Office of the
Privacy Commissioner
of Canada

PRIVACY

ANNUAL REPORT TO PARLIAMENT

2009

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. IP51-1/2009
ISBN 978-1-100-51132-0

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 2010

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, 2009.

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 2010

The Honourable Peter Milliken, 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, 2009.

Yours sincerely,

Original signed by

Jennifer Stoddart
Privacy Commissioner of Canada

TABLE OF CONTENTS

MESSAGE FROM THE COMMISSIONER

My fascination with privacy dates back to April 2000, when I happened to read a *New York Times Magazine* article about the erosion of privacy in the digital age.

The article, by the noted American legal scholar Jeffrey Rosen, described in frightening detail how access to personal information had become almost limitless thanks to computer-based technologies.

What struck me was the impossibility of deleting information and the illusions of privacy and security that we continue to indulge in – despite facts to the contrary.

Just a week after reading that article, I was asked to head up the *Commission d'accès à l'information du Québec*, where I was responsible for enforcing provincial privacy legislation. I jumped at the opportunity to work in such a challenging, engaging and important field.

A decade later, the threats to privacy have only multiplied. Jeffrey Rosen's closing call to action in the article that opened my eyes to the challenges of the digital world has become even more critical:

We are trained … to think of all concealment as a form of hypocrisy. But perhaps we are about to learn how much may be lost in a culture of transparency – the capacity for creativity and eccentricity, for the development of self and soul, for understanding, friendship and even love. There is nothing inevitable about the erosion of privacy in cyberspace, just as there is nothing inevitable about its reconstruction. We have the ability to rebuild some of the private spaces we have lost. What we need now is the will.[1]

1 Jeffrey Rosen, "The Eroded Self," *New York Times Magazine*, April 30, 2000

When I reflect back on how the Office of the Privacy Commissioner of Canada has worked to protect Canadians' private spaces over the past seven years, I am extremely proud of our accomplishments.

While the encroachments on our privacy in the digital era are immense, we have not allowed them to bowl us over. We are willing to take a strong stand when necessary, but I believe we have also developed a reputation for taking a reasonable, flexible approach to privacy.

In many ways, 2009 was a watershed year for the Office.

We saw an exponential growth in investigations dealing with new technologies – and it seems clear that technology issues will dominate our work in the years ahead.

Our investigation into a wide-ranging complaint against Facebook made waves around the world. And that was just the most high-profile example of our 2009 work to address the privacy risks stemming from new technologies, the Internet and our increasingly online world.

NEW TECHNOLOGIES

I am struck by how quickly technologies are transforming our lives – especially in the way we communicate.

It's hard to believe that the concept of online social networking didn't really exist when I became Commissioner, given that Facebook alone now has more than *400 million* users – and counting.

Back in 2003, we also didn't tweet on Twitter, share our photos and videos on Flickr and YouTube, tour neighbourhoods virtually on Google Street View, or follow one another's movements on location tracking services such as Loopt and Foursquare.

In the space of a few short years, even the telephone, it would seem, has become old-fashioned. A colleague recently described the horrified reaction of her university-aged daughter at the suggestion that she should actually pick up the telephone and call a friend: "Mom, you *do not* phone people; you text them."

It is increasingly clear that if data protection authorities want to remain relevant, the online world is where they need to be. And this is, indeed, where my Office has begun to shift more and more of its attention.

In 2009, our comprehensive investigation into Facebook's privacy policies and practices resulted in a commitment by this global social networking giant to make numerous changes in response to our concerns. We will be monitoring those changes in 2010 to ensure compliance with the agreement.

We also worked to address privacy risks related to other types of technological applications, such as street-level imaging, and deep packet inspection, which allows network providers to peer into the digital packets that make up transmissions over a network in order to, for example, search for viruses and spam. As a result of our interventions, both Google Street View and Canpages, which offer virtual, 360-degree tours of Canadian neighbourhoods, agreed to make changes to better respect the privacy rights of Canadians.

At the end of the year, we received a new complaint about Facebook, as well as complaints about another social networking site, an online dating service and some Internet retailers – setting the stage for online privacy issues to be a key focus of our work in 2010.

The online world – and technology more generally – will undoubtedly be the drivers of most emerging privacy issues in the years to come.

We've already responded to this shift by adding more technology experts to our staff. This team will support our investigation and inquiries work, and also provide advice and recommendations in support of audits and privacy impact assessment reviews, and reviews of proposed legislative and policy changes.

We are beginning to look at how we can deal with online privacy issues in a more proactive way in the future.

We will also need to look at our privacy laws and administrative structures to ensure they are keeping up with technological changes.

On the whole, the *Personal Information Protection and Electronic Documents Act* is working well and we have been able to apply the law to technologies and business models that didn't even exist when PIPEDA came into force. But it's important to ensure that it continues to meet the challenge of emerging trends.

CROSS-BORDER DATA FLOWS

Canada cannot function in isolation. The international picture is increasingly critical to protecting privacy here in Canada.

In today's wired world, my national mandate to protect the personal information of Canadians demands a global approach. Protecting privacy can no longer be done on a country-by-country basis – the international data flows are too great; the technologies are evolving too rapidly; and the jurisdictional challenges are too daunting.

Internet privacy challenges are international and therefore require global thinking and global solutions.

Transborder data flows have been an area of focus from the very beginning of my mandate. I have long been concerned about the risks to Canadians when personal information flows to countries with little or nothing in the way of legislated privacy protections. As well, privacy issues that cross borders can raise jurisdictional questions and be far more complex to investigate.

In order to address the growing challenges, we have been a keen participant in several initiatives aimed at developing global privacy solutions.

In 2009, I had the honour of being invited to lead a volunteer group that is helping the Organisation for Economic Co-operation and Development plan a series of events marking the 30th anniversary of the OECD Guidelines on the Protection of Privacy and Transborder Data Flows. PIPEDA is more closely based on the OECD guidelines than any other legislation in the world.

The need for international privacy standards has been a cause close to my heart from the earliest days of my mandate. I remain convinced that we will never be able to effectively protect the personal information of Canadians unless we develop a global privacy solution.

BUILDING A REGIONAL PRESENCE

It has also been a priority for me to build stronger connections with Canadians wherever they happen to live and work. I want to ensure that the Privacy Commissioner's Office is not perceived as either too Ottawa-centric or unaware of issues outside the National Capital Region.

Perhaps partly because I am a former provincial commissioner myself, I have always seen a need to build stronger ties with provincial colleagues and other stakeholders across the country.

A couple of years ago, Parliament agreed that we needed a stronger regional presence, and funded our Office accordingly. As a result, we have a number of initiatives underway.

In Saskatchewan, for example, we are working with the province's Information and Privacy Commissioner on a number of projects, including the development of privacy tools for Saskatchewan credit unions and small businesses.

We have also engaged a new Senior Research and Outreach Advisor to act as the face of our Office in Atlantic Canada. His outreach work is aimed at empowering individuals and business organizations in the region to protect and promote privacy.

We have recently begun looking at how to develop a more effective presence in the Toronto region, where much of Canada's business takes place. Two-thirds of our complaints against private-sector organizations involve companies headquartered in Ontario.

In recent years, we have also increased our collaboration with provincial counterparts – particularly those with their own private sector privacy legislation. For example, we've conducted joint investigations and developed numerous joint guidance documents for businesses.

STRENGTHENING THE OPC

I am happy to say that one of the biggest challenges I faced when I first joined the Office in 2003 is now well behind us. My appointment came as the Office was emerging from extremely challenging times.

A big part of my job in the first few years was getting our house in order after a tumultuous period of administrative, financial and organizational crises. We implemented a strong new management and financial framework.

The fourth and fifth years were about consolidation – our rebuilt Office emerged as an effective organization.

Our focus then shifted back to where it should be: fulfilling our mandate to protect the privacy rights of all Canadians. We're conducting ground-breaking investigations and reaching out in innovative ways to individuals and organizations.

Parliamentarians increasingly turn to us for advice; we receive speaking requests from every corner of the country; and we are a sought-after participant in global privacy discussions. All of this tells me that we are seen as a credible and respected voice for Canadians on privacy.

CONCLUSION

As Privacy Commissioner, I am secure in the knowledge that the work of my Office matters – that it makes a real and positive impact on the lives of Canadians.

While we keep hearing in certain circles that privacy is dead in this age of digital exhibitionism, I strongly disagree – as do many Canadians who contact my Office.

Privacy changes shape and it changes context. It looks different to each generation. This is nothing new.

My generation recorded its secrets in diaries that we tucked under the mattress. Many of today's youth pour their hearts out over the Internet – potentially for all the world to see.

