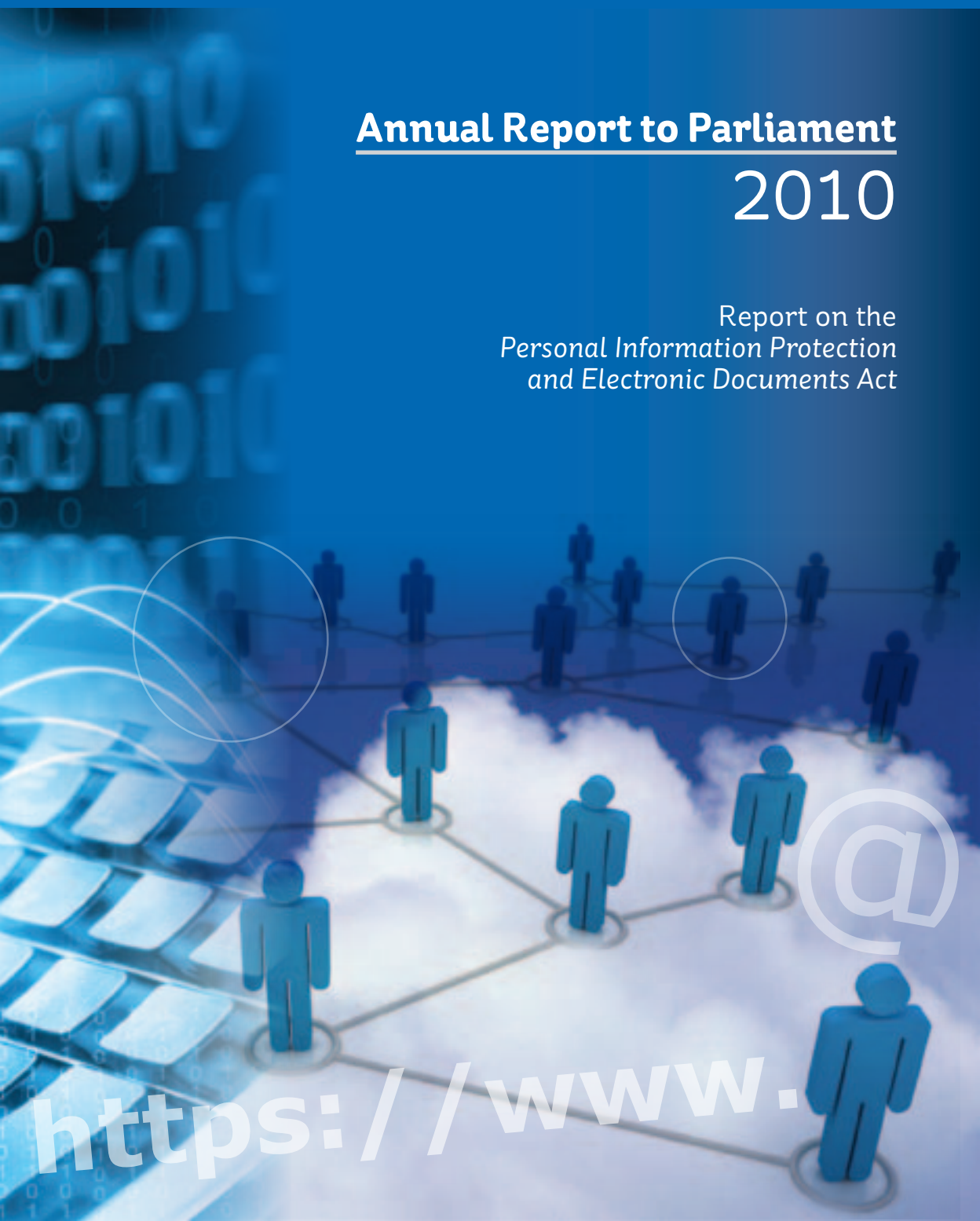
Office of the
Privacy Commissioner
of Canada

Privacy

Annual Report to Parliament
2010

Report on the
Personal Information Protection and Electronic Documents Act



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

Cat. No. IP51-1/2010E-PDF
ISBN 978-1-100-17832-5

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

Privacy Commissioner of Canada

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
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) 995-8210
Téléc. : (613) 947-6850
1-800-282-1376
www.priv.gc.ca

June 2011

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, 2010.

Yours sincerely,

Original signed by

Jennifer Stoddart
Privacy Commissioner of Canada

Privacy Commissioner of Canada

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
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) 995-8210
Téléc. : (613) 947-6850
1-800-282-1376
www.priv.gc.ca

June 2011

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, 2010.

Yours sincerely,

Original signed by

Jennifer Stoddart
Privacy Commissioner of Canada

TABLE OF CONTENTS

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. The Atlantic provinces, Ontario, Manitoba, Saskatchewan and the Territories are covered by PIPEDA.

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

Commissioner's Message

Protecting privacy rights is an increasingly complex challenge in the digital age, when more and more of daily life plays out on the Internet and our activities can so easily be tracked, stored, shared and analyzed.

The complex privacy issues of the online world were a major focus of our work in 2010.

As our social world shifts online, privacy safeguards have become critical. We were pleased to report in September that we were satisfied with how Facebook had implemented privacy improvements in response to our comprehensive investigation of the site.

Our investigation of Google's collection of sensitive personal data transmitted over unsecured wireless networks, meanwhile, showed the deficiencies in governance controls on privacy.

In the context of this complex, rapidly evolving environment, we heard questions being raised about whether privacy is evaporating in our current era of digital exhibitionism.

Of course, concepts of privacy *do* evolve over time and from generation to generation. However, it is clear to me that privacy continues to be a deeply cherished value – and we saw plenty of evidence of this in 2010.

"NEW SOCIAL NORM"

Early in the year, Mark Zuckerberg, the chief executive officer of Facebook, offered his view of privacy. He said:

> *People have really gotten comfortable, not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time. We view it as our role … to constantly be innovating and be updating what our system is, to reflect what the current social norms are.*

I don't disagree with the observation that social norms are changing. Privacy looks different today than it did a generation – or even a decade – ago. It is startling how people post the nitty-gritty of their intimate lives online.

But I also take heart in all the signs that people – including the biggest Internet users, youth – do, in fact, still care very much about privacy.

We see evidence of this whenever we go out to schools to talk with children and teens from Grades 4 to 12 about managing their online reputations. At the end of each presentation, young people ask questions that show how interested they are in privacy. They want to know how to manage who sees what in their online profiles. They want to know how they can see everything that others are posting about them. And they often ask how to permanently delete things – everything from items they wish they hadn't posted to old quiz information that they don't want on the Internet anymore.

Privacy remains an incredibly important and cherished value to Canadians – and to people around the world.

Those trying to convince us that privacy is out of fashion are consistently the people who stand to profit from its demise.

Personal information has become a valuable commodity. Companies make money from the use of personal information – it's no wonder that some would like us to believe that privacy doesn't matter.

I've even heard the question asked: "*Can we have both privacy and innovation?*"

The answer is a resounding *Yes*. Privacy does *not* stand in the way of innovation.

The pressure on privacy is *not* just the result of new social standards or new and captivating technologies. In the commercial sphere where PIPEDA applies, it chiefly comes from the fact that there is big money to be made in pushing the privacy boundaries.

PUSH BACK

But people are pushing back.

We've seen that with the two giants of the online world – Facebook and Google.

Facebook users spoke up – loudly – after the social networking site rolled out a series of changes that made it far more difficult for users to protect their privacy. The outcry had

an impact and Facebook scrambled to ratchet back some of its privacy modifications in order to quell the criticism.

Google, meanwhile, was also the target of a privacy backlash when it launched Google Buzz early in 2010.

The company took Gmail, which had been a private, web-based e-mail service, and abruptly melded it with a new social networking service. Google automatically assigned users a network of "followers" from among people with whom they corresponded most often on Gmail, without adequately informing those users about how this new service would work or providing sufficient information to permit informed consent.

There was a storm of protest by users around the world who were understandably concerned that their personal information was being disclosed.

The rollout of a product with such significant privacy flaws betrayed a disappointing disregard for fundamental privacy norms and laws. I was among a group of 10 international data protection authorities who jointly wrote to Google to remind it of the need to respect the laws of the countries in which they launch their products. That initiative was another sign of the continuing commitment to privacy protection right around the globe.

To its credit, Google quickly apologized to its users and introduced changes to address the widespread criticism.

PRIVACY STILL MATTERS

These two stories illustrate the fact that people *do* care.

Yes, many people – particularly young people – *are* willing to share more than we did in the past. But they want to do so on their own terms. They want to be able to control their personal information – and that just happens to be one of the basics of privacy law in Canada and many other countries.

Canadians clearly like many of the new services being offered online and they want to continue using them in order to connect with one another. More than half of Canadians are now on Facebook.

It's also clear, however, that people want a service that respects their privacy. This is what Canadians have told my Office in letters and telephone calls – and it is what I hear in my travels across the country.

I have a very strong sense that we *are* speaking on behalf of Canadians when we ask these big online companies to respect our laws.

PRIVACY ONLINE

Online privacy issues are an area of increasing focus for my Office, which is why we've chosen to make it a major theme in this year's annual report.

It's certainly an area full of challenges. The issues are often complex and highly technical. Websites seem to change every day, so a great deal of effort is required to keep up with what's happening. The online world that Canadians access for products and services is global – we're often dealing with organizations based outside the country.

There's no doubt that the digital world is raising monumental challenges for privacy rights. That means we need to work harder and smarter, not throw in the towel on privacy and "get over it" – as one tech titan famously stated a number of years ago.

There is a lot we *can* do in the face of new privacy risks stemming from technological change:

- We need to enforce our privacy laws and ensure they remain modern and relevant.

- We need even more cooperation between privacy authorities – we're far stronger when we speak with one voice.

- We, as a society, must ensure that our privacy literacy matches our online literacy because, at the moment, there's a gap.

MODERN LEGISLATION

Technologies are developing at an astonishing rate and these changes are raising interesting new questions and challenges from a legal perspective.

Are laws designed for a bricks and mortar world up to the task of protecting privacy in the online context? Do we need new laws? How do you deal with jurisdictional questions and enforcement when dealing with global online companies?

It is clear that our current regulatory framework for protecting the privacy rights of Canadians is being tested in the face of rapidly changing technologies.

It is critical that we ensure that we are constantly updating our laws to meet current and future challenges.

The architects of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) had the foresight to make the legislation technology neutral and also include a requirement for a Parliamentary review of the Act every five years.

The first review began in late 2006 and the next one is expected to start in 2011.

My Office has already begun laying some of the groundwork for the upcoming review.

We have commissioned a report on the effectiveness of our current ombuds model. As well, we held public consultations on the privacy issues related to both the online tracking, profiling and targeting of consumers by marketers and other businesses as well as cloud computing practices.

Both the report and our public consultations will help shape my Office's input during the next PIPEDA review.

The report was prepared by two noted legal scholars, Dean of Osgoode Hall Law School Lorne Sossin and Professor France Houle of the Université de Montréal. We asked them to examine the effectiveness of the ombuds model in protecting personal information in the private sector, particularly in light of changes in the technological, economic and legal context since PIPEDA was first enacted.

In their analysis, these authors suggest that the current ombuds model has had mixed success.

On the positive side, the authors take the view that my Office has succeeded in accomplishing important goals related to compliance by working with large industry sectors such as banking and insurance, building trust across the private sector, providing guidance on the interpretation and application of PIPEDA, responding to complaints, inquiries and concerns, raising awareness of PIPEDA and generally enhancing the profile of privacy issues.

However, they are also of the view that the ombuds model may be less effective in promoting compliance where small- and medium-sized businesses are concerned.

The professors have suggested, as an option going forward, that my Office could acquire targeted and limited power to make orders, including the ability to impose penalties such as fines. They also propose explicit guideline-making power, to assist with the fair and transparent implementation of new order-making powers.

My Office is assessing the authors' analysis, mapping it onto our experience under PIPEDA to date, and comparing it with our own views of the merits and effectiveness of the ombuds model. The authors' analysis will undoubtedly make a significant contribution to the public discourse on future evolutions of PIPEDA.

With our public consultations, meanwhile, we developed a deeper understanding of a couple of emerging technological trends that will have a significant impact on the privacy of Canadians.

The consultations were an historic first for us. We invited written comments, but also held a series of day-long panel discussions in Toronto, Montreal and Calgary, canvassing a broad range of views from business, government, academics, consumer associations and civil society.

As this annual report was being prepared, we were completing a final report on the consultations for publication in 2011.

As we begin thinking about recommendations for PIPEDA reform during the upcoming Parliamentary review, we are also looking forward to changes resulting from the last review.

They are contained in two bills – one that received Royal Assent in December 2010 and another that was before Parliament at the beginning of 2011.

The legislation that was still under consideration by Parliament would, among other things, amend PIPEDA to require organizations to notify my Office and affected individuals following significant data breaches. That would be a welcome change.

The bill that has passed is aimed at curbing the amount of damaging and deceptive electronic communications (spam messages) that circulate in Canada. In the year ahead, we look forward to taking on our enforcement responsibilities under this new anti-spam law.

This legislation amends PIPEDA to provide my Office greater discretion to refuse or discontinue complaints and to permit us to share information with our domestic and international counterparts. These two new discretionary powers apply to investigations generally, whether the matter involves spam or other privacy issues.

INCREASED COOPERATION

We must also work beyond our borders. Canada on its own cannot possibly tackle the plethora of privacy concerns cropping up across the World Wide Web.

There has also been a lot happening on the global stage. For example, we are taking part in a number of initiatives to develop an international privacy standard and we're a founding member of the new Global Privacy Enforcement Network.

We have also been involved in the privacy work of Asia-Pacific Economic Cooperation (APEC) and the Organisation for Economic Cooperation and Development (OECD), which in 2010 marked the 30th anniversary of its groundbreaking *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.

On a more informal level, in 2010 we saw an unprecedented collaboration of 10 data protection offices coming together to send a strong message to Google and other online companies about the need to respect privacy laws around the world when launching new products and services.

All of the authorities involved in that project recognized the need to – as much as possible – join forces to ensure our messages are heard.

PRIVACY LITERACY

Another key to online privacy is to find ways to build a better understanding of privacy issues on the part of both consumers and organizations.

Canada is a nation of early adopters when it comes to new technologies, with 80 percent of Canadians over the age of 16 now online. And while we are sophisticated when it comes to online literacy, I think our privacy literacy in the context of the digital world could be improved.

Many people don't know they're leaving a trail of digital bread crumbs when they click their way through websites and from website to website. They don't know that those crumbs are stored, analyzed and accessible. And they don't understand that this information may be used in ways they never imagined.

How many people actually read privacy policies? How knowledgeable are people about securing their home computers and networks?

The need for improved privacy literacy applies not only to individuals, but also to organizations. Businesses need to ensure that their employees are privacy literate; that they have knowledge of how personal information should be used and handled in the context of privacy values.

We're strong advocates for this kind of training, which can save an organization a lot of grief – and money. An employee who has spent time thinking and learning about

privacy is far less likely to leave a laptop containing personal information on the front seat of her car or to be cavalier about punching in a fax number when sending sensitive records.

Training – *ongoing* training – makes people stop and think about the need to protect personal information. It builds awareness that personal information should be private by default.

A recent poll conducted for my Office found that only 37 percent of businesses had provided privacy training for employees. We need to do better.

TORONTO OFFICE

The year 2010 marked a very exciting development in the history of the Office of the Privacy Commissioner of Canada: We opened our first office outside of the nation's capital.

Our new Toronto office creates an opportunity for a stronger presence for outreach and PIPEDA investigation work. A very large percentage of our complaints against private-sector organizations involve companies located in the Greater Toronto Area.

We expect that the Toronto office is going to lead to stronger, more effective relationships with our stakeholders there – and that's ultimately going to mean better privacy protection for Canadians.

A NEW MANDATE

At the end of 2010, I was honoured to be reappointed as Privacy Commissioner of Canada.

It has been a great privilege to serve Canadians and Parliament for the past seven years and I deeply appreciate that the Prime Minister and Parliament have confidence in me to continue on in this role. I look forward to the opportunity to build on what my Office has already accomplished.

I have been touched and gratified by the accolades that my Office has received for its work in recent years. While there are still improvements I would like to make to ensure that we are delivering the best possible service to Canadians, we have many achievements to be proud of.

The secret to these successes is the dedicated team of professionals at the Office of the Privacy Commissioner of Canada. They are a thoughtful, creative, passionate,

determined and tireless group that is always ready to meet the challenge of increasingly complex privacy issues.

Our Office has grown in recent years and we've been lucky to have some exceptionally talented and highly knowledgeable people join us.

This annual report is an opportunity to offer everyone in the Office my profound appreciation for all their outstanding work, which has a very positive impact on the day-to-day lives of people across the country.

In mid-2010, our Assistant Commissioner for PIPEDA, Elizabeth Denham, was appointed Information and Privacy Commissioner for British Columbia. While we miss her both on a professional and personal level in Ottawa, we are delighted that we now have another strong partner in British Columbia and the opportunity to continue working together on issues of mutual interest.

As a result of that appointment, Assistant Commissioner Chantal Bernier's responsibilities have been expanded and she is now responsible for both the *Privacy Act* – Canada's federal public sector privacy legislation – and PIPEDA. I am grateful to her for taking on such an enormous challenge and would like to publicly express my deep gratitude for her unfailing commitment and exceptional leadership in the Office.

There will be many new and ongoing privacy issues for our team to tackle together over the next three years. We still have many challenges before us, most notably, improving service to Canadians who reach out to our Office for help.

Protecting privacy in this rapidly transforming landscape demands agile and creative responses. This is what we will continue to strive to deliver on behalf of all Canadians.

Jennifer Stoddart
Privacy Commissioner of Canada

Privacy by the Numbers

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA IN 2010

PIPEDA inquiries received	4,793
PIPEDA early resolution complaints received	108
PIPEDA complaints received	99
PIPEDA investigations closed	249
Draft bills and legislation raising PIPEDA issues reviewed for privacy implications	13
Private-sector policies or initiatives reviewed (For example, a written analysis of a new technological application, or a paper on an industry practice to keep staff up to date on new developments.)	30
Policy guidance documents issued	14
Research papers issued	5
Parliamentary committee appearances	13
Other interactions with Parliamentarians or staff (For example, meeting with MPs or Senators.)	40
Speeches and presentations delivered	150
Contribution agreements signed	16
Visits to main Office website Visits to Office blogs and other websites (including OPC blog, youth blog, youth website, deep packet inspection website and YouTube channel) Total	2,349,741 1,124,258 3,473,999
"Tweets" sent	700
Publications distributed	15,478
Media interviews	250
News releases	42

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

CHAPTER 1

The Privacy Landscape
Key Accomplishments in 2010

1.1 Serving Canadians

PUBLIC INQUIRIES

Canadians phoned or wrote to our Office more than 9,200 times during 2010. Approximately half of those calls and letters involved a matter related to privacy issues in the private sector covered by PIPEDA. Other inquiries related to the *Privacy Act*, which applies to the federal public sector, or involved another jurisdiction or issues not exclusive to either of the Acts we enforce.

On the PIPEDA side, we continued to see a growing number of inquiries related to online issues.

For more information, see section 4.1

PUBLIC COMPLAINTS

Largely as a result of our strengthened efforts to resolve issues more rapidly at the front end, the number of formal complaints registered with our Office dropped significantly.

We received 108 early resolution complaints and 99 formal investigation complaints related to the private sector, for a total of 207 complaints. That compares with 231 formal complaints received in 2009.

As described in section 4, we have been extremely successful in our efforts to help individuals and organizations try to resolve issues before they become formal complaints.

In particular, we have established a formal early resolution process, which has quickly become an important tool for addressing issues in a timely manner. In some cases, an issue that would have taken months to resolve through the official complaint investigation process is now concluded in a matter of days.

In most early resolution cases, we were able to reach a satisfactory resolution without opening a formal investigation.

COMPLAINT INVESTIGATIONS

We closed 249 complaints relating to the private sector in 2010.

