sector

Sector	2011		2010		2009	
	Count	Percentage	Count	Percentage	Count	Percentage
Financial	62	22%	45	22%	55	24%
Transportation	34	12%	13	6%	15	6%
Telecommunications	30	11%	19	9%	42*	18%
Services	28	10%	35	17%	9	4%
Insurance	25	9%	27	13%	41	18%
Accommodations	24	9%	6	3%	7	3%
Internet	18	6%	19	9%	—	—
Sales/Retail	16	6%	18	9%	25	11%
Entertainment	8	3%	2	1%	0	0%
Professionals	7	3%	6	3%	10	4%
Health	4	>1%	4	2%	8	3%
Other	25	9%	13	6%	19	8%
Total	281		207		231	

*In 2010, we began counting Internet complaints as a separate sector. Previously, Internet complaints were counted under the telecommunications sector.

Complaints related to the financial sector continued to account for the largest proportion of formal complaints we accepted, roughly one in five.

Complaints in the transportation sector jumped this year compared to previous years. We intend to follow this potential trend closely in the coming months.

Complaints in the insurance sector have declined over the last two years. This may be because in the last couple of years we have seen an increase in clarity and awareness of privacy rules in the insurance sector.

SECTOR DEFINITIONS:

- **Financial:** Banking, credit intermediation (i.e. credit card issuers, sales financing, consumer lending, loan brokers, financial transactions processing activities), financial investment and related activities, investment and financial planning, monetary authorities.
- **Services:** Civic and professional organizations, personal care services, repair and maintenance services, rewards programs, administrative and support services (includes collection agencies, credit bureaus), educational services, social assistance.
- **Internet:** Data processing, hosting and related services, Internet service providers, social networking, web search portals.
- **Insurance:** Insurance carriers (liability, life and health, property and casualty).
- **Sales/Retail:** Automotive dealers, building materials and suppliers dealers, direct marketing, electronic commerce, retail sales (in-store and online).
- **Professionals:** Accounting, tax preparation, bookkeeping and payroll services, legal services, other professional, scientific and technical services.
- **Transportation:** Air, rail, transit and ground passenger transport, trucks, water transport.
- **Telecommunication:** Mobile applications, satellite telecommunication carriers, telecommunications equipment, wired and wireless telecommunication carriers.
- **Accommodations:** Condominium corporations, cooperative housing, real estate, rental accommodations and traveller accommodations.
- **Health:** Physicians, dentists, pharmacies and other health practitioners
- **Entertainment:** Amusement, gambling and recreation industries and other entertainment services.
- **Other:** Includes manufacturing, agriculture, utilities, no jurisdiction, publishers (except Internet), food and beverage, and government entities under the jurisdiction of PIPEDA.

Complaints Received by Type of Complaint

Type	2011		2010		2009	
	Count	Percentage	Count	Percentage	Count	Percentage
Use and Disclosure	89	32%	56	27%	59	26%
Access	74	26%	50	24%	64	28%
Collection	57	20%	33	16%	33	14%
Consent	19	7%	30	14%	22	10%
Correction/ Notation	14	5%	1	>1%	1	>1%
Retention	10	4%	10	5%	3	1%
Safeguards	9	3%	13	6%	21	9%
Accountability	4	1%	—	—	—	—
Accuracy	3	1%	4	2%	9	4%
Challenging Compliance	1	>1%	2	1%	2	>1%
Fees	1	>1%	—	—	—	—
Openness	0	0%	3	1%	4	2%
Identifying Purposes	0	0%	2	1%	0	0%
Appropriate Purposes	0	0%	1	>1%	0	0%
Other	—	—	2	1%	13	6%
Total	281		207		231	

The use and disclosure of personal information, access to personal information, and collection of personal information were once again the top three issues raised in complaints to our Office.