Although notions about privacy do shift, the concept of privacy continues to be critical – even for those who share so much online. Some version of privacy will *always* play a central role in democratic societies, where individuals are respected and their personal dignity is protected.

I confess that increasingly complex threats to privacy sometimes keep me up at night and that I struggle to understand the desire of some to make so much of their private lives so public.

That said, I am fundamentally optimistic about the future of privacy. This is because I take comfort in the fact that people *do* care about privacy.

One of the great privileges of being Privacy Commissioner is having the opportunity to meet Canadians from across the country. And, over the years, I have been struck by the fact that so many people – old *and* young – speak with deep passion about the need for privacy. When we went public with the results of our Facebook investigation, for example, it was incredibly gratifying to receive so many congratulatory e-mails and phone calls. I don't think this Office has ever seen such a strong public reaction. It was very moving.

Privacy remains an important and cherished value for Canadians – and indeed millions of people around the globe.

As Privacy Commissioner of Canada, I have the honour and the tremendous pleasure of working with many talented individuals – inside my own Office and beyond – who are dedicated to ensuring that privacy rights are protected.

The relatively small team at the Office of the Privacy Commissioner of Canada has been able to achieve some remarkable accomplishments thanks to their devotion to their jobs and passion for the issues – not to mention plenty of grit and determination! They have continually impressed me since the first day I arrived in the office.

I would be remiss if I did not single out Assistant Commissioner Elizabeth Denham for her strong leadership on private-sector issues. She has expertly guided the Office's work in the new realm of enforcing PIPEDA in an online context. Assistant Commissioner Denham has raised awareness about PIPEDA obligations and championed the cause of data breach notification by strengthening our relationships with the business community, where she has developed a reputation of being fair and forthright. She fully understands the need to reach out across this wide country and work closely with provincial Commissioners. She has been a highly effective champion of our work to increase our regional presence across Canada. Her many successes are a result of her practical approach to every issue.

Privacy continues to be a value worth fighting for. I am deeply grateful to the many people who agree with me and are working in their own ways to ensure that privacy and the protection of personal information remain a defining Canadian value.

EXECUTIVE SUMMARY

INTRODUCTION

The dominant theme of our work in 2009 was the protection of privacy in an increasingly online, borderless world.

A case in point was the investigation that resulted in more public attention than any other in our Office's history: Facebook.

The investigation was a huge undertaking for us because it was wide-ranging and the issues were incredibly complex and, in some aspects, highly technical. We were also dealing with a multinational organization based in the United States.

We expect that, as people continue to spend more time online, we will see a growing number of complaints about online organizations. And, with the digital world erasing the borders between countries, more complaints will be about organizations outside Canada.

DATA WITHOUT BORDERS

We live in a world in which global data flows have become multipoint and multidirectional.

These streams of personal information circling the globe are only going to increase as more individuals take advantage of information and communication technologies.

There are currently some 1.5 billion Internet users. A billion more people are expected to join the online world in the next 10 years, with many of the new users coming from countries such as China, India and Brazil.

The need for a global privacy standard is clear, given global data flows and ubiquitous communication and information technologies. In our interconnected world, we need to take a co-operative approach to protecting personal information.

In 2009, our Office worked with several organizations and initiatives to develop a global privacy solution, including the Organisation for Economic Cooperation and Development, Asia-Pacific Economic Cooperation, International Conference of Data Protection Commissioners and the International Organization for Standardization.

RESPONDING TO CANADIANS

One of the most important ways we serve Canadians is through our inquiries service and investigations branch.

In 2009, we handled 5,095 new inquiries about issues that fall under PIPEDA. These calls and letters dealt with everything from how to ask an organization for access to personal information to whether a particular company has the right to collect a digital fingerprint.

We find that more people are turning to our website when they are seeking information about privacy issues. In 2009, we developed many materials and tools for our website, including complaint and data breach reporting forms and numerous fact sheets and guidance documents for business.

Our Office received 231 new PIPEDA-related complaints for investigation in 2009 – a drop from the 422 we received the previous year.

Part of this decrease is explained by the fact that we are encouraging people to try to resolve issues directly with organizations before they make an official complaint. We're finding that many problems can be dealt with quickly – and in a way that is satisfactory to would-be complainants.

Our investigations dealt with a wide range of issues, including the online collection and use of personal information; covert surveillance by private investigation firms; workplace surveillance, such as the use of video cameras and location-tracking devices, and the collection of driver's licence information by retailers.

We closed 587 complaints in 2009, a significant increase compared with 412 the previous year. Our concerted effort to eliminate a backlog of complaints was successful, and this will allow us to complete future investigations far more quickly.

We were pleased that many private-sector organizations voluntarily reported data breaches to our Office. We received 58 breach reports in 2009. That was fewer than the previous year, when a large number of mortgage brokers reported breaches to us.

PROTECTING PRIVACY IN A CHANGING ENVIRONMENT

We continued to stress the need to ensure that laws keep up with changing threats to privacy.

We welcomed the adoption of legislation to combat identity theft through amendments to the *Criminal Code*.

Important legislation aimed at fighting electronic spam, the *Electronic Commerce Protection Act*, was also introduced and we hope it will be passed into law in the near future. Canada is currently the only G-8 country without anti-spam legislation.

That bill also included legislative amendments that would increase our Office's ability to share information about spam and other privacy issues with provincial and foreign counterparts who enforce laws similar to PIPEDA. It would also provide the Commissioner with greater discretion to accept complaints or discontinue investigations.

New technologies sometimes put privacy laws to the test – and this was the case in 2009 as well. Social networking sites and online street-level imaging applications, for example, highlighted new ways of collecting and using personal information.

We found that PIPEDA – a technology-neutral and principles-based law – appears to be flexible enough to guide commercial uses of new technology.

While we addressed privacy concerns in social networking as part of our investigative work, we dealt proactively with our concerns about street-level imaging during a series of discussions with Google Street View and Canpages. These discussions resulted in improved privacy protection on both websites.

We also did extensive work on the issue of deep packet inspection – both as part of an in-depth investigation and submissions to the Canadian Radio-television and Telecommunications Commission (CRTC). As well, we created a website showcasing a series of essays on deep packet inspection by leading academics and professionals working in telecommunications, law, privacy, civil liberties and computer science. The project grew out of our desire to better understand a technology that can be a tool for network traffic management, behavioural advertising, and law enforcement. We hope it will promote discussion about the privacy implications of deep packet inspection.

PRIVACY BY THE NUMBERS

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA IN 2009

PIPEDA inquiries received	5,095
PIPEDA complaints received	231
PIPEDA investigations closed	587
Draft bills and legislation reviewed for privacy implications	12
Private-sector policies or initiatives reviewed	15
Policy guidance documents issued	19
Research papers issued	7
Parliamentary committee appearances made	18
Other interactions held with Parliamentarians or staff	69
Speeches and presentations delivered	148
Formal visits from external stakeholders	32
Contribution agreements signed	12
Research contracts signed	7
Hits to Office website	1,695,564
Hits to Office blog	488,829
Total	2,184,393
Publications distributed	13,689
Media interviews provided	327
News releases and fact sheets issued	24

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

KEY ISSUE:
DATA WITHOUT BORDERS

The increasingly global nature of information flows is raising complex challenges for privacy. Our Office has been a strong advocate for a global approach to protecting privacy when personal information crosses borders.

We live in a world where countless bits of information about us – address, birth date, credit card numbers, financial information, buying habits and more – are constantly streaming around the globe.

Dramatic advances in communications and information technologies are making transborder data flows the rule rather than the exception.

A real-life example described in a 2009 report on global data privacy illustrates how extensive and complex data flows can be:

A marketer in Spain uses criteria developed by an analytics vendor in India to select a list of customers from a global customer relationship management system in the United States. This customer list is transferred to a telemarketing call centre in Mexico, which contacts the Spanish consumers. Those telemarketing campaign results are ultimately fed back to the United States in order to update the customer management system.[2]

This single marketing campaign involved sending personal data back and forth between *four* countries and *three* continents. Personal information from this single transaction is subject to the jurisdiction – and the vastly different privacy regimes – of each of those countries.

2 Paul M. Schwartz, "Managing Global Data Privacy," The Privacy Projects (2009).

Many of our own routine, daily activities involve our personal information leaving the country.

When we send e-mail, search the Internet or buy things online, our personal information may find its way into databases located in countries with less robust privacy protection regimes.

And when we provide information about ourselves over the telephone in order to book a home service call or for computer help it's increasingly likely that we're speaking to someone on the other side of the globe.