Online issues continued to play a major factor in our investigation work. In 2010, we worked on privacy issues related to major online players such as Facebook and Google. We also investigated the popular online dating site, eHarmony.

We've made online issues a special focus of this year's annual report. Summaries of our complaint investigations involving the online world are included in section 2.

Information on our other complaints investigation work is provided in section 4.

PUBLIC AWARENESS

The Commissioner, Assistant Commissioners and other officials from our Office delivered 150 speeches and presentations, many of them on private-sector privacy issues, during the course of 2010.

We were also asked to provide comment for dozens of media stories – many of them related to privacy issues cropping up in the online world.

Our paper publications continue to be in high demand – we distributed 15,478 copies of our pamphlets, brochures and guides at conferences and upon request from organizations and individuals during the year.

Meanwhile, the number of visits to our website soared by 36 percent from the previous year.

We continue to put a special focus on online youth privacy, with websites designed for young people and a popular school presentations program. In 2010, we also supported the first annual PrivacyCampTO, a conference on digital privacy.

For more information on our public awareness initiatives, please see section 5.

1.2 Supporting Parliament

APPEARANCES BEFORE MPS AND SENATORS

During 2010, our Commissioner, Assistant Commissioners and other officials of the Office made 13 formal Parliamentary committee appearances.

In October, for example, we appeared before the House of Commons Standing Committee on Access to Information, Privacy and Ethics concerning its study on the privacy implications of street-level imaging applications.

Google's Street View imaging cars had collected payload data from unsecured wireless networks. We initiated our own investigation into this matter.

We were pleased that the Committee took such an interest in the personal information handling practices of Google and the protection of Canadians' privacy. In our testimony, we continued to stress the importance of ensuring that privacy remains a key consideration as any organization develops new products and services involving the use of personal information.

In January 2011, the Committee issued its report, saying it was satisfied that the privacy concerns of Canadians with regard to street-level imaging technology are being taken seriously by all parties involved.

The Committee said it was reassured that our Office continues to monitor developments to ensure compliance with Canadian law. For its part, the Committee said it would also continue to monitor the issue and revisit the matter if necessary.

In its report, the Committee stated: "(T)echnology innovators need to ensure that privacy protection is a core consideration at the development stage of any new project. Potential privacy risks should be identified and eliminated or reduced at the onset of new projects and not be left to be addressed as costly afterthoughts."

The issue of national security – sometimes in a context that involves the private sector – continued to be a subject of dialogue between our Office and parliamentary committees.

For example, in November, we appeared before the House of Commons Standing Committee on Transport, Infrastructure and Communities on Bill C-42, *An Act to amend the Aeronautics Act.* The bill – prompted by the requirements of the U.S. Secure Flight program – would allow the sharing of personal information between Canadian airlines and U.S. authorities when an aircraft flies over, but does not land in, the United States.

While we understand that U.S. sovereignty extends to its airspace, we felt it was important to express our concerns about the potential consequences of the U.S. Secure Flight program for the privacy of Canadian travellers.

In our testimony, we noted that the Canadian government has an important role to play in working with the U.S. government and Canadian airlines to minimize the impact of Secure Flight. We proposed that the government ensure that the minimum amount of personal information is disclosed, that it question retention periods, and also negotiate robust and accessible redress mechanisms.

We also made presentations at other committee hearings, including:

- Senate Standing Committee on Social Affairs, Science and Technology on Bill C-36, the *Canada Consumer Product Safety Act* - November 25, 2010.

- House of Commons Standing Committee on Access to Information, Privacy and Ethics on the the 2009 Annual Report to Parliament on PIPEDA and the 2009-2010 Annual Report to Parliament on the *Privacy Act* - October 19, 2010.

- House of Commons Standing Committee on Transport, Infrastructure and Communities on aviation safety and security - May 11, 2010.

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

REVIEWS OF DRAFT BILLS AND LEGISLATION WITH POTENTIAL PRIVACY IMPLICATIONS

Meanwhile, we examined a total of 27 bills introduced in Parliament in order to consider potential privacy implications. Roughly half of those involved issues related to the private sector.

These included the following bills:

- C-22 - *An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service*.

- C-28 - *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of*

carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act.

- C-29 - *An Act to amend the Personal Information Protection and Electronic Documents Act. (Safeguarding Canadians' Personal Information Act.)*
- C-32 - *An Act to amend the Copyright Act. (Copyright Modernization Act.)*
- C-36 - *An Act respecting the safety of consumer products. (Canada Consumer Product Safety Act.)*
- C-42 - *An Act to amend the Aeronautics Act. (Strengthening Aviation Security Act.)*
- C-50 - *An Act to amend the Criminal Code. (Improving Access to Investigative Tools for Serious Crimes Act.)*
- C-51 - *An Act to amend the Criminal Code, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act. (Investigative Powers for the 21st Century Act.)*
- C-52 - *An Act regulating telecommunications facilities to support investigations. (Investigating and Preventing Criminal Electronic Communications Act.)*

LEGISLATIVE RENEWAL

In an environment where privacy issues are constantly evolving in the face of new technologies, it is critical to ensure that PIPEDA remains up to the task of protecting Canadians' privacy rights.

Fortunately, PIPEDA (unlike the *Privacy Act*) requires review by Parliament every five years.

As a result of the first review, a number of amendments to PIPEDA were introduced in Parliament as part of two separate bills.

One of those pieces of legislation – a bill to fight electronic spam – received Royal Assent at the end of 2010 and will bring about important changes for my Office.

The aim of the legislation is to deter the most damaging and deceptive forms of spam and to help drive spammers out of Canada and stop them from preying on Canadians from abroad. Our Office will have a role in enforcement along with the Canadian Radio-television and Telecommunications Commission (CRTC) and the federal Competition Bureau.

Included in the legislation are amendments providing our Office with a greater ability to share information with our international and provincial counterparts.

The same legislation also amended PIPEDA to provide the Privacy Commissioner with discretion to refuse or discontinue complaints. This is a welcome amendment which will help us target our limited resources to the most strategic issues for Canadians.

Going forward, we could decide not to accept a complaint if the complainant has not exhausted other available grievance or review procedures; if the complaint could be more appropriately dealt with under other federal or provincial laws; or if the complaint was not filed within a reasonable period of time.

Other amendments would provide the discretion to discontinue investigations. We could stop an investigation if, for example, there is insufficient evidence; the complaint is trivial or made in bad faith; the organization has provided a reasonable response; or the matter is already under investigation or has been investigated before.

We are required to provide the complainant and the respondent organization reasons for the refusal or the discontinuation.

Further proposed amendments to PIPEDA are included in the *Safeguarding Canadians' Personal Information Act*, which was still before Parliament at the end of 2010.

That Act called for, among other changes, new requirements for organizations covered by PIPEDA to notify the Privacy Commissioner and affected individuals following serious data breaches.

The creation of a mandatory data breach notification regime would be an extremely welcome step for privacy protection in Canada. We are lagging behind many other jurisdictions, which already have breach reporting requirements in place.

Consumers should have the right to know if the personal information they entrust to an organization is disclosed without authorization, if there is a substantial risk of significant harm to their pocketbook or their reputation, business or employment opportunities, or creditworthiness.

Our Office would also be in a better position to ensure that all steps are taken to correct or mitigate the damage. And, over time, we would also be alerted to patterns and trends that require special attention so that the personal information of Canadians continues to be protected.

In 2010, our Office began preparing for the next review of PIPEDA, expected to begin in 2011.

We commissioned a report on the effectiveness of our current ombudsman model. As well, we held public consultations on the privacy issues related to both the online tracking, profiling and targeting of consumers by marketers and other businesses and cloud computing practices.

Both the report and the consultations will help inform our input during the upcoming review of PIPEDA.

Further information about our public consultations is included in section 2.

1.3 Supporting Organizations

RAISING AWARENESS

In the fall of 2010, we officially opened an office in Toronto. Investigations concerning respondents in the Greater Toronto Area will be conducted from the new office and we will use our presence there to increase our engagement with businesses, industry associations and other stakeholders in the region. Our purpose is to enhance compliance with PIPEDA in the private sector through partnerships and education.

We also launched an enhanced online tool to help businesses protect their customers' privacy. The tool helps businesses figure out how much information they should have about their customers and how to protect it.

Further information about our efforts to raise organizations' awareness of privacy issues can be found in section 5.

AUDIT

One way in which we support compliance with privacy law by private-sector organizations is through verifying, through our Office's audit function, that they have the policies, procedures and controls in place to safeguard the privacy and personal information of their customers.

In 2010, we conducted an audit of Staples Inc. Following previous complaints about breaches involving returned electronic data storage devices and considering the potential

impact on consumers, we decided to examine the retailer's personal information handling practices and procedures.

The audit, described in detail in section 3 of this report, showed that, while Staples generally has good privacy practices, the management of returned data storage devices is an area that is yet to be fully addressed. In 15 of the 17 stores audited, we found devices that were resealed and verified as wiped of consumer information when such was not the case; devices that were not verified by a manager prior to being restocked; or devices that were sent directly to a return to vendor bin without being wiped of consumer information.

We made a series of recommendations to Staples to help ensure it is meeting its obligations under PIPEDA.

1.4 Advancing Knowledge

CONSULTATIONS

In the spring of 2010, we held public consultations on online tracking, profiling and targeting and cloud computing. We received numerous written submissions and held three public events in Toronto, Montreal and Calgary. The goal of the consultations was to learn more about certain industry practices, explore their privacy implications, and find out what privacy protections Canadians expect with respect to these practices. The consultations were also intended to inform the next legislative review process for PIPEDA.

We prepared a draft report that summarizes what we heard, what our views are, and how we see the road forward and published it for public comment. We will prepare a final report for publication in 2011.

RESEARCH

Research has become increasingly important in a world where complex technologies are raising new risks for privacy. Over the last couple of years, we have concentrated more resources on identifying and understanding the technological challenges to privacy.

In early 2010, we hired two highly qualified computer scientists and began equipping an internal lab to support their work. This investment supports two goals: building our in-house capacity to research developing technologies, and supporting investigations with a significant technological component.

We are continuing to expand the staff and equipment dedicated to this important function.

CONTRIBUTIONS PROGRAM

Our Contributions Program continues to provide funding for cutting-edge research and public education in privacy promotion and protection. The program has provided over $2 million to more than 60 initiatives across the country since it was created in 2004.

In 2010, 16 projects received funding. Recipients are advancing research in a number of key areas of interest to the Office, including:

- Targeted online advertising;
- Data-sharing between governments and commercial organizations through national security programs at the border and at airports;
- Video surveillance in public spaces by commercial organizations; and
- The privacy implications of patient websites, online health record databases and other "Health 2.0" tools.

In the area of public education, the program is providing funding for projects aimed at informing Canadians on issues relating to credit ratings and privacy, and the impact of new information technologies on consumer privacy rights and protection.

EMPLOYEE TRAINING

In response to the rapidly changing privacy landscape, our Office recognizes the importance of supporting training in the areas of leadership, management and specialist areas such as information technology and audit and investigation techniques. These competencies and specialized knowledge are required for achieving our mandate. In light of these requirements, we engage in activities to attract, develop and retain people with the aptitude and abilities to meet current and future organizational needs.

1.5 Global Initiatives

Privacy enforcement authorities worldwide are facing a similar challenge: How best to protect personal information that is constantly in motion across multiple jurisdictions.

Data protection authorities are increasingly recognizing that they cannot rely solely on national laws to protect data that doesn't recognize borders. In 2010, we saw some important first steps towards establishing international cooperation frameworks.

GLOBAL PRIVACY ENFORCEMENT NETWORK

Representatives from several privacy enforcement authorities came together at a meeting hosted by the Organisation for Economic Cooperation and Development (OECD) to launch the Global Privacy Enforcement Network (GPEN).

Our Office was one of the founding members. By the end of 2010, GPEN had more than 20 members on four continents.

GPEN is an informal network of privacy enforcement authorities that is intended to promote enforcement cooperation by sharing information about privacy enforcement issues and facilitating effective cross-border privacy enforcement in specific matters.

GPEN is an outcome of a 2007 recommendation of the OECD Council that called for the creation of a network of enforcement authorities. The recommendation was developed with the assistance of a volunteer group chaired by Commissioner Stoddart.

ASIA-PACIFIC ECONOMIC COOPERATION (APEC)

The Asia-Pacific Economic Cooperation (APEC) Cross-border Privacy Enforcement Arrangement became operational in July 2010. Our Office helped develop the Arrangement and we are a participant along with the U.S. Federal Trade Commission and privacy commissioners from Australia, Hong Kong and New Zealand.

Like GPEN, the APEC Arrangement is intended to encourage information sharing but it is limited to enforcement authorities in the Asia-Pacific region and it is focused on more formal cross-border cooperation through parallel or joint investigations and enforcement actions.

SHARING INFORMATION WITH GLOBAL COUNTERPARTS

Effective enforcement requires being able to share information with other data protection agencies. Our ability to share information has been severely restricted but this has changed as a result of the passage of amendments to PIPEDA contained in anti-spam legislation which received Royal Assent in December 2010.

The amendments will give the Commissioner clear authority to collaborate and exchange information with foreign counterparts that have similar functions and duties, as well as with our provincial colleagues.

The information-sharing provisions in the new legislation strike a careful balance. We will only be able to share information under a written arrangement that limits the information to be disclosed and restricts how it can be used. The Commissioner will also be able to enter into arrangements to engage in other activities such as developing standards, conducting joint research and participating in staff exchanges.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD)

The Organisation for Economic Co-operation and Development (OECD) has been a key player in developing global solutions to privacy and security issues. The efforts of the OECD Working Party on Information Security and Privacy are aimed at ensuring that the global flows of information are adequately protected and fostering cooperation among enforcement authorities.

The OECD *Guidelines on the Protection of Privacy and Transborder Data Flows* celebrated their 30th anniversary in 2010. PIPEDA incorporates the Canadian Standards Association Model Code, which was largely based on the OECD Guidelines.

To mark the anniversary, the OECD held three special events. The first covered the development of the Privacy Guidelines, their impact in various countries, and the Guidelines in the current privacy environment. The second event was held in Jerusalem, in advance of the International Conference of Data Protection and Privacy Commissioners, and addressed the evolving role of the individual in data protection. The third event concerned the economics of personal data and privacy.

Commissioner Stoddart heads a volunteer group that helped plan the events. Our Office also seconded a staff member to the OECD to help draft a discussion paper describing the new privacy environment and identifying the challenges to protecting personal information in the 21st century. This paper, which is expected to be made public in 2011, is intended to serve as a background document for further discussion about how well the Guidelines are meeting current challenges.

The OPC, which works closely with the Government of Canada representative, Industry Canada, will continue to support the important work of the OECD, as it moves forward with an assessment of the Guidelines.

IBERO-AMERICAN DATA PROTECTION NETWORK

We have also intensified our relationship with the Ibero-American Data Protection Network. The network was created to foster the exchange of information among Ibero-American countries.

In September, Assistant Commissioner Bernier delivered the keynote address on Canada's experiences during the first 10 years PIPEDA has been in force to the eighth Ibero-American Data Protection Meeting in Mexico.

Our Office closely followed the process leading up to the adoption of Mexico's new private-sector privacy law, *Ley Federal de Protección de Datos Personales en Posesión de Particulares,* which was greatly inspired by PIPEDA.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION

The International Organization for Standardization, better known as the International Standards Organization or ISO, is a key player in the development of privacy-related standards for the use and deployment of new and existing technologies.

ISO's sub-committee on Information Technology Security – and, in particular, its working group on Identity Management and Privacy Technology – is a focal point for the development of privacy-related standards, including a Privacy Framework standard and a Privacy Reference Architecture standard.

A senior member of our Office acts as the Canadian Head of Delegation and national expert to this working group, as well as acting as the liaison officer from the International Conference of Data Protection and Privacy Commissioners to the working group. In addition to this role, he represents Canada on a high-level Privacy Steering Committee. This committee is working on a broad range of issues related to privacy terminology and privacy-related initiatives underway within ISO. It also organized the first international privacy standards conference, which was held in Germany in October 2010. The goal of the conference was to foster information sharing and coordination amongst ISO technical committees engaged in privacy standards work and other important stakeholders such as the OECD, APEC and international data protection commissioners.

FRANCOPHONIE

Our involvement with the *Association francophone des autorités de protection des données personelles* (AFAPDP) continues to be an important focus of our international activities. The AFAPDP is the organization representing francophone data protection authorities around the world, and our Office was instrumental in its creation in 2007.

In 2010, Assistant Commissioner Chantal Bernier attended the association's annual meeting in Paris, where she made two presentations. She discussed our Office's experience with respect to new technological threats to privacy, notably in the online world, as well as the deployment of millimetre wave body scanners in Canadian airports. As well, she provided an overview of our Office as part of a discussion on best practices in data protection offices in francophone countries.

In future years, the AFAPDP plans to provide increased support to developing countries in the Francophonie as they establish new legislative frameworks to protect the privacy rights of their citizens. Our Office will strongly support these efforts.

" AND NOW, FOR MY NEXT TRICK, I WILL GUESS YOUR NAME, ADDRESS, DATE OF BIRTH, BANK ACCOUNT BALANCE AND WHERE YOU HAVE THAT SPECIAL TATTOO! "

CHAPTER 2

Key Issue
Privacy in the Online World

More than four of every five Canadians are now logging on to the Internet, the vast majority of them every day. They check the weather, arrange travel, chase after romance, shop, pay bills and taxes, watch videos, play games, hunt for information on products and services, and interact with friends, family and complete strangers.

The Internet is many things to many people: Convenient, comforting and familiar for some; a frustrating puzzle for others.

But what unites them all is that their online activities leave an unbroken trail of data.

Former Privacy Commissioner Bruce Phillips presciently raised concerns about this trail in his 1995-1996 annual report to Parliament, asking: "Nothing to hide? It's just as well...from the time we get up in the morning until we climb into bed at night we leave a trail of data behind us for others to collect, merge, analyze, massage and even sell – often without our knowledge or consent."

Since then, the trail has only widened. It not only tells others where we have been and what we were doing; increasingly, it is being used to define who we are.

Over time, our online trail crystallizes into a highly detailed digital dossier that is of extraordinary interest to a whole lot of other people and organizations.

Governments, with an eye to public safety, troll the Internet for potential evil-doers.

Scammers and schemers see opportunities adorned with dollar signs.

Meanwhile, legitimate businesses are anxious to know what Canadians are up to online, in order to lure them with targeted ads and offers and to invest their marking budgets

wisely. This can be welcome for people open to relevant information tailored to their interests. It can be intrusive for those who want to be left alone.

We live in what some have dubbed the era of "big data" – a global digital economy fuelled by massive international flows of data.

With advances in information and communication technologies and falling transmission and storage costs, these everyday transactions often result in multi-point transborder data flows.

Credit card purchases we make in another country using a card issued by a Canadian bank may be processed in a third country and data mined in a fourth jurisdiction.

With cloud computing, a Canadian-based company may use a web-based service provided by an American company to process and store personal information in multiple locations worldwide. This information, in turn, can be accessed by the Canadian company's employees from any place in the world where a network connection is available.

The Internet, and technology in general, are evolving at a breakneck pace.

This rapid change, combined with the global nature of the issues and the fact that organizations and individuals are still struggling to develop the appropriate rules of engagement, make the task of protecting privacy in this still relatively new environment a significant challenge.

Our approach has been to address the privacy issues of the online world with tools such as investigations, research, outreach to business, public education and collaboration with international partners.

In 2010, we conducted several investigations into the privacy practices of online organizations.

Social media networks, which some research suggests now link together more than half of all Canadian Internet users, were of particularly pressing interest to our Office.

In 2010, we followed up on our landmark investigation of the world's premier social network, Facebook, which we describe in section 2.1.

With Canadians increasingly likely to meet their romantic matches online, it's no surprise that we also found ourselves investigating an Internet dating site – eHarmony.

We also investigated the U.S.-based Internet giant Google.