Closed Complaints by Type of Complaint and Disposition

	Early Resolution	Not well-founded	No jurisdiction	Discontinued	Well Founded and Resolved	Well-founded	Resolved	Settled	Report not issued under 13(2)	Declined	Total	Percentage
Access	33	11	6	5	4	2	4	1	2	1	69	29%
Use and Disclosure	38	7	7	4	3	3	2	1	1	0	66	28%
Collection	23	5	4	5	3	2	1	1	0	0	44	19%
Consent	5	7	0	2	2	2	2	1	0	0	21	9%
Safeguards	8	2	1	1	1	1	3	0	0	0	17	7%
Retention	5	0	0	0	0	0	0	0	0	0	5	2%
Correction/Notation	4	0	0	0	0	0	0	1	0	0	5	2%
Accuracy	0	0	0	0	2	1	0	1	0	0	4	2%
Challenging Compliance	0	3	0	0	0	0	0	0	0	0	3	1%
Identifying purposes	0	0	0	0	0	1	0	0	0	0	1	>1%
Openness	0	0	0	0	0	1	0	0	0	0	1	>1%
Total	116	35	18	17	15	13	12	6	3	1	236	
Percentage	49%	15%	8%	7%	6%	6%	5%	3%	1%	>1%		

In 2011, we completed 125 early resolution files. We were able to reach a satisfactory conclusion in 116 of these cases. The remaining nine cases were transferred for formal investigation. We are pleased that we are maintaining an extremely high rate of successful resolution – over 90 percent.

We have significantly increased the number of complaints handled through this process – almost half of all formal complaints, up from about a quarter in 2010.

We also completed 120 investigations of complaints. The number of investigations concluded is significantly lower than in 2010, when we completed 249 investigations, as part of our two-year effort to clear a backlog of complaints.

Closed Complaints by Industry Sector and Disposition

	Early Resolved	Not well-founded	No Jurisdiction	Discontinued	Well-founded and Resolved	Well-founded	Resolved	Settled	Report not issued under 13(2)	Declined	Total	Percentage
Financial Sector	20	13	0	6	3	4	3	2	1	0	52	22%
Insurance	10	4	9	2	1	1	2	0	2	1	32	14%
Services	10	5	2	2	3	1	2	1	0	0	26	11%
Telecommunications	16	4	0	2	0	0	0	0	0	0	22	9%
Transportation	13	1	0	0	1	2	3	1	0	0	21	9%
Sales/Retail	11	2	1	0	5	0	1	0	0	0	20	8%
Internet	5	6	0	4	0	4	1	0	0	0	20	8%
Accommodations	10	0	0	0	2	0	0	0	0	0	12	5%
Professionals	4	0	3	0	0	0	0	0	0	0	7	3%
Health	3	0	0	0	0	0	0	0	0	0	3	1%
Entertainment	2	0	0	0	0	0	0	1	0	0	3	1%
Other	12	0	3	1	0	1	0	1	0	0	18	8%
Total	116	35	18	17	15	13	12	6	3	1	236	
Percentage	49%	15%	8%	7%	6%	6%	5%	3%	1%	>1%		

In a majority of investigations, we were able to find a satisfactory conclusion to issues. Only 6 percent of formal complaints ended up being deemed well founded (but not resolved), meaning we were not able to reach a conclusion that we found acceptable.

There was a significant decrease in the proportion of cases deemed either resolved, or well founded and resolved. These dropped by two-thirds, from 33 percent of all cases in 2010 to just 11 percent in 2011. This decrease was almost exactly offset by the increase in the proportion of cases settled through early resolution, which nearly doubled from 24 percent in 2010 to 49 percent in 2011.

In 2011, there was an increase in the number of complaints where we concluded that PIPEDA did not apply to the organization or activity that was the subject of the complaint – up to eight percent from two percent the previous year.

This jump is in part due to a 2010 Federal Court decision on the scope of application of PIPEDA where personal information is collected for the purpose of defending an insured individual against a tort claim arising from a motor vehicle accident. This led to a few complaints being closed because they had been received before this jurisdictional decision yet concerned activities over which the Court ruled PIPEDA does not apply.

TREATMENT TIMES

Average Treatment Times by Complaint and Resolution Types

Complaint Type	Early Resolution Cases		Formal Complaints	
	Number	Average Treatment Time in Months	Number	Average Treatment Time in Months
Access	33	2	36	17
Accuracy	0	—	4	18
Challenging Compliance	0	—	3	13
Collection	23	2	21	12
Consent	5	2	16	11
Correction/Notation	4	2	1	3
Identifying Purposes	0	—	1	12
Openness	0	—	1	21
Retention	5	2	0	—
Safeguards	8	3	9	19
Use and Disclosure	38	1	28	13
	Total 116	Weighted average* 2.0	Total 120	Weighted average* 14.3

*A weighted average is calculated by multiplying the number of cases of each type by the average treatment time for that type, totalling those numbers and dividing by the total number of cases. The weighted average provides a representative statistic of overall treatment times.