These shifts are changing the nature of our work. For example, we have received complaints from Canadians about online companies that have no, or little, physical presence in Canada. The Facebook investigation has been the most prominent, but not the only example to date.

Our message to business has been consistent: If you offer online products and services in Canada, you must ensure that you are in compliance with Canadian privacy laws.

The fact that we are seeing a growing number of complaints involving more than one jurisdiction has prompted us to explore ways in which to increase our collaboration with data protection regulators at the provincial level as well as in other countries.

It has been said that "the blood running through the veins of twenty-first century commerce will increasingly consist of information about individuals." [3] Those veins clearly stretch around our planet.

At the same time, more and more personal data is being shared between the private sector and governments trying to combat terrorism and transnational crimes such as fraud and money laundering.

When personal information moves across borders, people may lose some of their privacy rights such as the ability to request access to their information to ensure its security or to seek redress by a data protection authority.

3 Gehan Gunasekara, "The 'Final' Privacy Frontier? Regulating Transborder Data Flows," International Journal of Law and Information Technology Vol. 17 No. 2 (2009).

INTERNATIONAL EFFORTS

Increasingly, the only way to protect Canadians' privacy is by working with other countries to ensure adequate levels of protection for personal information around the globe.

International affairs have been a top priority of our Office for several years. We are working on global privacy solutions with a number of international organizations.

It's important to be involved for many reasons: Robust international standards are critical for the privacy rights of Canadians; we can influence outcomes by being involved; and our own data protection model – which takes a flexible, principles-based approach – is well worth promoting to other countries and international bodies.

In 2008, the Parliamentary Panel on the Funding and Oversight of Officers of Parliament recommended and Treasury Board approved giving us additional resources to support our international efforts – very important recognition of the need for a global response to the changing nature of privacy issues.

The urgent need for an international approach has also become clear to governments, data protection regulators, consumer advocates and multinational corporations around the world.

Indeed, this recognition has led to a number of initiatives – old and new – aimed at developing an international response to better protect global flows of personal information.

The search for these global solutions is not without its challenges.

It can be difficult to bring countries with different approaches together. Even on our own continent, the three largest countries have vastly different legal traditions when it comes to privacy.

Our Office has approached the international dialogue with the goal of establishing an equivalent level of basic protection around the world – one reflecting legal and cultural differences.

The following is a description of some of our involvements in international discussions on privacy protection.

OECD

The Organisation for Economic Cooperation 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.

We work closely with Industry Canada, which represents the Government of Canada, to ensure that we support the important work happening at the OECD.

The OECD Guidelines on the Protection of Privacy and Transborder Data Flows will be 30 years old in 2010. To mark the anniversary, the OECD is planning a series of events in 2010 to commemorate the Guidelines and to begin a discussion about whether they need to be revised.

Commissioner Stoddart has been asked to head a volunteer group helping the OECD plan these events. Our Office will help draft a discussion paper that will describe the new privacy environment and identify the challenges to protecting personal information in the 21st century. We are also participating in the planning of two workshops and a conference that will be held in October 2010 in conjunction with the International Conference of Data Protection and Privacy Commissioners.

The OECD Guidelines, which are directly reflected in PIPEDA, have stood the test of time and we look forward to participating in these events in 2010.

APEC

Important work is also taking place within the Asia-Pacific Economic Cooperation (APEC) in terms of implementing the APEC Privacy Framework. We think it's critical for Canada to be at the table for APEC discussions on privacy issues. We have an interest to ensure that Canadians' personal information is protected wherever it flows, and, increasingly, it is flowing to our Asia-Pacific neighbours.

APEC's 21 members – which account for over 40 percent of the global population and half of the world's trade and total economic output – are at very different stages in terms of the development of their economic, social and legal institutions. Canada, New Zealand, Australia and Hong Kong have roughly comparable privacy regimes, but the majority of APEC economies don't have privacy legislation.

Most of the work taking place at APEC's Data Privacy Subgroup is focused on developing "cross-border privacy rules" to govern transborder flows. Our Office has

been particularly involved in developing a framework to facilitate cooperation among enforcement authorities.

The APEC process is important because it exposes member economies without privacy regimes to principles and concepts that will be helpful as they develop domestic laws.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION

The development of privacy-related standards for the use and deployment of new and existing technologies has been the subject of considerable debate and discussion within both the international standards community and the international data protection community.

The International Organization of Standardization, better known as the International Standards Organization, or ISO, signalled its intention to push ahead with this work with the creation of a working group on identity management and privacy technologies in 2006.

Our Office has been an active participant in efforts by ISO to develop and maintain standards and guidelines addressing security aspects of identity management, biometrics, and the protection of personal information.

ISO's key projects in 2008-2009 included working towards a framework for identity management, a privacy framework, as well as identifying requirements for additional future standards and guidelines related to specific privacy-enhancing technologies.

A senior member of our Office chairs the Canadian Advisory Committee feeding into this international work and also heads the Canadian delegation to the ISO working group responsible for identity management and privacy technologies. In addition, he is the liaison officer responsible for presenting the views of the International Conference of Data Protection Commissioners to this ISO working group.

THE SPANISH INITIATIVE

At the 31st International Conference of Data Protection and Privacy Commissioners the world's data protection authorities endorsed a Draft International Standard on the Protection of Privacy that was developed under the leadership of the Spanish Commissioner, Artemi Rallo Lombarte.

The draft standard was developed by an international working group with representatives from a broad range of stakeholders, including Assistant Commissioner Elizabeth Denham.

Reaching agreement on broad data protection principles was a valuable first step towards a harmonized approach to data protection. The standard demonstrates that we can agree on high-level principles.

THE ACCOUNTABILITY PROJECT

The Accountability Project is considering what it means for an organization to be accountable for the personal information it collects and how it can demonstrate its accountability to data protection authorities and individuals.

The concept of accountability is central to PIPEDA. Assistant Commissioner Elizabeth Denham participated in the discussions that have taken place as part of the Accountability Project, which have helped us think more clearly about what the concept involves.

The discussions have also been useful because they have brought together global businesses and data protection authorities from around the world – two groups which haven't talked enough in the past. It has provided the opportunity for some big-picture, forward-looking thinking.

At the 2009 data protection commissioners' conference, the American-based Center for Information Policy Leadership and the *Commission Nationale de l'Informatique et des Libertés* (CNIL), the French data protection authority, announced Part II of this project, to be completed in 2010. This is important work globally and we will be participating in the second phase.

FRANCOPHONIE

Our Office continues to be involved in the activities of the *Association francophone des autorités de protection des données personnelles*, the organization representing francophone data protection authorities from around the world.

In late 2009, Assistant Commissioner Chantal Bernier attended the francophonie association's third international conference in Madrid, Spain, where she made a presentation on personal data protection in a globalized world.

In November 2009 we published a report providing an overview of the Canadian approach to privacy protection. We collaborated on the report with the privacy commissioners of Canada's two francophone provinces – Quebec's *Commission d'accès à l'information* and New Brunswick's Office of the Ombudsman. The report was distributed widely among members of the francophonie association.

MEMORANDUM OF MONTEVIDEO

Youth privacy is a priority for our Office. In July, we took part in the Montevideo Group's work on youth online privacy in the Americas.

The group brought together experts from various Latin American countries who adopted the Memorandum of Montevideo, which presents guidelines for legislators, government departments and agencies, businesses and educational institutions in Latin America to help them develop policies, practices and programs aimed at protecting youth privacy on the Internet.

In December 2009, we took part in the official launch of the Memorandum of Montevideo in Mexico.

Over the past few years, we have developed close ties with individuals working in the field of personal information protection in Latin America. We are committed to increasing this cooperation to promote youth privacy rights.

OTHER INTERNATIONAL INITIATIVES

We are seeing a number of other initiatives which could eventually have an impact on international privacy.

For example, the Security Prosperity Partnership – involving Canada, the U.S. and Mexico – has a committee looking at how protecting personal information when it crosses North American borders can facilitate trade and economic growth.

Meanwhile, the European Commission has launched a review of the European data protection framework which could result in significant changes to the European model that would bring us one step closer to a harmonized global approach.

In 2009, our Office accepted invitations to attend meetings of the Article 29 working group that advises the European Commission on data privacy and security. In one case, our European counterparts were interested in hearing from our Office and our counterparts in Quebec about how federal and provincial laws applied to the work of the World Anti-Doping Agency, which is headquartered in Montreal. We were also invited to attend hearings organized by our European colleagues on privacy issues related to search engines. Participating in the meetings offered us the opportunity to better understand what's going on in Europe and to share information about how Canada is addressing the cross-border data flow challenge.