Specifically, we investigated Google's collection of Wi-Fi data by vehicles gathering information for its Street View mapping function and found that the company had violated Canadian privacy law. We also publicly chastised Google for launching its Buzz social networking service without adequate regard for the privacy rights of its Gmail users.

Our message to all tech titans was clear: Think about privacy before you launch a new application; don't just leave it to luck and the lawyers.

Through a groundbreaking series of consumer consultations last spring, we sought to get a handle on the privacy implications of certain emerging technologies, including cloud computing and the online tracking, profiling and targeting of consumers by marketers and other businesses.

Our consultations zeroed in on the privacy issues specific to children and youth, who are the most avid users of the Internet, especially social networking sites.

We also explored the issues in detail in our outreach activities involving schools. And we convened an advisory panel of teens from across the country to share their perspectives on digital privacy.

The Internet's implications for privacy preoccupied us in other ways in 2010 as well. For example, in conjunction with a Government of Canada consultation paper on a Digital Economy Strategy for Canada, we reflected on the importance of digital literacy in helping people safeguard their privacy and anonymity online.

At the same time, we welcomed the passage of much-needed legislation to curb spam, bulk text messages and other forms of unwanted electronic communication. Spam carries threats such as spyware, malware and phishing attacks, thus undermining consumer confidence in the online economy. The new law, which received Royal Assent in December, gives our Office an enforcement role shared with the Canadian Radio-television and Telecommunications Commission (CRTC) and the Competition Bureau.

It also makes some key amendments to PIPEDA. Notably, it gives the Privacy Commissioner greater discretion over which complaints to investigate, allowing us to focus on more complex or systemic issues. The Commissioner also gains more explicit authority to share information with other enforcement authorities, both within Canada and abroad.

In short, 2010 was a busy year for online privacy issues. The following describes some of the highlights of our activities in this area:

2.1 Facebook Follow-up

In the fall, our Office announced that we had completed a review of the changes that Facebook implemented as a result of our investigation of the site, and had concluded that the issues raised in the original complaint had been resolved to our satisfaction.

In a statement, Commissioner Stoddart said: "The changes Facebook has put in place in response to concerns we raised as part of our investigation last year are reasonable and meet the expectations set out under Canadian privacy law."

The investigation, prompted by a complaint by the Canadian Internet Policy and Public Interest Clinic, a public advocacy group, resulted in significant change.

A major concern during the investigation was that third-party developers of games and other applications on the site had virtually unrestricted access to Facebook users' personal information.

In response to our recommendations, Facebook rolled out a permissions model that is a vast improvement. Applications must now inform users of the categories of data they require to run, and to seek consent to access and use this data. As well, technical controls ensure that applications can only access user information that they specifically request.

Other changes provide users with clear information about Facebook's privacy practices. The site developed simplified privacy settings and implemented a tool that allows users to apply a privacy setting to each photo or comment they post.

While we have closed the file on our original comprehensive investigation of Facebook, we have received further complaints about new issues. For example, we received complaints dealing with Facebook's invitation feature and Facebook "Like" buttons on other websites. Those issues were still under investigation as we prepared this annual report.

FACEBOOK TIMELINE
May 2008 – Canadian Internet Policy and Public Interest Clinic files complaint.
July 2009 – Privacy Commissioner announces her investigation has identified a number of privacy concerns related to the Facebook site and that some of those issues remain unresolved. She asks Facebook to respond to those concerns within 30 days.
August 2009 – Facebook agrees to make a series of changes in order to address the Commissioner's concerns. Facebook and the Commissioner's Office set a one-year timetable for implementing these changes.
September 2010 – Privacy Commissioner announces that her review of the changes Facebook has implemented as a result of her investigation is complete and that the issues have been resolved to her satisfaction.
Current: Investigations into further complaints against Facebook are ongoing at the time of writing this report.

2.2 eHarmony Investigation

Finding love and romance in the 21st century increasingly involves sitting in front of a computer screen.

The popularity of online dating sites has soared in recent years, joining introductions from friends and chance encounters in bars as one of the most common ways in which couples first meet. According to a statistic in the *Harper's* magazine Index, the chance that an American couple who met since 2007 first met online is now *one in four*.

Meanwhile, the online dating industry's revenues have been estimated at between $3 billion to $4 billion a year worldwide.

"It does seem to have displaced all other forms of dating…. I would say that it's been in the last five years that it's become hyper-mainstream," Susan Frohlick, a University of Manitoba cultural anthropologist who has studied online dating, told the *Washington Post* in 2010.

Protecting privacy in the context of online dating sites – where so many people post so much personal information – has also become a mainstream issue.

It is in this context that we completed our first investigation of an online dating site's privacy practices and policies in 2010.

eHarmony is a popular U.S.-based online dating site, which operates in Canada as eHarmony.ca.

To join the site, individuals must provide a substantial amount of highly personal information by completing a "comprehensive relationship questionnaire." It includes more than 300 questions about everything from character, intellect, family background and income, to physical appearance and sexual vitality.

COMPLAINT

A woman who had been a member of eHarmony complained to our Office that, upon ending her membership, she had asked eHarmony to delete her online account.

Days later, she went online to check that her instructions had been carried out. She discovered, however, that she could still sign in and that the account contained all the personal information she had previously provided.

She contacted eHarmony on several further occasions to repeat her request. According to the complainant, eHarmony replied that her account was now inaccessible to other members.

However, eHarmony told her that it could not entirely delete her record of having joined, or remove her personal information.

Dissatisfied with the response, she filed a complaint with our Office.

INVESTIGATION

When the complainant requested that the site "delete" her profile, she expected that her account and all her personal information would be permanently erased from eHarmony's servers.

In response to her request, however, eHarmony initially "closed" – or deactivated – her profile, making it inaccessible to prospective matches.

The complainant quickly told eHarmony that this was not what she wanted. At that point, she learned from eHarmony that it did not permanently delete members' personal information.

Our investigation found that the option to "close" an account was not readily accessible on the eHarmony website. Nor was there a clear explanation of what eHarmony meant by that term.

Moreover, there was no clear and separate permanent "deletion" option.

eHarmony stated that it "anonymizes" the information in the closed accounts – as it eventually did in the complainant's case, but did not explain under what circumstances it did so.

DATA RETENTION

PIPEDA requires that organizations develop guidelines and procedures with respect to the retention of personal information, as well as maximum and minimum retention periods. Under the law, eHarmony is allowed to retain personal information only for as long as necessary for the fulfillment of the purposes for which it was collected.

eHarmony stated that the reason it deactivated accounts and indefinitely retained the data – as opposed to deleting the accounts and the information in them – is that 40 percent of members reactivate within a two-year period. If the data is retained, individuals seeking to re-subscribe are not inconvenienced by the time-consuming task of completing a new questionnaire.

RECOMMENDATIONS

In our view, eHarmony should give users who decide to terminate their accounts a clear choice between account deactivation (temporary) and account deletion (permanent).

Further, it should make the distinction clear in its privacy policy.

During our investigation, we noted that if 40 percent of members tend to reactivate dormant accounts, then a majority – 60 percent – do *not*. Thus, they would not benefit from the indefinite retention of their information.

Therefore, we recommended that eHarmony:

- Develop, implement and inform users about a retention policy through which personal information in deactivated accounts will be deleted from eHarmony's servers, erased or anonymized after a reasonable length of time;

- Include an account deletion option; and

- Explain to users on their member account pages how account deletion is distinct from account deactivation, making both options clear and easily accessible. An explanation of the difference between account deletion and account deactivation should also be written into the general privacy policy.

RESPONSE

In its response, eHarmony confirmed that it had taken, or was in the process of taking, steps to address our concerns, including:

- Establishing a two-year retention period for personal information that the site collects from the users of its service;

- Providing a clear and efficient process for users to request removal of their personal information; and

- Providing users with clear information about the difference between deactivating an account and deleting an account as well as information about how long eHarmony retains personal information.

eHarmony also explained to our Office how and when it anonymizes users' data, which, in effect, permanently and irreversibly strips all personally idenfiable data from user accounts. eHarmony confirmed that the complainant's account had been anonymized in this manner and the information was rendered permanently depersonalized.

eHarmony also advised our Office that it has revised and improved its procedures for responding to privacy requests.

CONCLUSION

Given that eHarmony now offers users a clear option of completely deleting their accounts before the end of two years, we concluded that a default retention period of two years for inactive accounts is acceptable.

Ultimately, we were satisfied with eHarmony's responses. In addition to establishing a set retention policy, it has made its privacy controls clearer to users and improved processes for dealing with privacy concerns. Accordingly, the complaint was considered well founded and resolved.

OTHER OBSERVATIONS

Concerns about privacy policies and practices related to the use, retention and disposal of personal information by online dating sites are by no means confined to eHarmony.

A quick scan of other sites reveals that some do not even have privacy policies. Some that have privacy policies do not specify how they handle personal information after a user is no longer active on the site.

Unless a site deliberately clears out personal data that is no longer required to support the user's dating efforts, the information will remain on the servers. This introduces the risk of a data breach.

We urge users of any social networking site – and especially dating sites because of all the highly personal information collected there – to take steps to safeguard their privacy. For instance, users should:

- Make sure the site has a privacy policy and read the policy before signing up. The policy should be in clear and easy-to-understand language. It should state what types of personal information the site collects, how it is used, and how it will be protected.

- Check whether the site allows users to delete their profiles, and whether the deletion can be made permanent. Some sites allow users to "close" their account, but this merely deactivates it so it is not returned in a public search. The personal information remains intact on the database, possibly indefinitely.

- Check whether the site has a policy governing how long it retains personal information, and whether, when and how it deletes it. Some, for example, may only anonymize the data after a set period.

2.3 Google Wi-Fi

In October 2010, our Office published the results of an investigation into Google Inc.'s collection of highly sensitive data from unsecured wireless networks.

We found that the incident, in which Google Street View cars inappropriately collected personal information such as e-mails, usernames, passwords, phone numbers and addresses, was the result of 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 unlawful because it did not follow core principles of PIPEDA – user knowledge and consent to the collection of personal information. The incident was a serious violation of Canadians' privacy rights.

INVESTIGATION

Our Office launched its investigation after Google admitted that its cars – which were photographing neighbourhoods for the Google Street View mapping application – had,

over a period of several years, collected data transmitted over wireless networks. These networks, which were installed in homes and businesses across Canada and around the world, were not password protected or encrypted.

Technical experts from our Office travelled to Google's premises in Mountain View, Calif., to examine the data collected. They conducted an automated search for data that appeared to constitute personal information.

To protect privacy, the experts manually examined only a small sample of data flagged by the automated search.

Even from that sample, it was clear that some of the captured information was highly sensitive. For example, one document listed people suffering from certain medical conditions, along with their telephone numbers and addresses.

Because the study was not intended to be comprehensive, it is impossible to say how much personal information was collected from unencrypted wireless networks. It is likely, however, that thousands of Canadians were affected.

INTEGRATED CODE

Our investigation further revealed that Google collected the personal information because of a particular code integrated into the software used to collect Wi-Fi signals.

The code was developed in 2006 by an employee engineer who developed the code to sample all categories of publicly broadcast Wi-Fi data, and included lines that allowed for the collection of "payload data." This term refers to the content of the communications.

Through a lack of control by Google to ensure proper safeguards were in place, the code wound up being used in the Google Street View cars when the company decided to collect information about the location of publicly broadcast Wi-Fi radio signals. This information was fed into its location-based services database.

When the decision to use the code was taken, the engineer who created it identified "superficial privacy implications." Those implications were never assessed by other Google officials because the engineer failed to forward the code design documents to the Google lawyer responsible for reviewing the legal implications of the Wi-Fi project. This contravened company policy and controls were clearly lacking to ensure compliance.

RECOMMENDATIONS

In light of the investigative findings, the Privacy Commissioner recommended that Google ensure it has a governance model in place to comply with privacy laws. The model should include controls to ensure that necessary procedures to protect privacy are followed before products are launched.

The Commissioner also recommended that Google enhance privacy training to foster compliance among all employees. And she called on Google to designate staff responsible for privacy and compliance with Canadian privacy law.

She recommended further that Google delete the Canadian payload data it collected, provided this action is not prohibited by legal proceedings or other obligations under Canadian or American laws. Any Canadian payload data that could not be immediately deleted was to be secured and access to it restricted.

Google has responded to the Commissioner's recommendations and the investigation was ongoing in early 2011 to ensure full resolution of the matter by Google.

Our Office was one of several international data protection authorities that investigated the Google WiFi incident. For example, the Spanish authority announced in late 2010 that it had opened infringement proceedings against Google, an action that could potentially lead to hundreds of thousands of Euros in fines. As we were preparing to publish this report, the French data protection authority announced it had imposed a fine of approximately $140,000 Cdn for breaching that country's privacy laws.

Previously, Google had also raised significant privacy concerns in many countries, including Canada, with the launch of its Street View service.

2.4 Google Buzz

In April, Commissioner Stoddart and nine fellow data-protection authorities from around the world issued a joint letter that directed Google Inc. and other international corporations to respect the privacy rights of people who use their products and services.

The letter to Google's then-Chief Executive Officer, Eric Schmidt, made public during a high-profile news conference in Washington, D.C., warned organizations to comply with the privacy laws of each country where they propose to roll out online products and services.

In an unprecedented collaboration, the privacy guardians – representing a combined 375 million people in Canada, Europe, New Zealand and Israel – expressed deep concern about Google's privacy practices.

Central to the concern was the company's launch, two months earlier, of a social network called Google Buzz. In creating Buzz, Google simply started with its Google Mail, or Gmail, service. Taking what had been a private, one-to-one, web-based e-mail service, Google automatically assigned users a network of "followers" from among people with whom they corresponded most often on Gmail. In many cases, this list of followers was made public.

However, those users were not adequately informed about how this new service would work, and were not given sufficient information to permit informed consent. This violated the globally accepted privacy principle that people should be able to control the use of their personal information.

Gmail users, understandably concerned that their personal information was being disclosed, sparked an intense backlash. Google apologized and quickly introduced changes to address the widespread criticism.

The data protection authorities, however, noted in their letter that the privacy problems associated with the rollout of Google Buzz should have been "readily apparent" to the company. They called on Google and other organizations entrusted with people's personal information to incorporate fundamental privacy principles directly into the design of new online services, rather than to wait and test the product in the marketplace.

2.5 Anti-spam Legislation

As the year wound to an end, long-awaited anti-spam legislation received Royal Assent. The legislation regulates not only the sending of commercial e-mails and other forms of communications such as commercial text messages, but also other harmful practices such as electronic address harvesting and spyware.

Our Office had long supported such a law because unsolicited commercial e-mail violates the basic privacy principle of consent for the collection and use of personal information. Spam is also tied to phishing scams, identity theft and other privacy invasions.

In passing the legislation, Canada fell in step with all other G8 countries in addressing this assault on the online economy.

The new law will curb spam, including unwanted text messages and other forms of unsolicited electronic communications, by, among other things, strengthening consent requirements placed on senders.

Our Office will share oversight and enforcement powers with the Canadian Radio-television and Telecommunications Commission (CRTC) and the Competition Bureau.

The Act reinforces our Office's power to investigate the unauthorized collection of personal information through spyware or electronic address harvesting. The CRTC will guard against the sending of unsolicited commercial electronic messages, the re-routing of Internet communications without consent, and the installation of computer programs without consent. The Competition Bureau, meanwhile, will intervene in cases of misleading and deceptive marketing practices, including false headers and website content. Both of those institutions are empowered to impose significant penalties for individuals and organizations that violate the law.

To facilitate our Office's co-operation with these two institutions, the legislation gives the Privacy Commissioner more explicit authority to share information with other enforcement authorities. This authority is broad, permitting collaboration on anti-spam and other matters with data-protection agencies elsewhere in Canada and abroad.

The new Act, expected to come into force in the fall of 2011, also gives the Commissioner more discretion to decline to investigate or to discontinue a complaint.

As 2011 got underway, we were working on developing an enforcement strategy, preparing tools to raise public awareness, and hiring additional staff to carry out our new responsibilities under the law.

2.6 Consumer Privacy Consultations

In the spring of 2010, our Office organized consultations on issues that we felt could test the privacy of consumers, now and in the near future. As people and businesses increasingly move online and enjoy the benefits of the digital age, the ways in which online sites use personal information in order to make a profit need to be fully examined from a privacy perspective.

We chose online tracking, profiling and targeting of consumers, and cloud computing, as our key topics, because we see these trends as likely to have impacts on the privacy of Canadians. We also focused specifically on children online.

The aim of this consultation was to learn more about certain industry practices, explore their privacy implications, and find out what privacy protections Canadians expect with respect to these practices.

The consultation was also intended to promote debate about the impact of technological developments on privacy, and to inform the next mandated review process for PIPEDA, scheduled for 2011.

We received 32 written submissions in response to our notice of consultations. We also held three webcast public events, in Toronto, Montreal and Calgary.

ONLINE TRACKING, PROFILING AND TARGETING

With respect to the consultations on online tracking, profiling and targeting, participants generally agreed on the issues, but less on possible solutions.

The blurring of public and private lives and the effect this has on people's reputations was a major point of discussion. We heard concerns about children online. Children of all ages have a digital presence and their personal information needs to be protected. We heard about how privacy needs to be part of digital literacy or digital citizenship strategies.

Most industry participants maintained that PIPEDA is up to the task of protecting personal information in the face of evolving technologies and business models. Other participants were less definitive.

Examining online tracking, targeting and profiling through the lens of PIPEDA and the fair information principles, we noted the difficulties in determining what is and is not personal information. We also observed a lack of transparency around tracking, profiling and targeting, and what this means in terms of obtaining meaningful consent – a requirement under PIPEDA.

We recognize the work that industry associations do with their members in terms of helping them to be compliant with PIPEDA. Concerns were expressed during the consultations about what other new uses – besides behavioural advertising – could be made of individuals' browsing activity or their social networking and location data.

We urge industry associations to continue reminding their members that consent to new uses is an integral part of privacy protection under PIPEDA.

There was a lot of discussion about the challenges facing individuals when online data about them is retained permanently. Our Office encourages industry to develop technical approaches to addressing retention issues.

In addition to retention, accessing one's personal information and ensuring its accuracy are two important provisions in PIPEDA that can help address some of the reputational issues that stem from online activities. Our Office encourages industry to find innovative ways to meet the access, correction and accuracy provisions under PIPEDA.

CLOUD COMPUTING

A second consultation topic was cloud computing, which refers to a growing trend to store data with third-party providers through an Internet connection.

Cloud computing is popular because it can greatly reduce the cost and complexity of running a local data centre. Cloud computing can offer increased privacy and security capabilities if providers use sophisticated methods that would not normally be employed by companies in their own data centres.

Cloud computing touches on questions related to jurisdiction and applicable law.

The safeguarding of personal information is also a serious concern. Data must be protected as it travels over the Internet and when it is stored in remote locations. Moreover, since cloud providers serve multiple customers simultaneously, data must be properly segregated and protected from breaches.

DRAFT REPORT

On October 25, 2010, we issued a draft report summarizing what we heard in the consultations, providing our own observations, and asking for additional input on such issues as:

- Online identity management;
- Baseline measures for protecting children's personal information;
- How to better explain privacy practices;
- The nature of online tracking practices beyond behavioural advertising; and

- Efforts to develop security standards for the cloud.

We received 12 written responses to the draft report, which commented on some of these issues.

FINAL REPORT AND FOLLOW-UP

As we prepared this annual report, we expected to release our final report on the consultations in the spring of 2011.

While we learned a great deal from this initiative, much work still lies ahead.

For example, we have been mapping out the research activities we will be undertaking over the short and longer term, including public opinion polling and research into how we view what we think of as private and public information.

We plan to continue our outreach activities with young people. At the same time, we are considering ways to reach younger online users, as well as older users who may be new to the online environment.

We will continue to work with other stakeholders, such as industry associations, organizations and developers, provincial and territorial counterparts and federal government departments, on stronger privacy protection in the online world.