In 2011, with our backlog of complaints effectively eliminated, and with an increased use of early resolution, we were able to return to our 2008 staffing levels and still improve the timeliness of our investigations.

The average formal investigation time has dropped by several months to 14 months. Meanwhile, complaints resolved through early resolution were completed in an average of two months from complaint acceptance.

When combined, the average treatment time for all accepted complaints has dropped to slightly more than eight months. This is well below the 12-month requirement set out under PIPEDA.

Average Treatment Times by Disposition

Disposition	Number	Average Treatment Time in Months
Early resolution	116	2
Settled	6	6
Discontinued	17	7
Declined	1	3
No jurisdiction	18	23
Report not issued under 13(2)	3	23
Not well founded	35	14
Well founded resolved	15	15
Resolved	12	13
Well founded	13	16
Total	236	Weighted average 8.2

As signalled in the 2010 Annual Report, we are using a new definition of treatment time in this report. Treatment times here are measured from the date a complaint was *accepted* to when a finding is made or the case is otherwise disposed of. The date a complaint is accepted is the date we receive a *complete* complaint (i.e. one with enough information in it to begin an investigation).

Previously, we measured the treatment time from when a complaint was first received, not when it was complete enough to begin an investigation. However, this old definition led to artificially high treatment times when

complaints did not include all the information required in order to begin an investigation.

We were pleased that, in line with the Commissioner's priority of service delivery to Canadians, our average complaint treatment time in 2011 declined dramatically to 8.2 months.

For comparative purposes, if this year's treatment times were calculated the same way as last year's (from date received rather than date accepted) our average treatment time in 2011 would still be only 9.3 months, down from 15.6 months the previous year.

Voluntary Breach Notifications – By Industry Sector and Type of Incident

Sector	Breach Type					2011		2010	
	Accidental disclosure	Loss	Unauthorized access, use or disclosure	Total	Percentage	Total	Percentage	Total	Percentage
Financial	12	3	14	29	45%	29	45%	29	66%
Services	0	0	8	8	13%	8	13%	2	5%
Insurance	0	2	5	7	11%	7	11%	2	5%
Sales/Retail	2	0	3	5	8%	5	8%	1	2%
Telecommunications	1	0	2	3	5%	3	5%	2	5%
Internet	0	0	3	3	5%	3	5%	1	2%
Entertainment	1	0	1	2	3%	2	3%	2	5%
Accommodations	0	0	1	1	2%	1	2%	1	2%
Other	2	0	4	6	9%	6	9%	1	2%
Health	0	0	0	0	0%	0	0%	1	2%
Professionals	0	0	0	0	0%	0	0%	1	2%
Transportation	0	0	0	0	0%	0	0%	1	2%
Total	18	5	41	64		64		44	
Percentage	28%	8%	64%						

*As of 2011, incidents of theft of personal information are being reported under the category of unauthorized access, use or disclosure. This is being done because theft is a form of unauthorized access, and it is outside the scope of our Office to determine if an incident of unauthorized access is theft or not.

In 2011, 64 private-sector data breach incidents were voluntarily reported to us. While this is a 45 percent increase over the number of incidents reported to us in 2010, it is within the range of the last few years.

Breach notifications from the financial industry – the leading sector in routinely reporting breaches to us – remained steady at 29 incidents. By contrast,

breach notifications from all other sectors more than doubled from 15 in 2010 to 35 in 2011.

This suggests increased awareness about breach notification and its benefits has spread substantially beyond the financial sector to the broader Canadian private sector.

The profile of breach notification became greater in late 2010 and 2011 thanks to Alberta's introduction of mandatory breach notification and to the draft federal legislation to make breach notification to the Privacy Commissioner mandatory.

DATA BREACH TYPE DEFINITIONS:

Accidental disclosure: Incidents where an organization discloses personal information to unintended recipients by accident. For example, bank statements sent to the wrong address through mechanical or human error, or personal information made publicly available on an organization's website through a technical error.

Loss: Incidents where personal information is lost by an organization, usually through the loss of a laptop, CD or paper documents.

Unauthorized access, use or disclosure: Incidents where personal information is accessed, used or disclosed by someone without an organization's authorization. For example, a stolen laptop, an online hack of an organization's database, or an employee accessing or using personal information for unauthorized purposes.