Change also appears to be underway in the United States. The new Director of the U.S. Federal Trade Commission's Consumer Protection Bureau has said it is time for the body to "reconceptualize its privacy mission and to look for a new framework to approach privacy issues." David Vladeck, appointed in 2009, has advocated a view that data protection involves human dignity and privacy issues – and is more than simply a consumer harm problem.

We will be watching developments in the United States with great interest given the potential impact on the privacy of Canadians.

COLLABORATIVE ENFORCEMENT

Another important way in which data protection regulators are responding to expanding cross-border flows of information is by working together – both within Canada and outside.

Our Office has built strong working relationships with provinces that have their own private-sector privacy legislation. We have conducted joint investigations and have signed a memorandum of understanding on co-operation and collaboration in private-sector privacy policy, enforcement and public education with the offices of the information and privacy commissioners in Alberta and British Columbia.

We regularly collaborate with our provincial counterparts to ensure that, as much as possible, we take a consistent approach to addressing issues.

This is why we have worked with provincial counterparts to develop joint guidance for businesses on issues such as the collection of driver's licence information.

We have also launched some joint public education initiatives aimed at both individuals and organizations. In Saskatchewan, for example, we are working in partnership with our provincial counterpart to develop privacy tools for credit unions and small businesses, with a view to using the lessons learned in other provinces and territories. As part of this work, we, in partnership with the Saskatchewan Office of the Information and Privacy Commissioner, are developing a co-branded website to deliver content and interact with Saskatchewan credit unions and small- and medium-sized businesses.

We've seen here in Canada that we can accomplish more by working in partnership. We'd like to bring this experience to the international level in the future.

INTERNATIONAL COOPERATION

At present, our ability to work collaboratively with our international counterparts on enforcement matters is limited by provisions in PIPEDA that restrict our ability to share information. However, this may change in the near future.

The *Electronic Commerce Protection Act*, introduced in the House of Commons in April 2009, included much-needed anti-spam provisions, (see page 73 for details) but would also increase our Office's ability to share information with provincial and foreign counterparts who enforce laws similar to PIPEDA, allowing us to more effectively pursue investigations. Following the prorogation of Parliament at the end of 2009, this bill may be reintroduced and passed in the next session and we would welcome this step.

While we hope to be able to collaborate on investigative work in the future, we have already begun to cooperate with international organizations in other ways.

In 2009, for example, we saw the conclusion of court action taken by the U.S. Federal Trade Commission (FTC), proceedings in which we intervened at the appellate level, filing a submission in support of the FTC's position. The case involved an American online data broker, Abika.com, which was operating in Canada in violation of our laws. Our Office was granted leave to file an *amicus curiae* brief (a written submission to help guide a court in its decision-making process) in a proceeding before the United States Tenth Circuit Court of Appeals. We were also able to bring our investigation of Abika.com to a conclusion based on information provided to us by the U.S. FTC. (See pages 44 and 87 for more details.)

FUTURE GLOBAL DIRECTIONS

Many seeds are being planted, both in terms of work on international standards and closer cooperation, and it will be interesting to see how the current efforts will develop over the long term.

At this point, what we know is that there is tremendous value in the increased dialogue between various groups – data protection authorities, academics, business and advocates.

A single, global standard may be the ideal, although achieving it will be difficult. In the meantime, we should remain open to a combination of approaches that reflect differing social and cultural values.

The key will be to recognize the common elements in our different approaches and then connect the dots between them to better protect privacy on a global basis.

KEY ISSUE: RISKS REMAIN IN WAKE OF MORTGAGE BROKER BREACHES

An audit of selected mortgage brokers identified numerous outstanding risks to personal information following breaches which involved alleged criminal wrongdoing.

Red flags about privacy issues with a number of mortgage brokers went up in our Office when a string of Ontario brokers notified us of breaches involving the personal information of hundreds of people.

In each of the 14 breaches reported to us in the space of a few months in mid-2008, someone impersonating an experienced mortgage agent downloaded credit reports for people who hadn't even applied for a mortgage.

Credit reports, which contain extensive personal information, are attractive to criminals because they can be used to commit identity fraud. For example, they may include a date of birth, social insurance number and details of credit transactions and payments.

The alleged thefts by a small number of individual "rogue" agents became the subject of investigations by law enforcement agencies. (In light of these ongoing investigations, we are unable to provide detailed information related to the alleged criminal activity.)

Due to the serious and systemic nature of the incidents, the Privacy Commissioner determined there were reasonable grounds to warrant an audit of the personal information handling practices of selected mortgage brokers under Section 18 of PIPEDA.

We audited five Ontario-based brokers that had reported multiple breaches. The audit was aimed at assessing whether the selected brokers have developed and implemented policies and procedures which are sufficient to protect personal information.

While the mortgage brokers had taken some positive steps, our audit highlighted many serious outstanding issues that left the personal information of clients – not to mention any number of other people with no connection to the brokerages – at risk.

We concluded that the companies had failed to implement technological controls to raise the alarm about any future suspicious activity. We also had concerns about – among other things – security; haphazard storage of documents containing personal information; inadequate consent by clients; and a general lack of understanding about, and accountability for, privacy issues.

BACKGROUND

Brokers and their agents offer products, rates and terms for individuals seeking mortgages, and act as intermediaries between individuals and lenders, including banks and credit unions.

Mortgage brokers represent a large and growing segment of the mortgage industry in Canada. A 2009 Canada Mortgage and Housing Corporation survey showed that mortgage brokers accounted for one-quarter of all mortgage transactions, and 44 percent of first-time home buyers used mortgage brokers to secure funding for their homes.

Brokers and agents make extensive use of personal information to provide mortgage products for their clients. During the mortgage application process, they collect personal information such as name, address, telephone numbers, dates of birth, social insurance numbers, marital status, dependants, employment information, income, assets and liabilities.

Some of this information is used to obtain credit information about the person seeking a mortgage. Brokers and agents purchase credit reports from credit reporting agencies in order to assess the individual's eligibility for a mortgage.

Both the application and credit report information is shared with lenders and can be shared with mortgage insurers.

Our audit closely examined the policies, systems, administrative controls and safeguards implemented by five mortgage broker franchises located in Ontario, as well as four national brokers' head offices in Toronto and Vancouver. (One of the audited mortgage brokers was independent and therefore did not have a head office.)

As part of our work, we met with officials from the Canadian Association of Accredited Mortgage Professionals, the Independent Mortgage Brokers Association of Ontario and

the Financial Services Commission of Ontario. As well, we had discussions with law enforcement officials.

WHAT OUR AUDIT FOUND

During our audit, we concluded that the breaches were the result of a failure by mortgage brokers to fulfill their obligations under Canadian privacy law. PIPEDA requires that organizations safeguard the information they collect and protect it from unauthorized access. However, the brokerages did not have adequate controls to restrict – or to otherwise monitor access to credit reports and lacked rigorous hiring processes – leaving the door open for unauthorized access to personal information.

Since the breaches occurred, the audited mortgage brokers have significantly tightened their hiring practices. However, they still did not have proper controls to limit access or monitor access to credit reports.

Our audit found significant vulnerabilities with a web-based tool that brokers use to obtain credit reports. The breaches occurred when deceptive mortgage agents improperly downloaded hundreds of credit reports that were not required for mortgages. Months after the breaches, there was still no capacity for mortgage brokers to proactively monitor for suspicious activity or to place limits on the number of credit reports that an agent can download.

We also identified concerns about a lack of comprehensive privacy policies, procedures and training. While the mortgage brokers we audited were at different levels of privacy compliance, none fully met their obligations under PIPEDA.

KEY FINDINGS AND RECOMMENDATIONS

I. Safeguarding Personal Information

Organizations subject to PIPEDA are required to protect personal information by implementing security safeguards that are proportionate to the sensitivity of the information. We found shortcomings in several areas:

Risks to personal information had not been evaluated

None of the brokers had undertaken a threat and risk assessment to define threats, evaluate the associated risks, and recommend mitigating actions to address vulnerabilities.

Undertaking this type of assessment and acting on the recommendations could have helped these organizations meet their safeguarding obligations under PIPEDA. In the absence of a threat and risk assessment, they couldn't show they'd identified and mitigated security risks.

Physical security at varying levels of sophistication

We found varying levels of security among the five mortgage brokers.

Some mortgage brokers did not have alarm systems to protect their places of business – not even the one who informed us that a neighbouring business had been burgled.

All but one brokerage had solid and secure walls running around their suites of offices. However, none had solid interior walls that completely enclosed individual offices, including above their dropped ceilings. This raised the risk of unauthorized access, because someone could simply remove a ceiling tile in one area, then climb over the interior wall into a neighbouring office.