On our website, we are continuing to post information for individuals and businesses on issues in the online environment, such as behavioural advertising, cookies and a primer on cloud computing.

Canadians need to feel confident that they can embrace new technology and support new businesses without forfeiting all control over their personal information. The 2010 consumer privacy consultations were the start of our contribution to the discussion on how best to protect privacy in the coming years.

2.7 Digital Economy Consultations

In July 2010, our Office made a formal submission to the Government of Canada's Digital Economy Consultation. We argued that the rapid pace of technological innovation has implications for privacy and that privacy is key to the success of the digital economy.

Our submission noted that Canada's digital economy is, in fact, a global one, in light of the permeability of international borders to data flows. We also reviewed changing business models and technological advances, such as location-based services, electronic health records, analytics, and the sensor networks that make up the so-called "Internet of Things," and explored their implications for privacy.

The government's consultation paper asked for comments on the role that the federal government could play in supporting the digital economy. It proposed a series of mechanisms to foster the evolution of the digital economy. These included ensuring that the proper legislative or policy frameworks are in place; being a model user of digital technologies; building digital skills; supporting small- and medium-sized businesses; and funding more research and development.

Within those areas, our submission suggested ways to enhance the protection of personal information, while at the same time supporting the innovation that will make Canada a digital and privacy leader.

For example, we argued that the privacy impacts of new technologies could be addressed or mitigated if protections are built in right from the design stage. We also said that privacy needs to become an integral part of the business models that rely on technology, through a careful analysis of companies' activities. Privacy impact assessments, we argued, are a useful tool that the private sector should be encouraged to use because they can prevent problems from arising later.

In order to build privacy into the design and implementation of technologies, we further stated that technology designers and users (both businesses and individuals), need to have the appropriate digital skills. One of those is privacy literacy.

More specifically, Canadians need a solid grounding in fundamental privacy principles. They need to develop good habits for safeguarding their personal information and managing their online reputations.

2.8 Youth Outreach

Young people are generally among the most enthusiastic users of online technologies. They are also quick to try new applications, sometimes before all the privacy kinks have been identified and ironed out. With their readiness to text, post, tweet, "friend" and share video, it's easy to assume that youth care little about privacy.

But, as our educational outreach efforts underscore, that's not at all true.

In 2010, staff in our Office made 134 presentations to a total of 21,000 people in the education system – students in elementary and high schools as well as colleges, teachers, school resource officers, and parents.

What we heard, over and over again in the question-and-answer sessions, was that young people want to manage their online reputations. They want 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 they can know about everything others are posting about them. They also want to learn about targeted advertising, and what that means for their privacy.

Many are eager to learn how to permanently delete personal information, such as old responses to online quizzes that they no longer want circulating around the Internet, and items they wish they hadn't posted in the first place.

And then there's the ever-popular query about blocking Mom or Dad's persistent "friend" requests on Facebook.

During our educational outreach activities, we often hear stories about how teens – and sometimes adults – occasionally struggle with appropriate rules of engagement on social networking sites. For example:

- A principal at an elementary school reported that one of his students had created a fake Facebook profile for another student at the school, and added numerous peers as "friends". The youth did not understand that his actions could be damaging for the victim of his prank.

- A school principal requested a presentation from our Office after girls in Grades 7 and 8 were found to be circulating provocative images of themselves at school. Upon questioning, the girls insisted the incident was none of the principal's business, and many of their parents agreed.

- An individual in a foreign country began "friending" female students with autism and mild developmental disabilities, pretending he lived in the same city and was close to their age. Some refused the man's "friend" requests until he threatened them by claiming he could close down their Facebook accounts. Once he succeeded in "friending" the teens, he urged them to post revealing photos of themselves. Police said their hands were tied because the man lived outside Canada.

- Officials at several elementary and high schools told us that parents are "hacking" into their kids' Facebook accounts and sending rude or threatening messages to other youth with whom their children are having disputes. The principals tell the parents that such behaviour is inappropriate, but the parents respond that it's not the school's business.

CONCLUSION

Online issues will play a central role in our Office's work in the coming years. If we want to remain relevant as Canada's privacy guardian, the online world is where we must be focusing our attention. We will continue to make compliance and public awareness of online privacy issues a key priority.

CHAPTER 3

Key issue:
Destruction of Data in the Digital Age

Staples Customers' Personal Information Remains at Risk Following Privacy Breaches, Audit Finds

The Office of the Privacy Commissioner of Canada initiated an audit of Staples Canada Inc. after it was found that the retailer had, on repeated occasions, put returned data storage devices holding sensitive personal information back on store shelves for re-sale.

Indeed, when, as part of the audit, our Office tested data storage devices – laptops, USB hard drives and memory sticks – destined for resale, we found that, in a number of cases, they contained personal information. The devices had been brought back to Staples as a return and the company planned to resell them.

In a number of cases, the personal information we discovered on these devices was quite sensitive. For example, we found Social Insurance Numbers, passport numbers, banking information and tax records.

While the company did, after being investigated by our Office between 2004 and 2008, take steps to improve its procedures for removing personal information from electronic data storage devices, the audit found these procedures were not consistently applied, nor were they effective in erasing customer data in all cases.

As a result, our audit concluded that Staples had not met its obligations under PIPEDA.

Our Office has made a series of recommendations to Staples to improve its compliance under PIPEDA and the company has responded as to how it will address the recommendations. While Staples' collection, use, retention and disposal practices are generally in keeping with PIPEDA requirements, at the end of the audit, our Office had

ongoing concerns that privacy risks related to returned data storage devices had still not been addressed.

BACKGROUND

Staples, headquartered in Richmond Hill, Ont., is a large supplier of office supplies, business machines and office furniture, with more than 300 retail outlets across Canada.

Between 2004 and 2008, our Office investigated two complaints alleging that Staples had resold a computer and an electronic organizer that had been returned to the store without first ensuring that they had been wiped clean of personal data.

Following the investigation of both complaints, Staples agreed to change its processes and to implement a full "wipe and restore" procedure on all returned data storage devices.

After the company made these commitments, however, the media reported in March 2009 on another similar incident involving Staples.

Given the two complaints and the subsequent media report, our Office determined it had reasonable grounds to initiate an audit regarding Staples' personal information-handling practices in April 2010.

It is also noteworthy that the Information and Privacy Commissioner of Alberta has also investigated a similar complaint and found Staples had contravened provincial legislation by failing to safeguard personal information. The company similarly agreed to implement recommendations made by the Alberta Commissioner's Office.

As part of our audit, we examined Staples' policies, practices and processes for managing personal information, including the management of returned products with data storage capabilities. We looked at Staples' business processes and forms, as well as its privacy awareness training program. We also conducted inspections of selected retail outlets, in order to assess the physical and information technology security controls used to safeguard personal information. In addition, we tested returned data storage devices destined for resale to determine whether they had been wiped clean of personal data.

Staples was audited against PIPEDA and not assessed against, or compared to any practices or standards followed by other retailers.

WHY THIS ISSUE IS IMPORTANT

A large number of desktop computers, laptops, portable hard disks, memory sticks and digital cameras are sold in Canada every year. These devices have the capacity to retain vast amounts of data, including personal information.

Many retail organizations have adopted a "satisfaction guaranteed or money refunded" policy to support their business operations. Consumers may purchase an item, use it for a time and, if dissatisfied, return it for a full refund.

Moreover, computing and electronic devices are generally subject to a manufacturer's warranty, whereby a consumer may return a defective unit and receive a replacement. Some of these returned items are refurbished, repackaged and resold.

There is a risk that items may be resold before the customer data they hold is fully wiped, potentially exposing the personal information of previous purchasers. The unauthorized disclosure of such information could have serious consequences, including financial loss resulting from identity theft or fraud, which makes this an issue of significant public interest.

PIPEDA requires that organizations implement technical, physical and organizational safeguards to protect customers' personal information.

WHAT WE FOUND

The audit demonstrated that safeguards issues related to returned data storage devices had still not been addressed.

In an effort to mitigate the risk of further privacy breaches after the OPC's 2008 complaint investigation, the company revised its procedures for processing returned computing and electronic devices with data storage capabilities.

However, during this audit, we found that personal information remains at risk despite those changes.

In 15 of the 17 stores we inspected as part of the audit, we found:

- Devices that were resealed in packages and verified as having been wiped clean even though this was not the case;

- Devices that were not checked by a manager prior to being restocked; and

- Devices that were sent to a "return-to-vendor" bin without having been wiped of data.

We tested 149 data storage devices that had undergone Staples' wipe and restore process and were destined for resale. These devices included computers, laptops, USB hard drives and memory cards. Over one-third – 54 of the 149 tested – still contained customer data. In some cases, that residual data included personal information.

Some devices destined for resale contained highly sensitive personal information, including:

- Names, addresses, Social Insurance Numbers, and provincial health card or passport numbers;
- Employment history, diplomas and academic transcripts;
- Personal investment holdings, banking information, credit card statements and tax records; and
- Driver's licences, permanent residency cards and student visas.

We also examined a sample of digital cameras, global positioning systems (GPS), portable media players and personal digital assistants. The cameras and media players were cleansed of all residual data. However, two of eight GPS units were not restored to factory settings, thereby exposing the trip histories and home addresses of the previous owners.

The audit showed that Staples was not exercising proper care to ensure data storage devices were fully wiped prior to resale. Revised procedures have not been effective in addressing the deficiencies that existed in 2008, when we investigated Staples after a customer complaint.

The audit found that established procedures for processing returned devices were not always followed. Moreover, the procedure used to process a device varies by manufacturer, and, in some instances, was not effective in wiping all customer data.

Device	Number Tested	No Customer Data Found	Customer Data Found
Desktop and Laptop Computers	20	3	17
USB Hard Drive	55	36	19
Internal Hard Drive	10	9	1
Memory Stick	20	12	8
Memory Card	44	35	9
Total	149	95	54

Is the Data *Really* Gone?

When data stored by the customer is "deleted" from a data storage device, it is not actually removed; rather, the location where the data resided is simply reallocated as free space. The information the hard drive requires to find the data is deleted, *not* the data itself.

To ensure that customer data is securely erased, it must be wiped. The wiping process overwrites the content of the space previously occupied by the data. Security tools and software are available, and additional programs may be developed, for this purpose.

Unless a device is wiped, data previously "deleted" may be recovered using readily available tools that can restore it into a readable format.

During our testing process as part of the audit, each device was plugged into a laptop and viewed using Windows Explorer. Some of the devices contained accessible files containing personal information, while the remainder appeared to be wiped. Those appearing to be wiped were then examined for hidden content using readily available software downloaded from the Internet at no cost.

OTHER AUDIT FINDINGS

Our audit looked at other privacy and security issues related to safeguards and the management of personal information.

SAFEGUARDS

- **System Access**

The audit found that the use of common usernames and shared passwords on certain Staples computer systems prevent the organization from determining whether access rights to the system have been appropriately exercised.

Without a means of monitoring who is accessing the system, Staples cannot be certain that customer data is always being used and disclosed for legitimate purposes.

Controlled access to an information technology system and the data stored within it represents a key safeguard in protecting privacy. It mitigates the risk of personal information being compromised by restricting access to those with a legitimate need.

- **Document storage**

Staples' policy requires that all personal information be secured, either in a locked cabinet or room, when not in use. However, we found that 12 of the 17 stores we visited were not in compliance with the policy after finding filled-in delivery, transfer and special order forms stored in unlocked filing cabinets. Further, in some stores, return and repair forms were inadequately protected and returned data storage devices were kept in unlocked cabinets, or on open shelves or service counters.

- **Customer data in waste or recycling bins**

Customer data is generally disposed of at Staples stores under contract with a records destruction company. Stores are equipped with locked shredding containers. However, we found instances where order forms containing personal information were discarded in waste baskets or recycling bins, rather than in a shredding container.

MONITORING PRIVACY POLICIES AND PROCEDURES FOR COMPLIANCE

Comprehensive privacy policies and procedures are an essential ingredient of a strong privacy management framework. However, they need to be monitored to ensure they are functioning as intended.

While compliance with security procedures and controls are assessed under Staples' internal audit program, we found that the organization does not systematically monitor the collection, retention and disposal of personal information.

In terms of data storage devices, Staples' returns policy stipulates that a manager must verify that a device has been wiped of personal information prior to resale. We found this is not consistently done and most managers assume that the wipe-and-restore process has been effective.

Fourteen of the 17 stores we examined confirmed that random inspections were not carried out, and devices destined for resale were not tested as part of the internal audit process.

An ongoing monitoring strategy, including internal audits, would provide a means of mitigating privacy risks and provide a level of assurance that the organization's obligations under PIPEDA are respected in Staples' day-to-day operations.

MANAGEMENT OF PERSONAL INFORMATION

- **Cross-border data transfers**

We found that supply orders received by Staples' call centres, as well as records captured through its online copy and print service, are transmitted to and stored in the United States. However, we could find no evidence that customers were informed of these data transfers.

Today's globally interdependent economy relies on international flows of information. These cross-border transfers raise concerns about where personal information is going, as well as what happens to it while in transit and after it arrives at a foreign destination. As we state in our *Guidelines for Processing Personal Data Across Borders*, consumer confidence will be enhanced, and trust will be fostered, if consumers know that transfers of their personal information are governed by clear and transparent rules.

- **Unnecessary data collection**

We found that some Staples stores were taking photocopies of government-issued identification, such as driver's licences, passports and health cards, when customers applied for credit. These types of documents contain personal information such as physical characteristics that is not necessary to meet a credit issuer's legitimate need to identify and evaluate an applicant.

- **Records retained longer than necessary**

PIPEDA stipulates that an organization shall only retain personal information for as long as necessary to fulfill its purpose. During our audit, however, we found documents that were not covered by the retention and disposal schedule set by Staples, records that were kept beyond their scheduled disposal dates, and others that were assigned excessive retention periods and kept indefinitely.

During the course of the audit, Staples revised its retention and disposal schedule; records previously omitted were added to the schedule and the retention period for certain records was shortened. Notwithstanding these efforts, our Office is of the view that the company's retention period for documents related to the online service for Staples' copy and print centre is too long and therefore is not consistent with the limiting retention principle of PIPEDA.

- **Wiping of leased business machines**

Staples' retail outlets lease photocopiers to deliver their copy and print services. These machines have built-in hard drives that retain images of the information processed. When these copiers reach the end of their leases or are replaced, they are returned to the supplier.

Leasing agreements and Staples employees indicated that the photocopier supplier is responsible for the integrity of data held on the equipment. This includes ensuring the hard drives are wiped prior to disposal, recycling or reuse.

Staples confirmed that it relied on the assurances of the supplier in this regard; the company did not conduct any independent follow-up to ensure its customers' data had been erased.

RECOMMENDATIONS AND RESPONSES

1. Staples should include privacy specific compliance reviews as part of its internal audit program.

Staples Response

The company agrees with the recommendation. The company has made changes to its loss prevention audit checklist to address information storage, collection, retention and disposal of personal information and other privacy related items in more depth.

The company has established a program of weekly tech room inspections to further ensure privacy compliance. In addition, the company is conducting tech room privacy training in all of its stores to reinforce best privacy practices with respect to customer returns and repairs. The company has implemented Code of Ethics and Personal Information Management training, mandatory for all associates, which reinforces privacy protection priorities.

The company has centralized data recovery services to avoid having its stores retain customer data in its technical services area. The company further developed and released an automatic application that identifies files (that may belong to customers) inadvertently stored on tech room computers. All files so identified are removed in support of the company's policy not to retain customer data in its stores.

The company will continue to identify additional compliance reviews to support its privacy policies. The company has established a cross-functional privacy governance team to oversee privacy compliance.

OPC Comments: Our Office considers this response acceptable because the changes mean Staples will be checking for privacy compliance through internal audits. By expanding its internal audit checklist, Staples will be in a better position to catch any non-compliance with procedures in the stores and also address any problems to prevent personal information from being inappropriately handled. Furthermore, Staples has developed a privacy governance team to oversee privacy compliance.

2. Staples should make clients aware of all potential uses and disclosures of their personal information, including any data transfers to foreign jurisdictions.

Staples Response

The company agrees with the recommendation. The company will make appropriate changes to its corporate privacy policy by May 15, 2011.

OPC Comments: Our Office considers this response acceptable.

3. Staples should not collect and retain copies of government-issued identification as part of its in-store credit program.

Staples Response

The company agrees with the recommendation. The company's current policy prohibits copying and retaining government-issued identification for any reason. The company has re-communicated this to its stores and hereafter will continue to enforce this policy.

OPC Comments: Our Office considers this response acceptable.

4. Staples should ensure the processing of in-store credit applications is conducted in a private area.

Staples Response

The company agrees with the recommendation. The company has issued a directive to its stores reminding store associates of the obligation to maintain the privacy of all aspects of the credit application process and will continue to enforce this policy.

OPC Comments: Our Office considers this response acceptable.

5. Staples should limit the retention of personal information that accompanies on-line print/copy orders to a period that allows the client to review and address any issues related to print quality.

Staples Response

The company agrees that customers should be aware that online submissions will be stored for one year. The company feels that the retention of customers' online submissions for a period of one year is appropriate for consumers, as well as businesses, since the information is stored securely by a third party under appropriate agreements and restrictions. The only person who can trigger the re-use or disclosure of the information is the customer. However, the company will provide suitable notice to customers regarding such retention, thereby enabling the customer to opt to use over the counter copy services as an alternative.

OPC Comments: From our Office's perspective, Staples has not accepted our recommendation that on-line print/copy orders should be only retained for a period that allows the client to review and address any issues related to print quality.

Although Staples says it will inform its customers that on-line submissions will be stored for one year, it is our Office's view that this information is being retained longer than necessary and is not in keeping with the PIPEDA obligation for organizations to retain personal data only for as long as is necessary. Once the customer has picked up a print/copy order and is satisfied with the quality of the order, the purpose of the collection of personal information has been fulfilled and the personal information is no longer required.

Until the retention period is changed in accordance with our recommendation, Staples is not meeting its obligation under PIPEDA.

6. Staples should ensure that lease agreements with equipment suppliers include a requirement that the supplier issue Staples a certificate of destruction, confirming the date the hard drive was wiped or destroyed.

Staples Response

The company will require certificates of destruction from its copy equipment suppliers. This requirement has been communicated to existing suppliers and will be embedded in all new agreements with suppliers as they are initiated or renewed.

OPC Comments: Our Office considers this response acceptable.

7. Staples should review its procedures and processes for wiping data storage devices and implement enhanced controls to eliminate any risk of personal information being disclosed.

Staples Response

The company agrees with the recommendation. In response to a 2008 complaint, the company implemented a policy of wiping and restoring all returned product (with memory) prior to reselling such product. In the case of desktop and laptop computers, the company's wipe and restore process follows procedures and uses tools provided by manufacturers. Such procedures preserve only the original factory shipped software. Despite the manufacturers' warnings that this process will erase all files, data is in fact recoverable by using forensic software. No manufacturer recommends the overwriting of data as part of its recommended wipe and restore process. Overwriting processes may also damage a computer's hard drive and destroy the original factory-shipped software (including manufacturers' wipe and restore tools), rendering the universal use of such a process commercially unviable.

During the course of the audit by the Office of the Privacy Commissioner, the audit team was able to recover data from some computers that had undergone the manufacturers' recommended wipe and restore process, using forensic software. The audit team recommends a wipe and restore process that "overwrites" all the customer data to the extent that no customer data is recoverable.

The company is actively testing several means of wiping data from returned product (to the point that data is not recoverable using forensic software) without damaging or destroying hard drives, valuable operating systems and other manufacturer provided tools.

OPC Comments: At the conclusion of the audit, Staples had not fully addressed the issue that initially prompted our audit – previous complaints that customers' personal information remained on returned data storage devices that had not been adequately erased prior to being resold.

While the company adopted a wipe and restore process, it was not effective for all devices.

Although Staples is testing various means of removing data from devices without damaging operating systems, at the time of writing this annual report, the company had not responded to our request for information about how it was implementing controls to eliminate any risk of personal information being disclosed in the interim.

Until our recommendation on wiping customer data is fully implemented, personal information will continue to remain at risk and Staples will not meet its obligations under PIPEDA.

The position of our Office is that if Staples is unable to remove all customer data from a particular manufacturer's device, it is unacceptable to resell that device.

8. Staples should ensure that personal information is stored in locked cabinets or secured areas, as required by its policy.

Staples Response

The company has re-communicated and hereafter will continue to enforce its policies with respect to personal information storage and has included this matter in its internal audit procedures.

OPC Comments: Our Office considers this response acceptable.

9. Staples should ensure that staff members are reminded of the importance of using secure methods to destroy customer data.

Staples Response

The company has re-communicated and hereafter will continue to enforce its policies with respect to customer data destruction and has included this matter in its internal audit procedures.

OPC Comments: Our Office considers this response acceptable.

10. Staples should ensure that employees have unique system access credentials to facilitate user accountability and mitigate the risk of unauthorized access to customer data.

Staples Response

The company continues to look for practical systems access security solutions and it is expected that an application under current development will enable individual secured access.

It should be noted that the company's current policy prohibits the storage of personally identifiable information on any shared network other than those systems required for operational purposes. In addition, access control policies regarding the point-of-sale server in retail store front offices are in place and are subject to audit review. The company systems also provide for automatic logouts and the rotation of generic passwords.

OPC Comments: Our Office finds the commitment to look for solutions an acceptable response to our recommendation to implement a unique system access application. We have asked Staples to provide our Office with a confirmation when this recommendation has been implemented.

CONCLUSION

PIPEDA imposes obligations on private-sector organizations with respect to the management of personal information. The legislation balances an individual's right to privacy with the need of organizations to collect, use and disclose personal information for legitimate purposes.

In conducting its business, Staples handles a significant amount of personal information.

While contact information – name, address, telephone number and payment data – about customers is at the core of Staples' collection activities, this organization also handles personal information extending beyond its day-to-day business requirements.

Online copy and print orders can include sensitive information on resumés and legal documents such as divorce settlements and custody arrangements. A returned laptop or a computer brought in for repair may contain details about an individual's academic background, medical conditions or financial liabilities.

Staples, which was cooperative during our audit, has taken a number of positive steps to manage personal information. It has implemented policies and procedures to manage its information holdings; roles and responsibilities are clearly defined and understood throughout the organization; and various mechanisms, including mandatory training, are used to enhance privacy awareness amongst staff.

Our Office is of the view that Staples could nevertheless benefit from an ongoing monitoring strategy to ensure that these privacy practices and procedures are adhered to across the organization.

We are satisfied with the company's responses to our recommendations, with two significant exceptions.

As noted above, at the end of our audit, Staples was still not meeting its requirements under PIPEDA in relation to both the retention period for online print/copy orders and the wiping process for returned data storage devices.

It is particularly disappointing that the issue that prompted the audit remains unresolved.

In the wake of the previously investigated breaches involving returned data storage devices, Staples committed to our Office that it would take corrective action. Although the company did subsequently take steps to enhance its procedures and control mechanisms, they have not been consistently applied, nor effective in all cases.

Deficiencies that existed in 2008 persist. As a result, the personal information of Staples customers remains at risk.

Our view is that Staples and other retailers should not re-sell a returned data storage device if they are unable to remove all customer data from that device. We acknowledge that Staples is presently testing more effective ways to wipe data in response to our recommendation.

We will follow up with Staples on its implementation of our recommendations. We have asked Staples to provide, by June 30, 2012, a report from an independent third-party confirming how the company has complied with our recommendations.

We also plan to continue to track the privacy issues raised in this audit and, if necessary, follow up within the industry and with other interested stakeholders.

CHAPTER 4

Meeting the Concerns of Canadians

Inquiries and investigations make up 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 investigating their complaints about problems they've encountered when dealing with organizations.

During her appearances before Parliamentarians to discuss her nomination for reappointment in late 2010, Commissioner Stoddart stated that one of her areas of focus during the coming three years will be service delivery to Canadians. "At the end of the day, what is most important to me is that our work meets the needs and the expectations of Canadians," she stated.

The Commissioner has said she wants to ensure success in routine types of complaints that don't get any public attention – but that are of deep importance to the people who bring them to our Office.

The Office has recently begun a process to further refine our inquiries and complaints process in order to better serve Canadians.

4.1 Inquiries

Our inquiries officers offer a "privacy hotline" for Canadians who have questions about how federal privacy laws apply to situations they encounter in their day-to-day lives.

In 2010, we received a total of 4,793 inquires related to PIPEDA – roughly half of all the inquiries that came into our Office over the year.

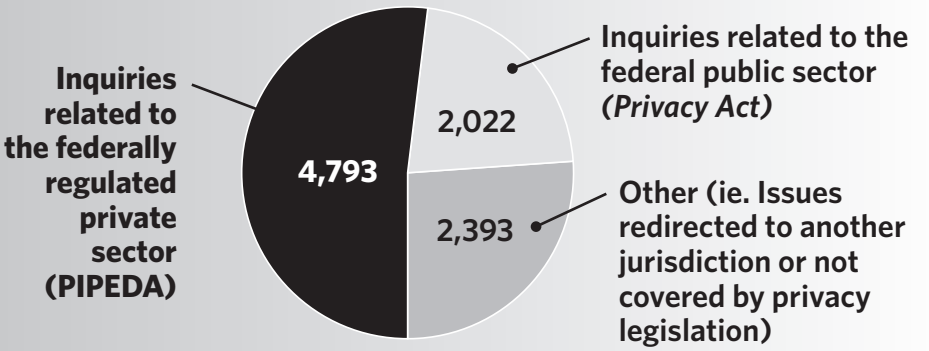
The number of PIPEDA inquiries we receive has been gradually declining in recent years.

At the same time, we have seen hits to our website increase dramatically, suggesting that more and more people are going online to find information rather than calling us to ask for it.

2010 PIPEDA (PRIVATE SECTOR) INQUIRIES RECEIVED

Telephone	4,081
Written	712
Total	4,793

INQUIRIES OF ALL TYPES RECEIVED IN 2010



During the first half of 2010, we noticed a marked increase in calls from people with questions about Facebook and Google Street View. Many of these individuals had heard about our investigations involving the two companies and were seeking information about how the issues related to their own personal situation. For example, we received inquiries about making changes to one's own Facebook account. We also had inquiries from people concerned that they could see their own home on Google Street View.

The number of calls to our inquiries line tends to spike in the days after our Office announces the results of an investigation or the Commissioner's comments on an issue are picked up by the media. Interestingly, however, the calls are often about issues completely unrelated to the topic that has been in the news. Media coverage about our Office would seem to serve as a reminder of the importance of privacy issues that touch on the daily lives of Canadians.

We continue to receive calls virtually every day about whether it is appropriate for organizations such as banks, landlords or retailers to collect government-issued identifiers such as driver's licence numbers and Social Insurance Numbers.

In one case, an individual called us with a complaint that he was being required to provide his Social Insurance Number in order to have access to an insurance company's online form. The inquiries officer contacted the company to discuss the issue. After this discussion, the company stopped requiring the number in order to open the online form. As well, employees of the insurance company received training on acceptable uses of Social Insurance Numbers.

One of the other issues we received a significant number of calls about is credit checks done to establish an individual's credit rating. For example, people had questions about landlords requesting Social Insurance Numbers in order to conduct a credit check as a condition of renting an apartment.

ROBUST FRONT-END SERVICE

We have significantly changed our processes for accepting complaints over the past couple of years.

Increasingly, we try to resolve issues *before* they become formal complaints to our Office.

Over the course of 2010, our Office implemented strategies to provide a more robust service for Canadians at the front-end of the complaints process.

Inquiries officers are often able to answer people's questions or concerns immediately. In addition, they may direct them to other sources of information or assistance, such as an organization's chief privacy officer.

As a matter of routine, inquiries officers ask callers whether they have raised their concerns with the organization – and with the *right* person within the organization. We maintain an up-to-date list of chief privacy officers with major organizations across the country, and encourage individuals to call them to try to resolve the issue. Oftentimes, all it takes is that one phone call to reach a satisfactory conclusion.

Following an initial analysis, if it is clear that the matter falls within our jurisdiction, our inquiries officers explain what our Office can do, within the limits of our authority under PIPEDA.

In some cases, our inquiries officers point people to past investigation case summaries that have already addressed the issue being raised anew.

As we build up a body of experience applying PIPEDA, the lessons learned can often be applied to similar sets of facts – avoiding the necessity of a whole new formal investigation process. Past case summaries are an important tool that we use to tell either a would-be complainant or an organization what we have determined in previous cases. Case summaries offer guidance on how an issue should be addressed.

Equipped with that information, individuals may be able to go back to the organization to press for their rights.

Inquiries officers are also responsible for collecting as much information as possible from a would-be complainant to help us determine how their concern should be dealt with.

Unresolved inquiries are brought forward to our complaints registrar, who will decide whether an individual's concern should be directed either to our early resolution process or to an investigator as a formal complaint.

4.2 Early Resolution

In late 2009, we developed a formal early resolution process and now have two designated early resolution officers – one for the private sector and the other for the federal public sector. Our goal was to provide better service to Canadians by addressing complaints quickly, with a less formal approach than our official complaint investigation process.

When individuals contact us about a problem where there is a high likelihood that the issue could be resolved quickly, they are referred 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 a matter of days. We've heard very positive feedback on the early resolution process from both complainants and organizations.

EARLY RESOLUTION COMPLAINTS OPENED

In 2010, we opened 112[1] early resolution complaints. We were able to reach a satisfactory conclusion in the vast majority of the complaints completed through the early resolution process.

Of those 112 early resolution files opened, we were able to reach a satisfactory resolution in 62 cases; another four were unresolved and transferred to investigations; and 46 were still open at the end of the year, to be dealt with in 2011.

The fact that we were able to reach a satisfactory resolution in 62 of the 66 completed 2010 early resolution files – over 90 percent of those cases – is a promising development.

Additionally, we successfully addressed another 14 early resolution complaints that were opened in 2009.

In total, 76 complaints (62 opened in 2010 and 14 from 2009) that in the past would likely have been dealt with under a more time-consuming investigation process were resolved satisfactorily in a relatively short period.

This is a positive step in terms of providing timely and effective service to Canadians.

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.

Our average treatment time for early resolution files is less than three months, which includes the time it takes to receive information from the complainant necessary to begin the early resolution process. We are changing our definition of treatment times in 2011 to provide a more accurate picture of how long it takes our Office to handle a complaint. We will start counting from the date that we have received from the complainant all of the information necessary to begin our work.

Since appointing designated early resolution officers, we have been able to close our early resolution files more rapidly than in the past. In 2009, for example, the average treatment time for an early resolved file was six months.

1 Note: Our statistical charts refer to 108, rather than 112, early resolution files opened in 2010. This is because four early resolution files were transferred to investigations and, as a result, are counted as a complaint received in our statistics.

The early resolution process has become an important tool for quickly and effectively addressing concerns that Canadians bring to our Office. Almost one third of all of the complaints we dealt with in 2010 were handled through the early resolution process.

PIPEDA EARLY RESOLUTION ACTIVITY IN 2010

Outcomes	Early Resolved	Further Investigated	Ongoing*	Total
2010 Complaints	62	4**	46	**112**

*Ongoing indicates that the early resolution file was still open at the end of 2010.

** In some of those cases, complainants wanted an investigation and formal letter of findings from our Office because, in addition to filing a complaint against an organization, they were contemplating legal action.

EARLY RESOLUTION SUCCESS STORIES

Credit inquiry prompts concerns

An individual noticed an inquiry on his credit report from a credit card company even though he hadn't had any dealings with that organization. He was concerned that the company was accessing his personal information without his consent and that the inquiry would have a negative impact on his credit score. An early resolution officer contacted the credit card company and learned that someone had fraudulently applied for a card in the complainant's name. The application was rejected because some of the personal information provided was incorrect. When someone applies for credit, the credit-granting organization normally checks that person's credit history. This check, known as a "hard" inquiry, is included on that person's credit report and, for years, it can be seen by other credit-granting organizations. Multiple "hard" inquiries can have a negative impact on an individual's credit score. While the credit card company couldn't remove the inquiry, it was able to have it considered a "soft" inquiry, which is only visible to the complainant and has no impact on his credit score. He was grateful for the information, which he said allows him to understand the need to vigilantly monitor his credit report for other fraudulent attempts to obtain credit in his name.

Manager uses emergency contacts in non-emergency

An employee with a small trucking company contacted our Office with concerns about how the company was using personal information contained in personnel files. The complainant wished to remain anonymous as he feared retribution if the issue was handled as a formal complaint. He stated that a manager had sent a letter to everyone that the company's drivers had listed as emergency contacts – spouses, mothers, siblings – in order to provide advice regarding their employees' health and safety. The letter stated in part: "I am hoping that we can count on you to do your part to make sure that your loved one is coming to work rested. Things like saving their 'honey do' list or other physically or emotionally draining tasks for days they are not working are a good start." An early resolution officer worked with the firm to explain how PIPEDA applies to employee information. A database that was created for the mailing was destroyed and the firm committed to respecting information contained in personnel files. The employee was satisfied and grateful that his identity was kept confidential.

Repeated requests to change address go unheeded

An individual contacted us after repeatedly asking her bank to update her address and finding that her bank statements kept being sent to her old address. This was particularly distressing to her because she believed that the new occupants of her former home were opening the mail. The bank thought that the issue had been dealt with but, after reviewing the issue with the early resolution officer, it found that correspondence had been sent to the wrong address and that other issues raised by the complainant had also not been addressed. As a result of our involvement, the bank worked with the complainant to address all of her concerns and ultimately offered her compensation.

Call to publisher stops unwanted marketing materials

A couple cancelled a magazine subscription and requested no further contact with the publisher. They were upset when they continued to receive marketing materials. An early resolution officer contacted the company, which investigated the matter and found that the request had not been processed. The company immediately removed the complainants' information from their databases. The complainants were grateful for the immediate response.

Unlisted phone number made widely available online

The complainant was shocked and unhappy to learn that an auto leasing company, whose services she was using to find someone to take over her car lease, had posted her unlisted telephone number on its website. Other automotive websites subsequently copied the listing. The company indicated that it had removed the posting. However, the information had been captured by a popular web search engine and it was proving difficult to have the information removed from search engine results. An early resolution officer contacted the web search provider and was successful in having the personal information removed.

4.3 Complaints

In recent years, we have seen a decline in the number of formal complaints received by our Office. This is largely because of our success in helping would-be complainants work with organizations to resolve issues before they become formal complaints. This is a welcome development because lengthy investigations are not always the best way to address Canadians' privacy concerns. By addressing more complaints through early resolution and public education, we can better focus our investigative resources on systemic issues with broad implications for people across the country.

As discussed in section 4.2, our early resolution process enabled us to find a satisfactory conclusion in dozens of cases that previously would likely have been handled through our investigation process.

In 2009, we received 231 complaints under PIPEDA. By comparison, in 2010, we received 207 complaints – including cases addressed through both our early resolution process (108) as well as formal complaints (99). That represents a 10 percent year-over-year decline in complaints.

4.4 Complaints by Industry Sector

Financial institutions were once again the target of the largest number of complaints, accounting for roughly one in five of all (early resolution and formal) complaints to our Office.

The number of complaints filed against this sector does not necessarily mean it is not compliant with PIPEDA. On the contrary, although we still identify some areas of concern through our investigations, our experience is that financial institutions have among the best-developed privacy policies and practices.

The size of the financial sector and the huge number of transactions it conducts with individual Canadians are major factors in explaining financial institutions' consistently high count when we break down complaints by sector.

MAJOR SECTORS TARGETED IN COMPLAINTS IN 2010

Sector	Early Resolution	Formal Complaints	Total	Percentage of all complaints*
Financial	21	24	45	22
Services	14	21	35	17
Insurance	13	14	27	13

*There were a total of 207 early resolution and formal complaints.

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

4.5 Types of Complaints Received

The use and disclosure of personal information as well as access to personal information were once again among the top issues raised in complaints to our Office.

We did, however, see a significant jump in the proportion of complaints received about consent issues. The percentage of total complaints related to consent doubled from 10 percent in 2009 to 20 percent in 2010.

It appears that part of this increase is due to the growing number of online-related complaints, which often involve issues around individuals' consent for the collection, use and disclosure of personal information. Of the 20 complaints alleging lack of appropriate consent that were opened in 2010, 11 related to social networking, websites or Internet service providers.

TOP 3 TYPES OF PIPEDA COMPLAINTS RECEIVED

Access:	Use and disclosure:	Consent:
Complaints about difficulties gaining access to personal information.	Complaints involving allegations that personal information was inappropriately used or disclosed, without consent, for purposes other than those for which it was collected.	Complaints that personal information has been used or disclosed without meaningful consent.
22.2 percent	22.2 percent	20.2 percent

4.6 Closed Complaints

In all, we closed 249 formal complaints in 2010. That was significantly lower than in 2009, which was an atypical year because of an all-out effort to clear a backlog of investigation cases.

We were pleased that, in a majority of cases, we were able to find a satisfactory conclusion to issues. Only 12 percent of formal complaints were deemed well founded and unresolved, meaning we were not able to reach a conclusion that we found acceptable.

In those unresolved cases, and where appropriate, the Commissioner may pursue the matter in Federal Court. Where the Commissioner considers it in the public interest, she may also exercise her discretion to name the organization publicly, with a view to informing Canadians about the organization's information-handling practices. The complainant may also choose to pursue his or her own case in Federal Court.

4.7 Snapshot of 2010 Investigations

The following is a look at some of the investigations completed during 2010. 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.

Note that investigations dealing with Internet organizations are included in Chapter 2, our special feature section on online privacy.

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

RISK: PROPERLY OBTAINING CONSENT

Bank Disclosed Personal Information without Consent

A married couple who held separate bank accounts and kept their financial information separate decided to apply for a joint mortgage and asked a mortgage specialist from their bank to come to their home to help them complete an application.

According to the complainant and his wife, while the mortgage specialist was setting up, the complainant left the room for a few minutes. He believed the meeting would not proceed until he returned.

During his absence, the mortgage specialist accessed credit report information, which she mistakenly believed to be that of the complainant, and disclosed it to his wife. The report revealed a high level of debt.

The complainant stated that, when he returned to the room, his wife was distraught because she thought he had a large amount of debt, of which she was previously unaware.

Later, it became evident that the information was that of the husband's father, who had the same name. Once it was established that the credit report was not his, the mortgage specialist tried to reassure the wife by showing her that the husband's actual debt load was insignificant. The complainant claimed that the specialist displayed his line-of-credit information and credit card balance on her laptop.

The mortgage specialist did not recall disclosing information to the wife about the complainant's line of credit or credit card account. She maintained that she would not have done so because the balances were too insignificant to mention.

The bank acknowledged that its employee improperly disclosed the complainant's father's credit report by mistake. With respect to the complainant's personal information, the bank argued there was implied consent on the complainant's part for the employee to discuss his credit information with his wife.

According to the bank, the usual practice of its mortgage specialists is to have an initial discussion with joint applicants to inform them, among other things, that a discussion of their assets and liabilities would be necessary. In the event one of the parties raises a concern, the mortgage specialist presents options such as talking about debts and assets with each party separately, or considering a single-applicant mortgage. If neither party raises an objection, the bank considers it reasonable to proceed on the basis of implied consent to disclosure.

In this case, the bank said it believed there was implied consent to discuss the financial status of each mortgagor in the presence of the other.

However, we found that the bank did not make a reasonable effort to ensure the couple was aware of the purposes for which their financial information would be disclosed to one another when applying for a joint mortgage. In this case, the bank's mortgage specialist did not follow the bank's usual practice of informing joint mortgage applicants about the need to discuss their assets and liabilities.