Inconsistencies in document storage

Some brokers we examined used secure filing cabinets, while others stored files in unlocked cabinets or stacked files openly on the floor or on desks within accessible offices. One broker had overflow storage in an unsecured parking arcade.

In addition to paper files, all brokers we examined keep copies of electronic files containing mortgage applications, credit reports, and spreadsheets. Computer network systems holding mortgage applications and credit reports were protected with log-in requirements and virus protection software. However, none had been tested for vulnerabilities.

Inadequate controls on access to credit reports

Mortgage brokers and agents use a web-based tool in order to obtain credit reports, which are used to assess a client's creditworthiness for mortgage products.

As discussed above, the breaches were the result of rogue agents downloading large numbers of credit reports for people who had not even applied for mortgages. This problem went unnoticed for some time.

We tested the web-based tool used to access credit reports and found that there were controls in place to authorize access to the credit reporting system. The system was encrypted and it required a log-in password.

We were deeply concerned, however, by the lack of a proactive system or measures to monitor for suspicious activity and then provide an alert. As well, due to limitations in the web-based tool, brokers were unable to limit the number of credit reports that their agents can download.

These types of controls are commonly used in other industries. For example, many organizations that provide employees with corporate credit cards use controls to monitor purchases, set spending limits and track total spending – thereby reducing the possibility of fraud.

The absence of controls meant there were only two ways for brokers to independently identify inappropriate access to the credit reporting system. The first was to review computer log files – a cumbersome process requiring technical expertise. Alternatively, a broker could monitor agents' activities by checking invoices from credit-reporting agencies for downloaded credit reports. In other words, a problem could only be identified *after* the fact.

In the breaches reported to us, the brokers discovered the suspected thefts of credit reports in a few ways. In some cases, credit reporting agencies spotted suspicious activity and contacted the brokers. As well, a few people who had requested their credit reports noticed the unauthorized credit checks and alerted the brokerages. Some brokers realized there was a problem after receiving unusually large invoices for credit report requests.

Our testing also raised concerns about the creation of duplicate files containing personal information. When a credit report is accessed electronically, a duplicate report remains in the requesting computer's "temporary" folder. Unless the contents of this folder are deleted, the credit report will remain on the computer.

Although we did not find cases where such duplicate versions resulted in a breach, there is a potential risk if computers are shared or if credit reports are accessed on public computers (ie. at an Internet café or library). Another concern is that computers containing duplicate reports could be disposed of without the necessary precaution of overwriting the hard drive – leaving highly sensitive personal information easily accessible.

Safeguard Recommendations

Audited mortgage brokers should ensure that:

- Adequate physical measures are in place, such as alarms and lockable filing cabinets; and,

- Additional controls are put in place to safeguard credit reports and limit the number that can be downloaded.

II. Identifying purpose, collection, consent, use, retention and disclosure

Organizations subject to PIPEDA are required to comply with certain fair information principles. For example, they must:

- Clearly identify the purposes for the collection of personal information before or at the time of collection;
- Obtain consent for the collection, uses and disclosures of personal information;
- Limit the information being collected to the minimum required to meet the identified purposes;
- Use and disclose the personal information only for the purpose for which it was collected; and,
- Retain personal information only for as long as necessary.

We found problems in all of these areas when we examined the mortgage brokers' privacy polices, consent agreements and procedures:

Privacy policies not always sufficiently detailed

Privacy policies are important documents that guide how an organization protects the personal information entrusted to its care. They also inform clients and would-be clients about what an organization will do with their personal information.

Two brokerage head offices we reviewed had very detailed privacy policies posted on their websites. By contrast, another broker we examined had a privacy policy posted on its website, but it lacked sufficient detail for individuals to understand how mortgage brokers manage their personal information. Moreover, the privacy policy link on the broker's "terms of service" page didn't work. The remaining two brokers had privacy policies which were not posted online or made available to clients.

Over-collection of personal information

Mortgage brokers collect a variety of personal information in order to verify a potential client's identity, including driver's licence numbers, birth certificate information and social insurance numbers.

Social insurance numbers are frequently used by agents and brokers to differentiate between clients with similar names. However, this number is *not* required to conduct a credit check, nor is there a legislative requirement for its collection as part of a mortgage application.

We found that mortgage application forms did not state that the provision of a social insurance number is optional. We believe that social insurance numbers should not be used as a general identifier and their uses should be restricted to legislated purposes only.

Consent is not always obtained before collection

In order for consent to be meaningful, PIPEDA requires that the purposes for collecting, using and disclosing personal information are clearly stated. Express consent is necessary when the information is sensitive.

In order to obtain a mortgage for their clients, mortgage brokers and agents need to disclose a client's personal information to both credit reporting agencies and lenders.

We found that, although brokers require their clients to provide written consent for brokers to access credit reports, agents sometimes obtain consent verbally and then ask clients to provide written consent after the credit report has been accessed. We also found cases where credit reports were obtained prior to consent having been recorded, and others where there was no record of consent ever having been obtained.

Clients cannot opt out of secondary uses of personal information

The consent forms we looked at stated that personal information could also be used for marketing and other secondary uses – and did not allow clients the choice of opting out of secondary uses of their personal information.

Three mortgage brokers informed us that personal information such as a names and telephone numbers may be shared with real estate agents, financial planners and other service providers as sales leads. The consent forms also permitted the use of personal information for marketing purposes such as sending newsletters and birthday greetings to clients.

Unapproved mortgages should not be retained for longer than necessary

Legislative requirements demand that mortgage brokers retain records related to approved mortgage applications for a specific time period, but there is no such requirement for unapproved applications.

However, mortgage consent forms frequently stated that files may be kept for specific periods of time – even if a mortgage was not approved by a lender. Four brokers' consent forms stated agents "can retain and use" personal information for seven years after an application was made. One broker claimed to have a policy of destroying unapproved mortgage application within six months, but an examination of its files showed the policy was not followed. The fifth broker's form stated that the retention period is three years.

None of the brokers were able to demonstrate a need to retain unapproved mortgage applications for long periods of time.

Disposal practices need to be strengthened

The audit also raised concerns about the disposal of personal information.

While all the brokerages had shredders, they were – with one exception – strip-cut shredders which do not adequately destroy documents. We did not find evidence that shredders were consistently used, nor could we confirm that brokers and agents who retained files in their homes disposed of them safely.

We identified one case where a broker had reused the reverse side of old, filled-out mortgage applications in order to print out new applications. This practice could clearly result in a client's personal information being shared with someone who has no need to know.

"Identifying" Recommendations

The mortgage brokers we audited should:

- Not routinely collect and retain personal information, such as social insurance numbers, unless necessary to fulfill a specific and specified purpose and/or in accordance with the law;

- Be able to demonstrate that clients have consented to the collection of their personal information; make clients aware of all potential uses and disclosures of

their personal information; and seek express consent for secondary uses of their personal information; and,

- Develop and implement policies and procedures regarding the retention of personal information.

III. Responsibility and accountability for privacy

Organizations subject to PIPEDA are responsible for the personal information in their control. They must also clearly establish who is responsible for protecting personal information and ensuring compliance with privacy legislation.

Our audit highlighted several concerns.

Mortgage brokers lack awareness of privacy roles

PIPEDA requires that organizations collecting personal information establish clear responsibility for privacy. Many organizations which handle personal information have a chief privacy officer as the key point of contact for privacy-related matters.

While all brokers we examined had designated a chief privacy officer, there was a lack of understanding about the responsibilities of this position. Many agents were unaware of who the chief privacy officer was, or to whom they should turn with a privacy-related question.

In one case, a broker franchisee told us that his organization's chief privacy officer was located at the brokerage's head office when, in fact, the policy manual stated that the chief privacy officer was the broker/owner himself.

Brokers and agents are not trained on privacy responsibilities

PIPEDA requires that employees be educated about privacy practices and policies and yet no agents with the mortgage broker companies we audited had been provided with formal and ongoing training on company-specific privacy practices, or their responsibilities under the law.

Brokers reported privacy breaches

None of the audited mortgage brokers had formal breach reporting policies in place at the time of the suspected thefts. However, they did contact our Office to determine how to contain and mitigate the breaches, and also notified those affected by the breaches.

During the course of our audit, one of these brokers developed a formalized breach reporting policy.

Post-breach hiring processes are more stringent

Mortgage brokers significantly tightened up their hiring processes after the breaches that were reported to our Office occurred.