As well, even if the mortgage specialist had believed at first that she could rely on implied consent to disclose the applicants' financial information, the fact that the wife was clearly unaware of her husband's accounts should have indicated that the presumption of implied consent was no longer reasonable or appropriate. At the very least, the bank employee should have clarified the situation before making any further disclosures. Following an investigation, our Office was inclined to believe that the bank mortgage specialist did disclose the complainant's personal information to his wife.

In past findings, our Office has repeatedly upheld the principle that personal information must not be disclosed to spouses without consent and has set a high standard of notification in that regard.

In sum, the bank did not establish a reasonable knowledge basis for inferring the complainant's consent and therefore did not have meaningful consent to the disclosure of his personal financial information to his wife.

However, the incident in question occurred as the result of an employee's one-time error, the bank responded appropriately, and had adopted reasonable practices with respect to protecting the personal financial information of joint mortgage applicants. As a result, the complaint was well founded and resolved.

RISK: EMPLOYEE FAILURE TO FOLLOW PROCEDURES

Bank Employee Discloses Personal Information

A woman complained to our Office that her bank had, on two occasions, disclosed her personal information to the lawyer of her partner's ex-wife, without her knowledge or consent.

The complainant's partner was involved in divorce proceedings. As part of these proceedings, the bank was served with two subpoenas from the ex-wife's lawyer. The first requested a bank employee to appear in court and bring a series of documents, including credit card statements for the complainant and her partner's joint credit card account.

A bank representative duly appeared before the court and produced the requested documents in the presence of the judge.

The complainant subsequently raised concerns to the bank that her personal information had been disclosed to her partner's ex-wife's lawyer without her consent.

The bank said it had mailed a form to the complainant and her partner to obtain consent, but never received a reply. However, the complainant stated she never received such a form prior to the first court appearance.

Prior to a second appearance in court, the complainant did receive by mail a consent form from the bank to disclose her personal information as part of the divorce proceedings. She objected to the request and did not provide consent.

According to the bank, in response to the second subpoena seeking further documents, a bank representative went to court with the specified information. While waiting to appear before the judge, lawyers representing the parties in the proceedings indicated to the bank representative that there was no need to appear before the judge and that the bank representative could produce the documents directly to the lawyers (one of the lawyers was the complainant's partner, who was representing himself in the proceedings).

The bank representative sought written consent from the complainant's partner for the disclosure of the documents.

While the complainant's partner agreed to the disclosure of his own information, he indicated in writing on the consent form that he objected to the disclosure of the complainant's personal information. The bank representative nonetheless disclosed the documents to both the lawyer for the ex-wife and the complainant's partner.

The bank has since claimed that, despite his objection in writing, the complainant's partner contradicted himself by verbally authorizing the representative to disclose it.

The bank contends that the complainant's partner should have either advised the judge directly of his objection, or have verbally advised the bank representative that he did not agree to the disclosure.

In its representations to our Office, the bank stated that it was obligated to provide the records containing the complainant's personal information, and did not require the complainant's consent. Under its formal procedures for producing subpoenaed records before the courts, the bank seeks to obtain consent to the voluntary disclosure of the information. If it does not obtain consent, a representative goes to court and the requested documents will be produced. If, however, lawyers involved in the case agree that it is unnecessary to appear before the judge, the bank obtains the client's lawyer's written consent and discloses the documents.

During the course of the investigation, the bank updated those internal written procedures regarding the production of records in response to a subpoena.

In this case, the subpoenas issued by the ex-wife's lawyer did not require the bank to disclose the documents to her; they simply required a bank representative to appear in court to give evidence and produce certain documents.

Therefore, with regard to the second subpoena, the bank could *not* rely on the exception to consent set out under PIPEDA and the complainant's consent should have been obtained.

In our view, the bank has good procedures in place to respond to subpoenas. However, in failing to obtain the complainant's consent for voluntary disclosure of the information, the representative did not follow bank procedures in this case. Since this incident occurred, the bank has ensured that employees are informed of the proper procedures.

Accordingly, the complaint was well founded and resolved.

RISK: OVER-COLLECTION OF PERSONAL INFORMATION

Vandalism Leads to Excessive Surveillance

The complainant was a tenant of an eight-storey apartment building with 26 video surveillance cameras recording activity in and around the building, around the clock. The individual alleged that the collection of his personal information via video surveillance was excessive and unreasonable.

During a visit of the building, we found that cameras located in hallways were positioned in such a way that they could capture images of some apartments when hallway doors were open. As well, a camera located outside the front of the building captured images of people passing by on a city sidewalk.

According to the property manager, the cameras were installed in response to break-ins and vandalism that jeopardized the safety and security of tenants.

Under PIPEDA, an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances.

Our Office has developed a four-part test to determine whether this standard has been met in specific circumstances.

1. Is the measure (the video surveillance system) *necessary* to meet a demonstrable need?

Given the break-ins, theft and vandalism, we were satisfied that the building management had a valid purpose – to protect tenants and premises – for installing video cameras.

2. Is the measure effective in meeting the security need?

We concluded that the presence of the cameras had been an effective deterrent against vandalism and other crime. The number of incidents had declined significantly in areas where cameras were installed.

3. Is the loss of privacy proportional to the benefits gained?

We concluded that a better balance should be struck between tenants' privacy rights, and the amount and type of information currently captured by the cameras.

For example, it was unreasonably invasive for the apartment door of tenants to be under constant video surveillance, means by which their daily comings and goings could be easily monitored. And it was equally intrusive for images of the inside of their apartments to be caught as part of 24-hour video surveillance of the hallways.

4. Is there a less privacy-invasive method of achieving the same end?

While the property management had a duty to protect the building and was frustrated by the actions of certain individuals who have, for example, thrown eggs at a lobby wall and overturned trash cans, these reasons alone do not justify the proliferation of cameras. While potentially curbing the actions of wrongdoers, the video surveillance adversely impacted the privacy of law-abiding tenants. There was a need to consider less privacy-invasive methods to achieve the same end.

We recommended that the property managers review the location of each video camera to ensure cameras were not aimed at areas where there is a heightened expectation of privacy, such as inside people's apartments and at their front doors and landings; that cameras did not capture images of passing pedestrians; and that cameras captured images solely in keeping with the stated purpose of ensuring the security of the building and its residents.

We also recommended that video images should only be reviewed or monitored in conjunction with security purposes, and only after an incident.

The property management agreed to:

- Remove and relocate to stairwells all cameras located inside hallways.
- Reposition outside cameras so that they capture only images within the property boundaries.
- Ensure that video is reviewed only after a security issue is brought to management's attention.

As a result, we concluded that the matter was well founded and resolved with regard to collection.

RISK: USING SOCIAL INSURANCE NUMBERS AS IDENTIFIERS

Complaint Highlights Ongoing Concerns about a Longstanding Problem

We received a complaint alleging that a bank was improperly using Social Insurance Numbers as an identifier when clients telephoned its investment service centre.

The complainant contacted our Office after he called the service centre and was asked to provide his full Social Insurance Number as part of the bank's authentication protocol.

Social Insurance Numbers are collected by organizations such as banks for the sole purpose of reporting income to the tax authorities.

It has long been the position of our Office that a Social Insurance Number should *not* be used as a personal identifier and organizations should restrict their collection, use and disclosure of this number to legislated purposes. This is consistent with the federal government's position that a Social Insurance Number should be used only for legislated purposes.

Although the bank was using the full Social Insurance Number as part of its telephone authentication process, it stopped this practice during the course of the investigation and began using only the last three digits.

Accordingly, the complaint was found to be resolved.

Social Insurance Numbers and Privacy

The Social Insurance Number was created in 1964 to serve as a client account number in the administration of the Canada Pension Plan and Canada's varied employment insurance programs. In 1967, what is now Canada Revenue Agency started using the number for tax reporting purposes.

The Social Insurance Number is a key piece of information to open the door to an individual's personal information. For example, it can be used to steal someone's identity. Along with other personal information, someone may be able to use a Social Insurance Number to apply for a credit card or open a bank account, and then fraudulently ring up hefty bills and write bad cheques.

Although only certain government departments and programs are authorized to collect and use the Social Insurance Number, there is no legislation that *prohibits* private-sector organizations from asking for it.

Indeed, some organizations continue to ask for a Social Insurance Number because it is a simple method of identification. Many use it as a client account number to save them from setting up their own numbering systems.

This is why our Office has repeatedly recommended that no private-sector organization request a Social Insurance Number from a customer, and that no customer provide this number, *unless* the organization is required by law to request it.

RISK: INADEQUATE ACCESS REQUEST PROCEDURES

Poor Response to Access Requests Leads to Unnecessary Deletion of Personal Information

An individual complained to our Office after a major telecommunications organization wound up deleting his personal information as part of its standard retention and disposal policies – even though he had previously requested access to that information.

An initial request from the complainant to access his personal information (notes and recorded conversations related to several accounts dating back 13 years) went unanswered despite numerous follow-up e-mails sent over a period of several months.

According to the company, one of its offices misdirected and mishandled the request. The individual was thus invited to make the request again. He did so, addressing the second formal request to the organization's chief privacy officer.

The firm failed to respond to this second request within the 30-day time limit required under PIPEDA. However, five weeks after the second request was sent, the firm contacted the customer, seeking his permission to extend the limit because of the volume of information he was seeking.

More than 70 days after the date of his second request, the firm sent the complainant copies of all his account notes. The delay was partially caused by the necessary decoding and transcribing of information from a data format no longer used by the firm's current computer system.

However, the client's call recordings for his accounts were not included. The organization advised us that, prior to the second access request, it had erased all audio recordings more than six months old, in accordance with its retention policy.

While it had had in its possession recordings of the customer's calls dating back to six months before his first (mishandled) request, these had since been destroyed in accordance with its usual retention policy.

As a result of the deletion, the individual permanently lost access to some of his personal information. The deletion could have been avoided had the firm properly processed the complainants' first access request, or had at least replied to his ensuing messages, if it was unsure about it.

During the investigation, the organization made commitments to improve its policies and practices concerning customer access requests, and to make allowances in its

information retention policy for personal information that is part of an unresolved access request.

We concluded that both the complaint concerning time limits and the complaint concerning access were well founded and resolved.

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 summaries describe investigations where we were unable to reach a satisfactory conclusion.

Investigation Highlights Airport Authority's Non-Compliance with PIPEDA

An individual filed a complaint with our Office because he was concerned by the non-consensual collection of personal information by an employee of the Greater Toronto Airports Authority (GTAA), and the GTAA's failure to provide access to his personal information.

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.

Following our investigation, we concluded that the GTAA's actions were not in compliance with PIPEDA. We found that the photographs were not taken for a proper use in that they were taken without knowledge and consent, and for purposes that were clearly beyond normal surveillance requirements. As well, we found that the airport authority took more than two months – far beyond the required 30 days – to respond to the complainant's access request. We were also aware that the GTAA held more

personal information about the complainant than it had provided in its belated response to the complainant's access request.

We recommended that the GTAA:

- Provide a comprehensive list of the complainant's personal information, regardless of format, that was under its control, up to and including the date the complainant made the access request;

- Implement a system whereby all common-use computers having access to video surveillance equipment require a login procedure for individual employees using them;

- Develop an employee policy on video surveillance and ensure it is reviewed and signed by authorized employees having access to surveillance equipment.

While the GTAA did provide a response to the Office's recommendations, the Office ultimately deemed the GTAA's response insufficient and found the complaints to be well-founded. Given that the complaints were well founded and remained unresolved, the Privacy Commissioner initiated an application in Federal Court under section 15 of PIPEDA. Details of this application are included in section 6.

Laurier Optical Improperly Discloses Client's Personal Information

A customer who asked for a refund after obtaining two pairs of prescription eyeglasses that didn't satisfy him, was shocked to discover that Laurier Optical had copied its written response to his request to 10 different parties.

The individual complained to our Office that the optometry chain, which has locations in Ontario and Quebec, disclosed his personal information without consent and subsequently failed to provide him with access to his personal information.

The man had obtained two prescriptions from Laurier Optical and found that neither satisfied him. As a result, he obtained a prescription from an independent optometrist who worked elsewhere.

After receiving the refund request, Laurier Optical initiated a complaint against the independent optometrist with the Ontario College of Optometrists. The company alleged the optometrist had incorrectly told the complainant that Laurier Optical had not performed a proper eye exam.

In its written response to the refund request, Laurier Optical included the complainant's home address, telephone number and details of his three prescriptions, as well as a description of the prescription dispute. The complainant felt it contained false statements damaging to his character. The letter also stated that Laurier Optical would ask two other professional bodies and the two biggest lens manufacturing labs in Canada to evaluate the three prescriptions and obtain neutral opinions.

The letter was copied to 10 different parties, including various Laurier Optical officials; the Ontario College of Optometrists; the College of Opticians of Ontario, the independent optometrist; the company that made the complainant's lenses, as well as another lens manufacturing company.

The complainant also requested access to his personal information held by Laurier Optical, but received no documentation in response.

Following an investigation, our Office found both the disclosure and access complaints to be well founded.

It was not necessary for Laurier Optical to disclose the complainant's personal information to the College of Opticians or the lens manufacturers in order to demonstrate that the lenses it had provided to the complainant were appropriate. Even if these organizations could provide relevant input, they could have done so without knowing the complainant's name, address, telephone number or details of the dispute. Similarly, it was not necessary to provide the independent optometrist with this information.

We recommended that Laurier Optical train its staff about PIPEDA's requirements regarding the protection of clients' personal information.

The organization did not respond.

As a result of the circumstances examined in this investigation and the outstanding issues, the Privacy Commissioner was of the view that Laurier Optical's personal-information handling practices in this case should be made public and exercised her discretion to publicly name the organization.

Rapid Oil Change Garage Unnecessarily Scanned Customers' Vehicle Registration Information

A customer of an automotive oil change and lubrication service business objected to the recording of personal information from his vehicle registration document, just to have his car's oil changed.

When he later challenged the practice and raised questions about how his personal information was being handled, he received no reply from the company. He filed a complaint with our Office.

The complainant was a regular customer at the rapid-oil-change garage. On one visit, an employee asked him to produce his vehicle registration document so that the bar code on it could be scanned. The complainant wondered why this was necessary because the car's Vehicle Identification Number provided enough information (i.e., make, model, year, and oil grade and filter number) for an oil change.

He became more concerned when he later learned from his provincial insurance board that his vehicle registration bar code also contained his driver's licence number.

When he called the shop's offices for a more satisfactory explanation, no one returned his calls, nor did its privacy officer respond to a written request for information.

In response to questions from our Office, the company's owner admitted that scanning the vehicle registration code can detect more personal information than scanning the Vehicle Information Number, but stated that this can be useful when confirming the spelling of information from the customer's file.

First-time customers are also asked for their name, address and telephone number – though this is not mandatory. The information is requested in case of warranty work or service complaints, or as a precaution in case something goes wrong during servicing and the client needs to be contacted.

Although more personal information is recorded in the vehicle registration bar code (e.g., the owner's provincial insurance and registration costs and driver's licence number), we confirmed that the oil-change company's scanning technology was only capable of reading the name and address of the vehicle's registered owner, vehicle year, make, model, class and colour, and the licence plate number.

Although it was established that the organization did not obtain from the complainant's scanned vehicle registration any personal information about the complainant other than what was already on file, we agreed that he had valid concerns about scanning vehicle registrations in order to perform a simple automobile maintenance service. The collection of any information from a customer's vehicle registration document is not necessary for the purpose of changing motor oil in vehicles.

We recommended that the company cease the unnecessary practice of requesting and scanning customers' vehicle registration documents.

We also recommended that the company put policies and procedures in place to direct individuals to a privacy officer capable of handling privacy inquiries and complaints.

The company did not respond to the recommendations or return follow-up telephone calls from our Office.

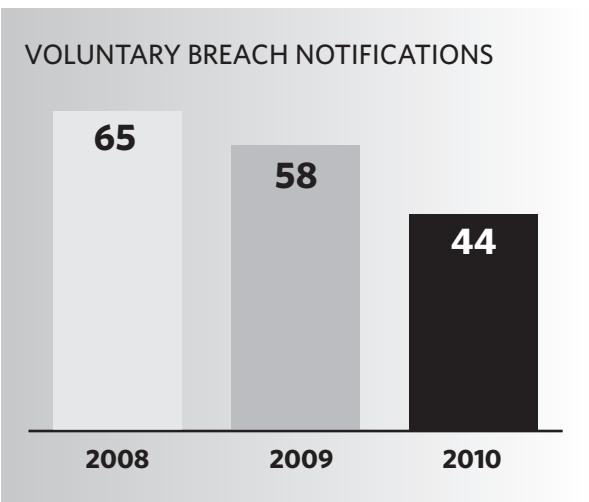
The Office considered taking the case to the Federal Court to enforce the company's compliance with its privacy obligations, but the complainant requested we not pursue the matter further. PIPEDA requires that the Privacy Commissioner obtain a complainant's consent to apply to the Court for a hearing.

4.8 Data Breaches

Our Office encourages organizations to voluntarily report data breaches to us.

In 2010, 44 private-sector data breach incidents were voluntarily reported to us. This marks the second year in a row in which the number of voluntary reports have dropped.

We continue to look forward to the passage of legislative amendments that would make it mandatory to report significant breaches to our Office and to the affected individuals. The amendments were before Parliament at the end of 2010.



A mandatory reporting scheme will 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.

The financial industry appears to be the one industry sector routinely reporting breach incidents. In 2010, two-thirds of voluntary breach reports – 29 – came from financial institutions. We have heard from privacy officers at Canada's major financial institutions

that they have made a conscious decision to proactively report breaches, even though the legislation requiring them to do so has not yet been passed into law. We commend them for doing so.

The fact that our Office has been informed of a breach and is monitoring the actions an organization is taking in response can often reassure those affected and prevent concerns that result in complaints to the Privacy Commissioner.

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.

In 2010, more than one-third – 15 of 44 – of the breach reports we received involved unauthorized access to personal information – in many cases by employees of the organization.

Almost as many of the incidents (14) involved the theft of personal information – in many cases when a laptop was stolen.

EXAMPLES OF BREACH INCIDENTS

Database Hacked

A Canadian children's clothing retailer had its customer database hacked and customers' personal information was visible on the site for a short period of time. During this time, a search engine "cached the website" and the personal information became searchable. The media became aware of the incident and reported on what had happened. In response to an inquiry from our Office, the company acknowledged there had been a breach. The retailer told our Office it had tried without success to get the search engine to remove the pages. An early resolution officer intervened and the information was finally removed.

Telephone Redial Concerns

Our Office received a media inquiry about telephones at two banking kiosks which customers could use for telephone banking. The media outlet alleged that the telephones' redial buttons permitted individuals to obtain information that would allow them to access customer accounts, obtain information, and even move money around. When contacted by our Office, the bank stated that its tests on the phones suggested it was not possible to press redial and obtain the information needed to access someone else's accounts. However, as a precaution, the bank replaced the phones at both locations with new ones that did not have a redial feature. The bank also committed to replacing phones at all its locations.

CHAPTER 5

Reaching out to Canadians

An important part of our role is to inform Canadians about their privacy rights and to help organizations understand how they can better meet their obligations under PIPEDA.

We live in an age when some people are living their lives like reality TV stars, enthusiastically sharing even their most intimate thoughts and images online.

Others aren't digital exhibitionists, but they're still giving up plenty of information about themselves. By using loyalty cards, for instance, they're actively trading personal data for retail discounts or other goodies.

And that's just what people do consciously. Beneath that lies a whole other layer that most people know little about, including the massive data collection that occurs when people browse Internet websites or make online purchases.

All these activities have profound implications for privacy, but it's not always easy to understand how the pieces fit together.

And yet, that doesn't mean that people don't care about their privacy. On the contrary, surveys show they do.

That's why 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.

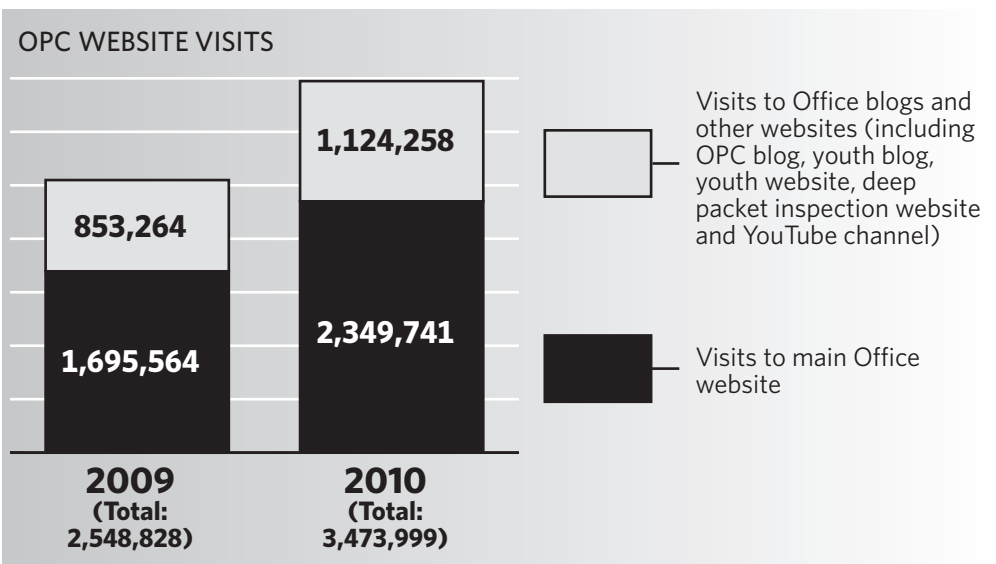
Important mainstays of our public outreach efforts include making presentations and exhibiting at conferences and other events. We are invited to speak at high-profile conferences and events around the globe. In 2010, we accepted approximately

three-quarters of the speaking requests we received. The Commissioner, Assistant Commissioners and other members of our staff delivered 150 speeches and presentations. We received 200 speaking requests during the year.

We also consider the media an extremely effective tool for reaching out to individual Canadians and organizations. Over the last couple of years, we've seen an increase in media interest in privacy issues – particularly in the online realm. Our Office accepts as many media interview requests as possible – 250 in 2010 alone – in order to take advantage of opportunities to deliver messages about important privacy issues.

In the online context, our focus is on digital literacy – honing the skills and knowledge that individuals need to protect their personal information, and also ensuring that businesses provide their customers with the right information and tools to allow them to make informed privacy choices.

Visits to our growing list of Office websites – our main site, blog, youth website, youth blog, deep packet inspection website and YouTube channel – have increased dramatically. Between 2009 and 2010 alone, we saw total website visits jump by 36 percent.



Over the past three years, our Office has used social media tools to engage the public on these issues.

We launched an OPC blog in 2007 and a youth blog in 2008. In addition, we created a Twitter account in 2010 to share news and information and to engage with privacy

stakeholders and other interested people. By the end of the year, we had sent out more than 700 "tweets" and attracted nearly 2,000 followers.

We used Twitter to stimulate discussion during our consumer privacy consultations in the spring. We "live-tweeted" the events and encouraged attendees to do the same. We took questions via Twitter from people in the audience and those following the webcast.

Our paper publications also remain popular. We distributed 15,478 publications in 2010. These included – among other pamphlets, guidance documents and fact sheets – our guides for businesses and individuals, our *Privacy in a Changing Society* booklet, and our annual reports.

We also use other creative means to get the privacy message out. For example, a cartoonist helps us to offer privacy messages in a humorous way. The cartoons have been used in presentations and on posters, postcards and our popular calendar.

Here is a snapshot of some of our major outreach initiatives in 2010:

5.1 Outreach to Business

TORONTO OFFICE

In the fall of 2010, the OPC officially opened an office in Toronto. This Toronto presence bolsters engagement with businesses, industry associations, academics and other stakeholders in the region. It enables us, for example, to be more targeted and effective in the way we deliver guidance and enhance awareness on key privacy issues.

We also conduct a number of our investigations from the Toronto office. An analysis of PIPEDA complaints received between January 2008 and mid-May 2010 found that 44.5 per cent of respondent organizations were located, or had their headquarters in the Greater Toronto Area.

We have established collaborative networks to support our current and future public education and outreach activities in the area. We have also held a series of information sessions with businesses and privacy practitioners in the Greater Toronto Area. Those

sessions covered systemic privacy issues, promoted awareness of privacy compliance obligations, and showcased OPC tools and information products.

In planning for the Toronto office, we surveyed large and small businesses, and found that a majority supported such a presence. They perceived it as a means to promote privacy discourse and to inform industry – and particularly small- and medium-sized enterprises – about privacy regulation and compliance.

SMALL BUSINESS ONLINE TOOL

Our Office marked Small Business Week in October 2010 by launching an enhanced online tool to help businesses protect their customers' privacy. The tool helps businesses figure out how much information they should have about their customers and how to protect it.

The Privacy for Small Business online tool offers an interactive privacy assessment specifically designed for businesses. It leads users step by step through the information they need to comply with privacy laws and to provide customers with the privacy protection they expect.

The tool is easy to use, and the assessment can be completed in approximately half an hour. At the end, business owners have:

- An information audit of their business;
- Consent provisions required specifically for their business;
- A security plan for protecting personal information in their care;
- A sample privacy brochure for their customers; and
- A training needs assessment.

IT COMMUNITY

With the addition to our staff of two new information technology research analysts, our Office has been able to boost its targeted outreach to the broader information technology community.

During 2010, these analysts were invited to speak on technology and privacy issues to students at the University of Waterloo, Harvard University, Columbia University, Princeton University and the University of Pennsylvania.

They also made presentations at major privacy and security conferences, such as the Reboot Privacy & Information Security Congress, the National Cyber-Forensics & Training Alliance Canada eCrimes Summit, and the Digital Crimes Consortium.

5.2 Outreach to Individuals

YOUTH PRIVACY

Children are going online earlier in life, and spending more time online. Young people also tend to be among the early adopters of new technologies, before some of the privacy risks have come to light. Recognizing the new challenges young people face when they go online, our Office is adapting our youth privacy education and outreach programs.

To help identify the knowledge gaps among young people and to strengthen our understanding of how youth prefer to get their information, we convened an advisory panel of teens from across the country. Their opinions and perspectives have proven invaluable in guiding our digital privacy initiatives.

Since 2009, our staff has been delivering presentations to students on the privacy risks of online social networking. These presentations skyrocketed in popularity over the past year. In 2010, we delivered 134 presentations to well over 21,000 students in Grades 4 to 12, as well as to parents, teachers and school resource officers – police officers assigned to work with schools.

We also offered modified versions of the presentation to specialized audiences. These included autistic and developmentally delayed teenagers, most of them on Facebook. We also spoke to teenagers attending alternative high schools.

Feedback on our presentations suggested that adults and young people alike benefited from the information and expertise we were sharing. The interactive nature of the presentations also sparked young people's engagement with the subject matter, and strengthened our own understanding of youth behaviour online.

Our youthprivacy.ca site continues to be a source of information and guidance for parents, teachers, and young people on preserving privacy on the Internet. In 2010, the Office contributed posts to the youthprivacy.ca blog on geotagging, digital citizenship, phishing, and third-party apps on social networking sites – all written with a view to attracting and informing children and teens.

For the second year in a row, we held a student video contest. We were overwhelmed with the response, receiving more than 100 videos from students across the country. At an event held in conjunction with the Encounters with Canada youth forum, winning videos were chosen by 120 young people hailing from every part of the country.

PrivacyCampTO

In June 2010, the Office supported the first annual PrivacyCampTO, a conference on digital privacy. The one-day event, held at Toronto's Ryerson University, was collaborative in the sense that participants shaped the agenda at the start of the event. It prompted a lively exchange of perspectives between researchers, academics and activists.

Participants discussed privacy threats related to social media. The conference also featured "speed geeking" – a process (which gets its name from speed dating) to deliver presentations in a very short blocks of time. Presentations offered technical skills to strengthen privacy such as an introduction to encryption tools and tips on how to permanently delete social networking profiles.

SPEAKER SERIES

In 2010, our Office launched Insights on Privacy, a series of public armchair discussions aimed at amplifying new voices doing interesting work in the privacy field.

The first event that we hosted in December featured broadcaster and Internet strategist Jesse Hirsh and privacy researcher Christopher Soghoian. Their provocative insights on the future of privacy attracted more than 60 people to the event, which was videotaped and posted to YouTube (where we also have other videos posted).

We plan to continue this series, inviting a range of speakers to discuss current privacy issues with live audiences.

5.3 Outreach across Canada

Federal, provincial and territorial privacy commissioners agreed at their September 2010 meeting in Whitehorse to work together to raise awareness of privacy issues among Canadians.

Our Office's goal is to work with provincial and territorial commissioners to build productive and sustainable outreach programs. Key focuses are small business awareness

of privacy issues and safeguards, and digital literacy among Canadians, particularly youth.

We are also working with our provincial and territorial partners to develop localized and targeted programs in their jurisdictions.

In Atlantic Canada, a two-year interchange agreement we had established with a senior research and outreach advisor in that region came to an end in 2010. From his base in St. John's, Nfld., our representative delivered more than 70 presentations to youth, small business, community organizations, professional associations, chambers of commerce and business development corporations all over the region.

5.4 Contributions Program

For the third year in a row, our Office's Contributions Program funded public education and outreach initiatives in addition to research into privacy issues.

In 2010, for instance, our support enabled Option consommateurs to hold educational workshops and develop an information guide aimed at improving consumer awareness about the collection and use of personal information in credit reports.

Contributions Program funding also allowed another consumer group, Union des consommateurs, to organize a two-day conference to examine the challenges and opportunities consumers face in the digital era. The conference took place in Montreal in March 2011.

5.5 Speaking Engagements

Speaking engagements are another important ongoing component of our Office's outreach program. We provide presentations on a wide range of privacy issues to industry groups, conferences, schools and universities.

In 2010, we participated in 150 public events across the country. The Commissioner, Assistant Commissioners and staff members spoke at conferences aimed at specialists in various fields. These included the International Association of Privacy Professionals Canadian Privacy Summit 2010, the ITechLaw 2010 World Technology Law Conference, the 11th Annual Privacy and Security Conference, and the SC Magazine World Congress Canada.

CHAPTER 6

In the Courts

In terms of jurisprudence, PIPEDA remains relatively new legislation and its interpretation continues to raise novel legal questions. In 2010, the courts grappled with, among other things, the scope of the Commissioner's powers, the definition of "commercial activity", and the question of when damages should be awarded for a contravention of PIPEDA.

Our Office continued to appear before the courts in order to help guide them in resolving these and other issues and in enforcing organizations' obligations under the Act.

Under PIPEDA, a complainant may, after receiving a report from our Office and in specified circumstances, apply to the Federal Court for a hearing in respect of any matter referred to in his or her complaint or that is referred to in the Commissioner's report (section 14 of PIPEDA).

PIPEDA also allows the Privacy Commissioner, with the consent of the complainant, to apply directly to the Federal Court for a hearing in respect of the same matters (section 15 of PIPEDA). It also allows the Commissioner to appear before the Federal Court on behalf of any complainant who has applied for a hearing; or, with the permission of the Federal Court, to appear as a party to a hearing initiated by a complainant (section 15 of PIPEDA).

This year, the Commissioner initiated new applications under the Act and a number of Commissioner-initiated applications filed in past years were decided. In one case, we were able to reach a settlement before the case got to 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.

6.1 Commissioner-initiated court applications (section 15 of PIPEDA)

Privacy Commissioner of Canada v. Canad Corporation of Manitoba Ltd., c.o.b. Canad Inns
Federal Court File No. T-586-08

In 2010, we reached a settlement in a legal proceeding that had been initiated by the Commissioner. The investigation concerned the collection of personal information of bar patrons. The patrons were required to use a machine that copies and stores personal information appearing on the front of an identification card such as a driver's licence.

As reported in our 2009 annual report, the investigation was prompted by a complaint from a Canad Inns customer who objected to having her driver's licence information scanned.

Our Office understood Canad Inns' need to effectively verify the age of its patrons and to ensure an appropriate level of security in its nightclubs. In addition to the identification machines, Canad Inns also used video surveillance, metal detectors, pat downs, security personnel and lists of banned people in order to secure the safety of patrons.

Following an investigation, we found that the identification machines collected more information than was necessary to achieve Canad Inns' stated purposes of verifying the age of patrons and ensuring security. We recommended that Canad Inns stop collecting and retaining personal information in this manner, and remove customers' personal information from its identification machine storage units.

Canad Inns disagreed with the recommendations. With the complainant's consent, our Office filed a Notice of Application for a hearing before the Federal Court to enforce her recommendations.

Following court-ordered mediation in early 2009, the Court gave Canad Inns a period of time to determine feasible means to limit the personal information it collects.

In July 2010, we reached a settlement with the Canad Corporation of Manitoba Ltd. (Canad Inns). As part of the settlement, the company made commitments to:

- Stop collecting personal information at its nightclubs via its identification machines;
- Destroy the personal information collected with the machines; and
- Limit the amount of personal information found on its list of barred people and ensure that this information is adequately secured.

Our Office is pleased that Canad Inns has agreed to take steps to ensure that the privacy rights of its patrons are respected.

Thus, only limited personal information (names, dates of birth and photos) will be collected from bar patrons and this personal information will only be retained for 24 hours.

This is a similar approach to that taken in both British Columbia and Alberta, where provincial privacy commissioners have investigated similar issues.

Privacy Commissioner v. Air Canada
Federal Court File No. T-143-09

Following an incident during a short-haul flight, an individual requested access to his personal information from Air Canada. The airline refused to provide the information on the basis that it was subject to solicitor-client privilege.

The individual complained to our Office and we were unable to resolve the matter in the course of our investigation because Air Canada refused to provide the Office with sufficient information concerning its claim of solicitor-client privilege. In particular, we had asked for a sworn affidavit in support of its claim of privilege.

Air Canada took the position that the Privacy Commissioner's Office lacked jurisdiction to investigate claims of solicitor-client privilege following the Supreme Court of Canada's decision in *Canada (Privacy Commissioner) v. Blood Tribe Department of Health.*

In January 2009, we filed a Notice of Application seeking, among other things, a declaration confirming the Commissioner's statutory jurisdiction, under subsection 12(1) of PIPEDA, to investigate complaints in respect of Air Canada's refusal to provide access to personal information on the basis that it was protected by solicitor-client privilege (under paragraph 9(3)(a) of PIPEDA) by requiring the provision of affidavit evidence in support of a claim of privilege.

The matter was heard in March 2010 and the decision of the Federal Court was issued on April 20, 2010.

On the issue of whether the Commissioner was entitled to request that Air Canada justify its claim of privilege by way of affidavit, Justice Harrington relied on the Supreme Court of Canada's decision in *Canada (Privacy Commissioner) v. Blood Tribe Department of Health,* [2008] 2 S.C.R. 574, determining that the Commissioner "could not stipulate the steps Air Canada had to take to satisfy her that the documents were truly privileged."

Justice Harrington held that it was the Federal Court that was the ultimate decision-maker with respect to the issue of solicitor-client privilege, and not the Privacy Commissioner. Justice Harrington was of the opinion that Air Canada had provided "sufficient particulars" to make out its claim of privilege to the Commissioner. Justice Harrington further noted that if the Commissioner did not agree with Air Canada's assertion of privilege, she could come before the Federal Court to have the issue decided.

On the issue of whether the documents withheld by Air Canada were privileged, Justice Harrington held that not all of the documents in question were privileged, as the airline had claimed. One report prepared by an Air Canada customer service representative was a "routine end-of-shift synopsis." Justice Harrington was of the view that this document was not privileged and ordered the company to provide the individual complainant with a copy of the report.

Privacy Commissioner v. Sobeys Inc.
Federal Court File No. T-243-10

This Federal Court application, initiated by the Privacy Commissioner under section 15 of PIPEDA, 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. As a result, the Privacy Commissioner determined that it would not be necessary to proceed with her application.

Privacy Commissioner of Canada v. Association of American Medical Colleges
Federal Court File T-1275-10

This Federal Court application, initiated by the Commissioner under section 15 of PIPEDA, 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.

At the time of writing this annual report, the parties had filed their affidavits and documentary exhibits in Court.

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

This application was initiated under section 15 of PIPEDA by the Privacy Commissioner. It 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 raises, 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 knowledge and consent. As well, it raises the issue of whether the GTAA provided the complainant with access to all of his personal information under its control.

Our Office is also seeking damages under paragraph 16(c) of PIPEDA due to facts surrounding the collection of personal information in the circumstances of this case.

At the time of writing this report, the matter was still pending before the Federal Court.

The complainant, who is represented by legal counsel, had also proceeded to file a separate application under section 14 of PIPEDA. The complainant was seeking various forms of redress, including damages.

Note: Further information about our investigation into this matter is included in Chapter 4.

6.2 Judicial review applications (section 18.1 of the *Federal Courts Act*)

State Farm v. The Privacy Commissioner of Canada and Attorney General of Canada
Court File No. T-604-09

This case stems from an application for judicial review filed by the State Farm Mutual Automobile Insurance Company (State Farm) pursuant to which State Farm challenged the Privacy Commissioner of Canada's jurisdiction to investigate a complaint against State Farm under PIPEDA.

In its application for judicial review, State Farm sought various forms of relief, including a declaration that State Farm is not engaged in commercial activities when it collects, uses or discloses personal information in the course of defending its insured against litigation initiated by the complainant and, if State Farm is found to be engaged in commercial activities in this context, that PIPEDA is not constitutionally valid.

This case was heard in April 2010 and Justice Mainville of the Federal Court issued his decision in July 2010.

In this case, a person (hereafter referred to as "G.") was involved in a car accident with another person (hereafter "V."), the latter being insured by State Farm. G. subsequently commenced legal proceedings against V. with respect to injuries and damages allegedly sustained in the accident.

State Farm hired an investigator to investigate G.'s claim. G. subsequently sought from State Farm access to his personal information stemming from the investigation, in particular copies of any surveillance tapes or reports about him. State Farm refused his request and G. filed a denial of access complaint with our Office. G. also complained that State Farm disclosed his personal information without consent and failed to safeguard his personal information.

Our Office commenced an investigation and sought information from State Farm relating to the investigation. State Farm refused to cooperate with the investigation or provide any information. State Farm took the position that it had not collected, used or disclosed G.'s personal information in the course of commercial activities and that, therefore, the Office did not have jurisdiction to investigate G.'s complaints.

State Farm commenced judicial review proceedings challenging the Privacy Commissioner's jurisdiction to investigate, naming the Privacy Commissioner and the Attorney General of Canada as respondents.

The following issues, among others, were raised before the Court:

- Is the collection of evidence by an insurer acting for one of its insured in the defence of a third-party tort action "commercial activity" within the meaning of PIPEDA?

- In the affirmative, is the application of PIPEDA to organizations that are not federal works, undertakings or businesses beyond the constitutional authority of Parliament?

On the first issue, Justice Mainville ruled that the collection of evidence on a plaintiff by an individual defendant, for the purpose of defending him or herself against a civil tort action brought by that plaintiff, is not a commercial activity within the meaning of PIPEDA because there is no commercial character associated with that activity.

In determining whether there is a commercial activity for the purposes of PIPEDA, Justice Mainville held that if the primary activity or conduct at hand is not a commercial activity contemplated by PIPEDA, then that activity or conduct remains exempt from the application of the Act, even if an individual retains third parties to carry out that activity or conduct on his or her behalf. Justice Mainville concluded that the primary characterization of the activity or conduct in issue is the dominant factor in assessing the commercial character of the activity or conduct.

Applying his analysis to the case at hand, Justice Mainville ruled that "the investigation reports and related documents and videos concerning G. and prepared by or for State Farm or its lawyers to defend V. in the civil tort action taken against her by G. are not subject to PIPEDA".

In so finding, Justice Mainville held that the Privacy Commissioner still has authority to investigate in this context. He noted that "there must nevertheless still be mechanisms in place to test the *bona fides* of the exemption or non-application claim".