As of 2008, the *Mortgage Brokers, Lenders and Administrators Act 2006* requires all individuals and businesses who conduct mortgage brokering activities in Ontario to be licensed by the Financial Services Commission of Ontario. To obtain a license, brokers and agents must take a course, pass an examination and undergo a criminal background check.

Prior to the breaches, brokers relied heavily on interviews, the applicant's knowledge of the business and references. They may not necessarily have contacted lenders with whom the applicant had dealings. One broker did not always confirm the applicant's licensing status with the Financial Services Commission of Ontario.

After the breaches, one brokerage now ensures that a regional manager from the broker's headquarters meets all prospective employees and that a senior manager from headquarters approves all new hires. This same brokerage required that all agents be members in good standing of the Canadian Association of Accredited Mortgage Professionals. Two brokers we audited began verifying all references.

Many brokers are taking the further precaution of restricting new agents' access to credit reporting software. For example, one broker would not permit a new agent to access credit reporting software for a minimum of 90 days.

Accountability Recommendations

The mortgage brokers we audited should:

- Clearly establish who is responsible for privacy training and monitoring compliance with PIPEDA;
- Develop and implement privacy policies and procedures to ensure compliance with PIPEDA principles, including developing information to explain the organization's information handling policies and procedures;
- Ensure their staff are trained on company-specific privacy policies and procedures, as well as on their responsibilities under PIPEDA; and,

- Ensure that mortgage brokers and clients are aware of and can readily access privacy policies.

RESPONSE OF THE AUDITED BROKERS

We sent a preliminary draft of our audit to four of the five brokers we audited; the fifth is no longer in the mortgage broker business.

All four stated that they would implement all of our recommendations.

CONCLUSION

Our Office appreciates the cooperation we received from the mortgage brokers we audited. For the most part, they were supportive of our work, and were open and responsive to our recommendations.

The mortgage brokers stressed to us that their key concern is service to their clients, and growing their business. Many of the privacy issues we raised – particularly around privacy procedures and practices – simply had not occurred to them.

To address this lack of understanding, our Office is now working with mortgage broker associations to develop guidance documents that will help brokers meet their privacy obligations, and also inform Canadians about how they can ensure their personal information is used appropriately by mortgage brokers.

RESPONDING TO CANADIANS: COMPLAINT INVESTIGATIONS AND INQUIRIES

Social networking, new technologies and surveillance concerns were some of the major themes of our investigative work in 2009.

For our Office, the most important investigations we undertake are the ones that ultimately result in change that has a meaningful impact on the day-to-day lives and privacy rights of Canadians.

As people spend more and more time online, it is increasingly clear that the Internet must be a major focus of our attention. Indeed, a growing number of our investigations are exploring how privacy laws apply in the virtual world.

In 2009, for example, we completed a comprehensive investigation into Facebook – a social networking site that has attracted millions of Canadian users. At the end of our investigation, Facebook made a commitment to put in place changes that would offer better privacy protections for users in Canada and around the world. We will closely follow the roll-out of these promised changes in 2010.

Facebook was only one of many investigations related to rapidly developing technologies with implications for privacy. We also examined the use of various technologies as part of our investigations into issues such as covert and workplace surveillance as well as street-level imaging applications and deep packet inspection.

INQUIRIES

Our inquiries officers have always had the extremely important responsibility of acting as Canadians' first point of contact with our Office. They answer questions, explain how privacy legislation may – or may *not* – apply in specific situations and also help Canadians to understand the mandate and role of our Office.

During 2009, we handled 5,095 new inquiries about issues that fall under PIPEDA – an average of 425 per month. That's down 20 percent from the 6,344 inquiries we received a year earlier.

It appears that more people are turning to our website rather than calling or writing us when they are seeking information about privacy issues. We have posted a number of new resource guides and fact sheets on our website. As well, we've introduced a new complaint form on our website, which makes it easy to understand how to make a formal complaint or report a data breach. We received close to half a million more hits to our website in 2009 than the previous year.

The drop in inquiries numbers is also due in part to the introduction of a new case management system which tracks some statistics differently. In the past, an inquiry from one individual about two different issues was counted twice. Now, the system would count that call as one inquiry.

Amongst the calls and letters that we continue to receive, we have noticed an increase in inquiries related to how online organizations are handling personal information. Following media reports about our Facebook investigation, for example, we received numerous inquiries about social networking sites.

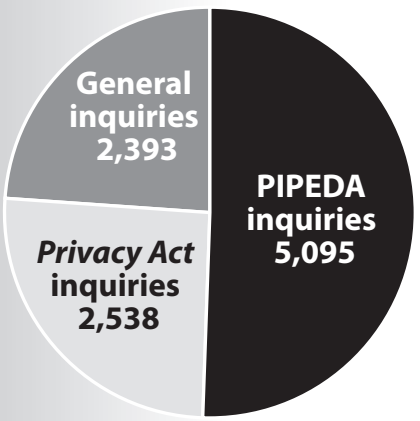
In some cases, we are hearing from Canadians who have typed their name into a search engine and been surprised to find their personal information on a particular website.

A long-standing concern that we still receive many calls about is the use of social insurance numbers by organizations. We also receive numerous inquiries about the collection of other types of information such as driver's licence numbers. A question we hear often is: *Can they do that?*

Some people who contact us mistakenly believe that our Office

PIPEDA inquiries received	2009	2008
Telephone inquiries	4,043	5,280
Written inquiries (letter and fax)	1,052	1,064
Total	5,095	6,344

Inquiries of all types received in 2009



can levy fines against organizations. We want to ensure their expectations are in line with what we can provide.

When people call about a problem they've experienced with a particular organization, one of the key questions we ask is: *Have you spoken with that organization about your concerns?*

Problems can often be resolved quickly – and without initiating a formal complaint investigation process – when individuals deal directly with an organization. In some cases, we see that even problems which remain unresolved after discussions with front-line employees *can* be addressed with a phone call to the organization's chief privacy officer. We maintain a database of chief privacy officers so that we can ensure that people with a privacy concern can easily contact the right person within an organization.

This is why we encourage people to initially deal directly with an organization when they have a concern.

However, where a problem cannot be resolved between the parties, we ask people to come back to us to further discuss whether a formal complaint should be made.

Besides answering questions over the telephone, we have a large number of fact sheets and guidance documents which can help people to understand privacy issues related to the collection and use of their personal information. For example, in 2009 we published information on: the collection of driver's licence information in the retail sector; street-level imaging; PIPEDA and anti-money laundering legislation; the processing of personal data across borders and covert video surveillance in the private sector.

COMPLAINTS

Our Office received 231 new PIPEDA-related complaints in 2009. This represents a substantial drop from 2008, when we received 422.

Meanwhile, we closed 587 complaints, compared with 412 the previous year.

We believe that a big reason for the decreased number of incoming complaints is our success in helping people to deal with concerns more efficiently. Many of the problems that people have called us about were solved informally with a phone call to the right person within an organization.

As a result, we will increasingly be able to focus our investigative resources where they belong – on more complex cases or significant or systemic privacy issues.

Our Facebook investigation, for example, involved many complicated and technical issues which warranted a comprehensive investigation. Increasingly, we are seeing complaints involving new technological applications that demand a thorough examination.

Facebook was also an example of the increasing number of investigations we undertake that involve companies based outside of Canada. This reflects the dramatic growth in transborder data flows.

Another investigation involving new technologies examined how Bell Canada uses deep packet inspection to manage traffic on its telecommunications networks. The investigation concluded the way in which network traffic was being managed was generally acceptable, but the Assistant Commissioner also emphasized that expanded use of deep packet inspection would require renewed consent.

Other issues we dealt with in our investigative work included covert surveillance by private sector organizations, workplace surveillance, including the use of video cameras and location-tracking devices, and the collection of driver's licence information.

While the overall number of complaints we received fell, there was little change in the distribution of these complaints amongst industry sectors.

Financial institutions, the telecommunications sector and insurance companies were once again the targets of the largest numbers of complaints. Together, the three sectors were the subject of more than half of all complaints to our Office.

The size of these industries and the enormous number of transactions they conduct with individual Canadians each year is a major factor explaining their consistently high rankings when we break down complaints by sector.

One of the trends we continue to see with respect to insurance-related complaints is the use of lawyers or "facilitators" to file complaints on behalf of complainants. Most of these cases involve issues around access to personal information, collection of personal information, or consent for the disclosure of personal information. Facilitated complaints made up more than a quarter of all backlogged complaints in mid-2009.

In many cases, the complaint relates to a legal dispute between an individual and an insurer, a medical examiner or other benefit providers. These complainants often file multiple complaints related to the same issue. Gathering evidence is sometimes challenging because the complaints flow from an event which occurred several years earlier; the cases often involve a first party, second party and third party insurer and benefits schedules.