However, Justice Mainville added that, where the organization being investigated raises solicitor-client privilege or litigation privilege, the Privacy Commissioner's investigative authority is limited in that regard, and noted that the Privacy Commissioner could pursue two other options: either refer the question to the Federal Court, or issue a report and bring an application to the Federal Court for relief under section 15 of PIPEDA.

Having found that the activity at issue did not constitute commercial activities, Justice Mainville did not address the constitutional questions raised by State Farm.

CHAPTER 7

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 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.

Newfoundland and Labrador's *Personal Health Information Act* (PHIA) received Royal Assent on June 4, 2008. It is expected to come into force in 2011.

New Brunswick's *Personal Health Information Privacy and Access Act* (PHIPAA) received Royal Assent on June 19, 2009 and came into force on September 1, 2010.

Nova Scotia's *Personal Health Information Act (PHIA)* received Royal Assent on December 10, 2010.

As requested by Industry Canada, we have reviewed Newfoundland and Labrador's Act and New Brunswick's Act and provided comments on whether they are substantially similar to PIPEDA. At the time of writing this report, we had not yet been asked to review Nova Scotia's Act. A proposal to declare New Brunswick's PHIPAA substantially similar to PIPEDA was published in the *Canada Gazette* on March 12, 2011. An Act cannot be declared substantially similar until it is in force.

CHAPTER 8
The Year Ahead

As we begin 2011, we expect another year filled with challenges and new issues.

Upon her reappointment for a three-year term in December 2010, the Commissioner stated that she plans to focus during the remainder of her mandate on: leadership on priority privacy issues; supporting Canadians, organizations and institutions to make informed privacy decisions; and service delivery to Canadians.

LEADERSHIP ON PRIORITY ISSUES

As Canadians live out more and more of their daily lives in this digital environment, it is clear that *that* is where we need to be focusing much of our attention as we fulfill our mandate to enforce PIPEDA. These are critically important issues in light of the role the Internet plays in daily life. Many Canadians now interact, shop, learn, and pretty much *live* online.

Looking ahead, we will continue to develop a deeper understanding of privacy issues in a digital world. We will build on our information technology expertise and create links with outside experts.

We will also continue to enhance cooperation with our territorial, provincial and international, colleagues.

SUPPORTING INFORMED PRIVACY DECISIONS

Another piece of the privacy protection challenge is making sure that Canadians develop strong digital literacy skills. We will continue to use online tools and other creative means to help Canadians better understand their privacy rights, and to make well-informed choices in a rapidly changing privacy landscape.

SERVICE DELIVERY

We will continue efforts to ensure that our work meets the needs and the expectations of Canadians. We will also remain responsive to the needs of businesses, government and Parliament.

A quick snapshot of what's ahead in 2011:

INQUIRIES AND INVESTIGATIONS

Our investigations and our inquiries functions are our most direct service to Canadians and therefore needs the best possible support structure. As we prepared this annual report, we were in the process of implementing some changes to our organizational structure. These include creating two distinct investigation units for complaints under the *Privacy Act* and PIPEDA. Each will have its own Complaints Registrar and be responsible for its own early resolution functions. Responsibility for our inquiries unit will move to our communications branch. This fresh approach will help ensure we have the best possible support structure for our most direct service to Canadians – our investigations and our inquiries functions.

ANTI-SPAM

With the passage in late 2010 of legislation aimed at combating spam, we look forward to working with the other agencies responsible for enforcement of the anti-spam legislation, the Canadian Radio-television and Telecommunications Commission and the Competition Bureau.

PRIVACY AND LEGISLATION

The second Parliamentary review of PIPEDA is expected to be launched in 2011.

Amendments could help ensure the law remains an effective tool for protecting the privacy rights of Canadians. This is a possibility we are considering. For example, we will be considering the conclusions of a report we commissioned from two leading academics, who analyzed the effectiveness of the ombudsman model. We are also looking at other compliance models worldwide.

We will welcome the eventual passage of long overdue amendments to PIPEDA that will require organizations to notify our Office and affected individuals following data breaches. That legislation was before Parliament at the end of 2010.

CONSULTATIONS

We will release the final report of our consultations with Canadians on online tracking, profiling and targeting of consumers by businesses; and cloud computing. In terms of next steps, we plan to increase our outreach efforts with the technical community, as well as small- and medium-sized enterprises by providing them with more targeted information and guidance materials. We expect to continue our outreach to younger Canadians and to provide more information about privacy to parents.

INTERNATIONAL

We will continue to assert Canada's leadership in international discussions on how to improve privacy protections around the globe. This will include our work with organizations such as the Asia-Pacific Economic Cooperation (APEC), the Organisation for Economic Cooperation and Development (OECD), the Ibero-American Data Protection Network, the *Association francophone des autorités de protection des données personelles* and the International Conference of Data Protection and Privacy Commissioners.

We plan to use our new legislated authority to share information with international colleagues with a view to addressing common challenges raised by global corporations.

We are very pleased that one of our staff members now participates in meetings of the Commission for the Control of INTERPOL's Files, chaired by our colleague from Ireland, Commissioner Billy Hawkes. This will provide a valuable opportunity for our Office to learn about international law enforcement issues and it will also allow us to contribute to ensuring that INTERPOL respects privacy protection principles.

APPENDIX 1
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:

- **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 ended before a full investigation of all the allegations. A case may be discontinued for any number of reasons – for instance, the complainant may no longer want to pursue the matter or cannot be located to provide information critical to making a finding.
- **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).** 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.

INVESTIGATION PROCESS UNDER PIPEDA

Inquiry:

An individual contacts OPC by letter, by telephone, or in person to complain of violation of the Act. Our inquiries officers provide information about the law and the role of our Office. A key question we ask is whether the individual has tried to resolve the issue directly with the organization. In many cases, a solution can be reached quickly and without a formal investigation.

↓

Complaint:

Where a problem cannot be resolved quickly, our inquiries staff review the matter to determine whether it constitutes a complaint, i.e., whether the allegations could constitute a contravention of the Act.

An individual may complain about any matter specified in Sections 5 to 10 of the Act or in Schedule 1 – for example, denial of access, or unacceptable delay in providing access, to his or her personal information held by an organization; improper collection, use or disclosure of personal information; inaccuracies in personal information used or disclosed by an organization; or inadequate safeguards of an organization's holdings of personal information.

Our inquiries staff help individuals to formulate their complaints and our online complaint form offers complainants detailed information about the information we will need.

↓

Complaints Registrar

Our Complaints Registrar reviews each complaint to ensure it is appropriate for our Office to investigate it. The registrar also assesses the complexity of the complaint; whether it is a high priority; and whether it can be resolved quickly.

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

Sent to Investigation:
Complaints of a serious, systemic or otherwise complex nature – for example, uncertain jurisdictional matters, multiple allegations or complex technical issues – are assigned to an investigator.

Sent to Early Resolution Officer:
Complaints which we believe could potentially be resolved quickly go to an Early Resolution Officer. These complaints include matters where our Office has already made findings on the issues; where the organization has already dealt with the allegations to our satisfaction; or where it seems possible that allegations can be easily remedied.

Investigation:

An investigation provides the factual basis for the Commissioner to determine whether the individual's rights have been contravened under PIPEDA.

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

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

Analysis (on next page)

Settled? (on next page)

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

Analysis:

The investigator analyses the facts and prepares recommendations to the Privacy Commissioner or her delegate. The investigator will contact the parties and review the facts gathered during the course of the investigation. The investigator will also tell the parties what he or she will be recommending, based on the facts, to the Privacy Commissioner or her delegate. At this point, the parties may make further representations.

Analysis will include internal consultations with, for example, Legal Services, Research, or Policy Sections, as appropriate.

Settled?

The OPC seeks to resolve complaints and to prevent contraventions from recurring. The Commissioner encourages resolution through mediation, negotiation and persuasion. The investigator assists in this process.

Findings:

The Privacy Commissioner or her delegate reviews the file and assesses the report. The Privacy Commissioner or her delegate, not the investigator, decides what the appropriate outcome should be and whether recommendations to the organization are warranted.

Preliminary report

If the results of the investigation indicate to the Privacy Commissioner or her delegate that there likely has been a contravention of PIPEDA, she or her delegate recommends to the organization how to remedy the matter, and asks the organization to indicate within a set time-period how it will implement the recommendation.

Final Report and Letters of Findings

The Privacy Commissioner or her delegate sends letters of findings to the parties. The letters outline the basis of the complaint, the relevant findings of fact, the analysis, and the response of the organization to any recommendations made in the preliminary report.

The possible findings are:

Not Well-Founded: The evidence, on balance, does not lead the Privacy Commissioner or her delegate to conclude that the complainant's rights under the Act have been contravened.

Well-Founded: The organization failed to respect a provision of the Act.

Resolved: The investigation substantiates the allegations but, prior to the conclusion of the investigation, the organization has taken or has committed to take corrective action to remedy the situation, to the satisfaction of our Office.

Well-founded and resolved: The investigation substantiates the allegations but the organization has taken or has committed to take corrective action to remedy the situation, as recommended in the Commissioner's preliminary report at the conclusion of the investigation.

No report prepared pursuant to subsection 13(2). 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.

In the letter of findings, the Privacy Commissioner or her delegate informs the complainant of his or her rights of recourse to the Federal Court.

Where recommendations have been made to an organization, OPC staff will follow up to verify that they have been implemented.

The complainant or the Privacy Commissioner may choose to apply to the Federal Court for a hearing of the matter. The Federal Court has the power to order the organization to correct its practices and to publish a notice of any action taken or proposed to correct its practices. The Court can award damages to a complainant, including damages for humiliation. There is no ceiling on the amount of damages.

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

APPENDIX 2
PIPEDA Investigation Statistics for 2010

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

EARLY RESOLUTION STATISTICS

Early Resolution Complaints Opened by Industry Sector

	Count	Percentage
Financial Sector	21	19.4
Telecommunications	16	14.8
Services	14	13.0
Insurance	13	12.0
Other	12	11.1
Sales/Retail	11	10.2
Transportation	9	8.3
Accommodations	4	3.7
Health	4	3.7
Entertainment	2	1.9
Professionals	2	1.9
Total	**108**	

Early Resolution Complaints Opened by Type

	Count	Percentage
Use and Disclosure	34	31.5
Access	28	25.9
Collection	19	17.6
Consent	10	9.3
Retention	6	5.6
Safeguards	5	4.6
Accuracy	2	1.9
Openness	2	1.9
Correction/Notation	1	0.9
No Jurisdiction	1	0.9
Total	**108**	

Early Resolution Complaints Closed by Industry Sector

	Count	Percentage
Financial Sector	24	30.0
Sales/Retail	11	13.8
Other	10	12.5
Telecommunications	10	12.5
Transportation	6	7.5
Insurance	5	6.2
Services	5	6.2
Accommodations	4	5.0
Entertainment	2	2.5
Health	2	2.5
Internet	1	1.3
Total	**80**	

Early Resolution Complaints Closed by Type

	Count	Percentage
Use and Disclosure	27	33.8
Access	23	28.8
Consent	10	12.5
Collection	8	10
Safeguards	5	6.3
Openness	2	2.5
Retention	2	2.5
Accountability	1	1.3
Accuracy	1	1.3
Correction/Notation	1	1.3
Total	**80**	

COMBINED EARLY RESOLUTION AND FORMAL COMPLAINT STATISTICS

Early Resolution and Formal Complaints Received by Type

Type	2010				2009	
	Early resolution	Formal complaints	Total	Percentage	Total	Percentage
Use and Disclosure	34	22	**56**	27	**59**	26
Access	28	22	**50**	24	**64**	28
Collection	19	14	**33**	16	**33**	14
Consent	10	20	**30**	14	**22**	10
Safeguards	5	8	**13**	6	**21**	9
Retention	6	4	**10**	5	**3**	1
Accuracy	2	2	**4**	2	**9**	4
Openness	2	1	**3**	1	**4**	2
Identifying Purposes	0	2	**2**	1	**0**	0
Other	1	1	**2**	1	**13**	6
Challenging Compliance	0	2	**2**	1	**2**	Less than 1
Appropriate Purposes	0	1	**1**	Less than 1	**0**	0
Correction/ Notation	1	0	**1**	Less than 1	**1**	Less than 1
TOTAL	**108**	**99***	**207**	**100**	**231**	**100**

*Note: Four complaints opened as early resolution files were ultimately transferred to investigations and are therefore included under the formal complaints column to avoid double counting.

In 2010, we received a total of 207 complaints in both streams – formal complaint (99) and early resolution (62 resolved and 46 ongoing files) – during 2010. That represents a 10 percent drop from the 231 complaints received in 2009.

As reported in section 4.2, a total of 112 complaints brought to our Office in 2010 were opened as early resolution files. In the past, those cases would have been sent directly to investigations.

Of the 112 early resolution files opened in 2010, 62 were successfully resolved, four were unresolved and transferred to investigations and another 46 were ongoing at the end of the year.

The top three types of complaints have remained consistent year over year.

Early Resolution and Formal Complaints Received by Industry Sector

Sector	2010				2009	
	Early resolution	Formal complaint	Total	Percentage	Total	Percentage
Financial	21	24	45	22	55	24
Services	14	21	35	17	9	4
Insurance	13	14	27	13	41	18
Internet*	0	19	19	9	--	--
Telecommunications	16	3	19	9	42	18
Sales/Retail **	11	7	18	9	25	11
Transportation	9	4	13	6	15	6
Accommodations	4	2	6	3	7	3
Professionals	2	4	6	3	10	4
Health	4	0	4	2	8	3
Entertainment	2	0	2	1	0	0
Other	12	1	13	6	19	8
Total			**207**	**100**	**231**	**100**

* In light of the growing number of online-related complaints we receive, we have begun counting Internet complaints as a separate sector. Previously, Internet complaints were counted under the Telecommunications sector.

In 2010, 19 individual complaints, or nine percent of all the complaints we received, related to the Internet, making it the third-largest industry sector for complaints. By way of comparison, we received 13 Internet complaints in 2009 – just over 5 percent of total complaints.

** The name of this category was previously "Sales" but it included complaints against retail organizations.

SECTOR DEFINITIONS:

- **Financial:** Banking, credit intermediation (ie. 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.
- **Other:** Includes manufacturing, no jurisdiction, publishers (except Internet), food and beverage

Closed Early Resolution and Formal Complaints by Disposition

Disposition	2010		2009	
	Cases	Percentage	Cases	Percentage
Well-founded resolved	76	23	61	10
Early resolution	80	24	76	13
Not well-founded	68	21	142	24
Resolved	32	10	51	9
Well founded	30	9	45	8
Discontinued	18	6	118	20
Report not issued under 13(2)	9	3	4	1
Settled	8	2	55	9
No jurisdiction	8	2	35	6
Total	**329 ***	**100**	**587**	**100**

* Includes 80 early resolution cases and 249 formal complaints

Closed Early Resolution and Complaints files by Type

	Well-founded resolved	Early Resolution	Not well-founded	Resolved	Well-founded	Discontinued	Report not issued under 13(2)	Settled	No jurisdiction	**Total**	**Percentage**
Access	25	23	15	12	8	4	8	3	2	100	30
Use and Disclosure	22	27	18	6	12	4	1	1	1	92	28
Collection	10	8	10	4	7	2	0	1	2	44	13
Consent	8	10	10	2	1	1	0	0	2	34	10
Safeguards	6	5	7	2	1	3	0	2	1	27	8
Accountability	3	1	3	3	0	2	0	0	0	12	4
Accuracy	0	1	3	2	0	0	0	0	0	6	2
Retention	1	2	0	0	0	1	0	1	0	5	2
Time Limit	1	0	1	0	1	1	0	0	0	4	1
Openness	0	2	0	1	0	0	0	0	0	3	1
Correction/ Notation	0	1	1	0	0	0	0	0	0	2	Less than 1
Total	76	80	68	32	30	18	9	8	8	**329**	

Closed Early Resolution and Formal Complaints by Industry Sector

	Discontinued	No Jurisdiction	Not well-founded	Report not issued under 13(2)	Resolved	Early Resolved	Settled	Well-founded	Well-founded resolved	**Total**
Financial Sector	2	0	13	1	7	24	2	3	17	**69**
Insurance	0	3	23	7	12	5	2	5	6	**63**
Other	0	0	5	0	3	10	2	11	10	**41**
Telecommunications	6	0	7	0	3	10	1	0	10	**37**
Services	0	3	3	0	4	5	0	3	13	**31**
Transportation	1	0	3	0	2	6	0	4	4	**20**
Health	1	0	8	0	1	2	0	2	5	**19**
Sales/Retail	3	0	2	0	0	11	0	2	1	**19**
Professionals	0	0	4	1	0	0	1	0	7	**13**
Internet	4	1	0	0	0	1	0	0	3	**9**
Accommodations	1	1	0	0	0	4	0	0	0	**6**
Entertainment	0	0	0	0	0	2	0	0	0	**2**
Total	18	8	68	9	32	80	8	30	76	**329**

“Services” includes: Services, Administrative and Support Services (includes collection agencies, credit bureaus), Social Assistance.

"Other" includes: Manufacturing, No jurisdiction, Publishers (except Internet), Food and Beverage

TREATMENT TIMES

Average Treatment Times by Complaint and Resolution Types

	Early resolution cases		Formal complaints	
Complaint type	**Number**	**Average treatment time in months**	**Number**	**Average treatment time in months**
Retention	2	1	3	7
Correction/Notation	1	7	1	10
Safeguards	5	2	22	13
Openness	2	4	1	15
Consent	10	3	24	17
Accuracy	1	5	5	18
Access	23	4	77	19
Accountability	1	2	11	18
Use and Disclosure	27	3	65	20
Time Limits	0	–	4	26
Collection	8	2	36	26
	Total 80	**Weighted average 3.16**	**Total 249**	**Weighted average 19.4**

Average Treatment Times by Disposition

Disposition	**Number**	**Average treatment time in months**
Early resolution	80	3
Settled	8	6
Discontinued	18	11
No jurisdiction	8	14
Report not issued under 13(2)	9	16
Not well founded	68	18
Well founded resolved	76	21
Resolved	32	22
Well founded	30	29
Total	**329**	**Weighted average 15.6**

Treatment times were measured from the date a complaint was *received* to when a finding is made or the case is otherwise disposed of.

In future annual reports, we will use a revised treatment time definition, specifically the date a complaint is *accepted* to when a finding is made or the case is otherwise disposed of. This is because the current definition leads to artificially high treatment times. In many cases, for example, we receive complaints that do not include all the information required in order to begin an investigation. We can't start our work until a complaint is complete.

We were pleased that our average complaint treatment time in 2010 declined to 15.6 months from 18.5 months the previous year.

The Commissioner has stated that one of her priorities over the next three years is service delivery to Canadians. One of the ways in which we will improve our service is by continuing to decrease our complaint treatment times.

Voluntary Breach Notifications –
By Industry Sector and Type of Incident

	Accidental disclosure	Loss	Theft	Unauthorized access, use or disclosure	Total
Accommodations	0	1	0	0	**1**
Administrative and Support Services	0	0	1	0	**1**
Construction	0	0	0	1	**1**
Entertainment	0	0	0	2	**2**
Financial	6	3	11	9	**29**
Health	0	1	0	0	**1**
Insurance	1	0	0	1	**2**
Internet	1	0	0	0	**1**
Professionals	0	0	1	0	**1**
Sales/Retail	0	0	0	1	**1**
Service	0	1	0	0	**1**
Telecommunications	1	0	1	0	**2**
Transportation	0	0	0	1	**1**
Total	**9**	**6**	**14**	**15**	**44**

As discussed in section 4.8, we continue to look forward to the passage of legislative amendments to establish a mandatory data breach reporting regime.

In 2010, two-thirds of voluntary breach reports came from financial institutions, which have adopted policies to proactively report breaches to our Office.

More than one-third of the breach reports involved unauthorized access to personal information, oftentimes by the organization's employees. Almost as many of the incidents involved the theft of personal information, for example, a stolen laptop.