Complaints Received by Industry Sector

	Count		Percentage	
	2009	2008	2009	2008
Financial Institutions	55	93	24	22
Telecommunications	42	63	18	15
Insurance	41	71	18	17
Sales	25	63	11	15
Transportation	15	38	6	9
Professionals	10	33	4	8
Services	9	21	4	5
Health	8	9	3	2
Accommodation	7	15	3	4
Other	19	16	8	4
Total	**231**	**422**	*	

Industry Sector Categories

Financial Institutions: Banks, collection agencies, credit bureaus, credit grantors, financial advisors

Telecommunications: Broadcasters, cable/satellite, telephone, telephone/wireless, Internet services

Insurance: Life and health insurance, property and casualty insurance

Sales: Car dealerships, pharmacies, real estate, retail, stores

Transportation: Air, land, rail, water

Professionals: Accountants, lawyers

Services: Daycare, hairdressers, beauticians

Health: Chiropractors, dentists, doctors, physiotherapists, psychologists/ psychiatrists

Accommodation: Hotels, landlords, condominiums, property management

Other: For example, private schools, aboriginal bands, security companies and private investigators.

*Note: Numbers do not total 100 percent due to rounding.

Three types of complaints – access, use and disclosure, and collection – continued to make up the lion's share (68 percent) of all the complaints we receive.

We noticed a significant increase in the proportion of complaints dealing with access to personal information – 28 percent of total complaints, compared with 17 percent the previous year. Many small- and medium-sized businesses are still lacking in awareness of individuals' right to access their personal information under PIPEDA and also of how to process access requests within legislated timelines.

SNAPSHOT OF 2009 INVESTIGATIONS

The following is a look at some of the investigations completed during 2009. Additional details about many of these cases are available on our website.

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

INVESTIGATIONS INVOLVING CROSS-BORDER DATA ISSUES

As Canadians increasingly live their lives online – making purchases from web-based retailers and communicating with friends via social networking sites and so on – it is not surprising that more and more of the privacy issues they encounter will be with organizations that have little or no "bricks and mortar" presence in Canada.

For our Office, this means we are beginning to receive more complaints about multinational – often U.S.-based – corporations.

PIPEDA applies to transactions involving personal information when there is a real and substantial connection to Canada. This includes online transactions and even, in certain circumstances, where the organization is based outside Canada.

Facebook

In July 2009, Assistant Commissioner Denham released her findings in a comprehensive investigation into the privacy practices of Facebook, a California-based social networking site with millions of Canadian users. The investigation was prompted by a complaint from the Canadian Internet Policy and Public Interest Clinic at the University of Ottawa.

The investigation report uncovered a number of privacy problems. The most significant of these involved the risks posed by the over-sharing of personal information with third-party developers of Facebook applications such as games and quizzes.

With more than one million developers around the globe, the Assistant Commissioner was concerned about a lack of adequate safeguards to effectively restrict those developers from accessing users' personal information, along with information about their online "friends."

Another concern was that, in some cases, Facebook was not providing enough information to allow users to understand how their personal information would be handled. For example, there was confusing information about the distinction between account *deactivation* – whereby personal information is held in digital storage – and *deletion* – whereby personal information is actually erased from Facebook servers.

At the end of the investigation, Facebook committed to making a number of changes to improve privacy protections for its users.

Most significantly, Facebook agreed to retrofit its application platform in a way that will prevent any application from accessing information until it obtains express consent for each category of personal information it wishes to access. Under this new permissions model, users adding an application would be advised that the application wants access to specific categories of information. The user would be able to control which categories of information an application is permitted to access. There would also be a link to a statement by the developer to explain how it will use the data. This change required significant technological changes and was expected to take one year to implement.

Facebook also agreed to introduce changes to help users to better understand how their personal information will be used and, ultimately, to make more informed decisions about how widely to share that information.

As agreed, Facebook has been reporting to us on those commitments and undertakings. We will continue to monitor all developments closely, and provide our feedback.

The Facebook investigation was reported by media outlets around the world and raised our profile amongst global corporations.

Immediately after the report was published, another major social networking site contacted us regarding compliance with Canadian laws and other U.S.-based companies requested meetings to talk to us about their global applications. This is a new development that we hope will lead to better privacy protections for Canadians and people around the world.

Accusearch, Inc. (Abika.com)

Responding to a complaint, we investigated the information-handling practices of a Wyoming-based search services website. Assistant Commissioner Denham found it violated key provisions of PIPEDA in its collection, use and disclosure of the personal information of residents of Canada.

Abika.com provided a range of search services using third-party researchers who search for and obtain personal information about individuals from a variety of public and private records and databanks. It also compiled "psychological profiles" which purport to describe an individual's behaviour and personal traits.

The U.S. Federal Trade Commission (FTC) separately investigated the activities of Abika.com. (See page 87 for information about our Office's involvement in supporting the FTC in a legal case involving Abika.com.)

Based largely on information provided by the FTC, our investigation determined that the American company collected, used and disclosed to third parties the personal information of Canadians, without their knowledge or consent, in contravention of PIPEDA. As well, in some cases, the company knowingly turned over the personal information of Canadians for purposes that a reasonable person would consider highly inappropriate in almost any circumstances.

The Assistant Commissioner recommended Abika.com stop collecting, using and disclosing the personal information of people living in Canada without their knowledge and consent. Given the effectiveness of the FTC's efforts against this organization, in particular the successful outcome of the FTC's legal case, it was determined that no further action was required by our Office.

The investigation marked an important step in international co-operation and collaboration that will become increasingly necessary to adequately protect privacy rights on both sides of the border in years to come.

INVESTIGATIONS INVOLVING NEW TECHNOLOGIES

Bell Canada – Deep Packet Inspection

Deep packet inspection is a technology used to manage traffic on large and small telecommunications networks. It can also be used to help target advertisements on some of the very same networks.

Network managers argue that deep packet inspection is one tool among many that help them ensure networks can accommodate the varying bandwidth demands of their users. Privacy advocates, however, note that it can also be used to peer into the content passing between users on networks – whether they are mp3 files, personal messages or corporate documents.

We investigated a complaint alleging that Bell Sympatico uses deep packet inspection technology during Internet transmissions to collect and use personal information from its customers without their consent.

The complainant also alleged:

- This practice collects more personal information than is necessary to fulfill the company's stated purposes of ensuring network integrity and quality of service; and

- Bell does not adequately inform its customers of its practices and policies concerning the collection of their personal information during Internet transmissions.

Although Bell acknowledged that the deep packet inspection technology it uses on its network has the capability to inspect content such as e-mails and Internet searches, the company said it does *not* use it for this purpose. We did not find that the technology was being used to target advertisements.

The complaint was not well-founded with regard to consent and limiting collection, but well-founded with regard to the matter of openness.

The investigation concluded that managing network traffic by targeting peer-to-peer file-sharing applications in order to ensure adequate bandwidth and quality of Internet service for its customers is an acceptable business purpose for an Internet service provider. The Assistant Commissioner was unconvinced that Bell was collecting or using any personal information of individuals other than the IP addresses and subscriber IDs of Sympatico customers when it uses its DPI technology for the purpose of network traffic management.

Assistant Commissioner Denham recommended that Bell provide clear information to its customers about deep packet inspection and how the company's traffic management practices impact the privacy of customers.

She also noted that any expanded use of deep packet inspection by Bell, in such a way that personal information is collected, used or disclosed for purposes other than the

current purpose of managing network traffic, would require renewed, meaningful and informed consent.

Street-Level Imaging Company

We received a complaint against a company alleging that it had collected an individual's image, without his knowledge or consent, using street-level imaging cameras mounted on top of a vehicle.

The individual also complained that he did not know where his image was being stored or how it was being protected.

We received this complaint prior to the online launch of an application which allows people to take virtual tours of neighbourhoods. Following discussions with our Office, the company agreed not to publish the complainant's image online.

The complainant said he was satisfied with the company's undertaking. On that basis, the complaint was considered settled during the course of the investigation.

Our Office has taken part in detailed discussions with companies involved in the collection and use of street-level imaging over the past few years. Further details about this work are provided on page 71.

INVESTIGATIONS INVOLVING COVERT VIDEO SURVEILLANCE

Private Investigation Complaint

A woman and her daughter complained to our Office after they were surprised to learn that they'd been captured on videotape during covert video surveillance of the woman's sister.

Our Office has developed guidance on the use of covert video surveillance in the private sector. These guidelines, completed in 2009, are available on our website.

The surveillance was conducted by a private investigation firm hired by the sister's insurance company. The sister had been involved in a car accident and had begun legal proceedings against her insurer over benefits.

The insurer admitted that images of the complainant and her daughter were captured inadvertently during the covert investigation.

The private investigation firm argued that it was not reasonable to expect that consent be obtained from all parties whose information was inadvertently caught on videotape

during an investigation. It also objected to having to blur the images of individuals accidentally recorded during video surveillance.

There are times when PIPEDA, under paragraph 7(1)(b), permits the collection of personal information via video surveillance of a third party (someone who is not the target of surveillance) without their consent. This includes, for example, situations where the organization has reason to believe this information is relevant to the purpose for collecting information about the surveillance target. The insurer confirmed that was not the situation in this case.

The Assistant Privacy Commissioner made several recommendations, including that the firm:

- Stop collecting personal information unless paragraph 7(1)(b) applies to the situation;
- Depersonalize (by blurring, for example) as soon as practicable or remove extraneous personal information that is collected, unless 7(1)(b) applies;
- Incorporate into its privacy policy specific procedures and policies that pertain to the collection, use and disclosure of personal information obtained by covert surveillance, including extraneous third-party personal information; and
- Provide regular training of employees and subcontractors on these new policies and procedures.

The firm agreed to provide training, however, it declined to revise its privacy policies and procedures on video surveillance as recommended. It also refused to depersonalize or remove third-party information collected without consent.

The complaint was well-founded.

The complainants also filed a complaint against the insurance company that hired the private investigation firm and that investigation was still in process at the end of 2009.

The complaints were instrumental in leading to the development of our Office's guidance on the use of covert video surveillance in the private sector. This involved exhaustive consultation with the private investigation and insurance industries. We continue to monitor industry compliance with those guidelines.

INVESTIGATIONS INVOLVING WORKPLACE SURVEILLANCE

Transit Company – GPS Tracking

An individual objected to the installation of a mobile data terminal containing a global positioning system, or GPS, tracking device on vehicles he drove for a municipal transportation service.

He alleged that the transit company, which provides services for disabled people – was improperly collecting his personal information – specifically his daily movements while on the job.

The complainant alleged that the transit organization was using the new system to keep track of his time throughout the day and to ensure he did not take a break or stop for lunch.

According to the organization, however, the purpose of the new system was to increase efficiency and the quality of the service, for example, by making it possible to immediately send scheduling changes to drivers without a dispatcher.

The Assistant Commissioner determined that the information collected with the new tracking system did not differ substantially from that collected with a manual system that was replaced. Before the installation of the new system, the organization had been collecting the same types of information on paper forms. In this sense, its use of new technologies was no more privacy invasive than other tracking methods it had used for over twenty years, the investigation found.

Further, the information in dispute was collected and used strictly for an appropriate purpose – providing efficient service to clients. There was no evidence that personal information was being used to manage employee performance.

The complaint was not well-founded.

Bus Company – Overt Video Surveillance

A man complained that his employer, an inter-city bus company, was using 22 video cameras installed in a bus depot to monitor and manage employee performance. He claimed there were no signs in the depot advising employees or the public of the video surveillance and was concerned that the organization was collecting personal information without consent.

The organization explained that the purpose of the video camera surveillance system was to:

- Ensure the safety and security of customers and employees at the depot, where there had been a significant level of criminal activity;
- Reduce and discourage incidents of vandalism and illegal conduct; and
- Limit the potential for liability for damages due to fraud, theft or inappropriate operational procedures.

The organization also correctly pointed out there were signs at the entrance of the terminal notifying the public of the existence of video surveillance. It also noted that cameras were not hidden from view.

The Assistant Commissioner found that the purposes stated by the organization for the collection and use of the information captured by the video surveillance cameras were reasonable.

These purposes were supported by evidence specific to the depot in question as well as data collected from comparable company depots. None of the purposes cited by the company were to monitor or manage employee performance, and we observed that the locations of the cameras in the depot were consistent with the stated purposes.

There was adequate signage in the depot to alert employees and the public of the fact that there was video surveillance, although we found that reasonable efforts had not been made by the organization to explain to employees the purposes of the surveillance.

The organization agreed to improve its video surveillance policy, train its security personnel and managers, and adequately inform its employees.

The complaint was well-founded and resolved.

COLLECTION OF DRIVER'S LICENCE NUMBERS

Retailer

A woman applying for a membership at a store was asked for both her driver's licence number and date of birth and was not told why this personal information was being collected.

Guidance for retailers on the collection of driver's licence information is available on our website.

When the woman later asked for access to her personal information, her written request and follow-ups were ignored until our Office contacted the organization.

The retailer told us it needed personal information such as a driver's licence number or full date of birth both to detect and track fraud and to perform a credit check on members who would receive cheque-writing privileges.

We noted the application form did not state that a credit check would be done. As well, credit reporting agencies advised us that a driver's licence number is not required to perform a credit check.

The organization said the driver's licence number was used to identify individuals who have previously engaged in fraudulent activities and to prevent them from re-applying for membership. It said the number helps to differentiate between customers with common names.

The retailer stated it collects the date of birth of applicants in order to verify a minimum age requirement. However, during our investigation, the organization agreed this could be achieved by simply looking at an identification card.

We made numerous recommendations to the company, including that it:

- Verify an applicant's age and identity by looking at a piece of photo identification without recording the information;
- Obtain consent for a credit check by providing applicants with notice that a credit check may be required before cheque-writing privileges are granted;
- Collect either the day and month of birth or the year and month, where this information is only being collected for the purpose of fraud prevention and detection (i.e. from customers who are *not* seeking cheque-writing privileges);
- Ensure front-line staff are aware of the privacy policy and procedures; and

- Remove from its database the numbers associated with identification documents that have previously been collected from customers.

The organization agreed to the recommendations concerning membership applications. It also committed to updating its company privacy statement to inform individuals of the collection of partial date of birth information for fraud-prevention and detection purposes, and – for those opting for cheque-writing privileges – of the collection of full date of birth for both credit-check and fraud-deterrence purposes.

The Assistant Commissioner concluded that the matters were resolved**.**

OTHER NOTEWORTHY CASES

Landlord Organization – Sharing Tenant Information without Consent

An advocate for tenants' rights complained about a landlord organization whose website included lists of people deemed to be "bad" tenants as well as people who were late paying their rent.

This personal information was available to landlords who were members of the organization. However, at one point, a portion of the information was available to anyone with access to the Internet.

The tenants' advocate complained that sensitive personal information was being collected, used and disclosed without consent.

Following an investigation, we determined that the documents used by the organization and landlords were not adequate to inform tenants or prospective tenants about how their personal information would be used or disclosed; nor could these documents be considered a valid consent form for posting tenants' personal information on the website.

The investigation found the organization was negligent in not mentioning in its service contract that a landlord must obtain tenant consent when collecting personal information to update credit histories, or add information to the bad or delinquent tenant lists.

As well, landlord members failed to obtain appropriate consent for such collection, use and disclosure of their tenants' personal information.

The investigation confirmed that the personal information of over 1,300 people available on the website was not adequately protected, although the organization later added acceptable safeguards for the delinquent tenant list.

Given the unresolved issues related to consent, the Assistant Commissioner recommended the organization:

- Revise the membership agreement to make it clear that landlords must obtain meaningful tenant consent to disclose personal information;
- Revise the rental agreement form to include a specific consent provision for disclosures of personal information to the organization;
- Confirm that the bad tenant list, or any other such compilation of personal information, has been dismantled; and
- Confirm that any and all other lists will be dismantled unless the respondent can show that meaningful consent of tenants had been obtained.

The complaint concerning consent was well-founded. The complaint about safeguards was resolved. The Office was unable to follow up on the recommendations as the organization is not longer active.

Consumer Data Organization – Matching Publicly Available Personal Information with Geographically Specific Demographic Statistics

We received a complaint about the use and disclosure of personal information by an organization that supplies lists of consumer data to businesses for direct-marketing purposes.

The complainants alleged that the organization created personalized demographic information through data matching of telephone book information with Statistics Canada data. They argued that the use and disclosure of this newly created "personal information" required consent.

Moreover, the complainants believed that, because the organization used and disclosed detailed demographic information, a reasonable person would expect consent to be obtained before such information about her or him was compiled and sold.

However, our investigation determined that the organization's process of compiling consumer lists did not change the status of the telephone book information from publicly available personal information to personal information subject to consent requirements.

The publicly available personal information included in the consumer lists had merely been sorted according to geo-demographic data.

The Assistant Commissioner was of the view that the lists consisted of information about neighbourhoods, rather than identifiable individuals. Thus, she found the consent complaint to be not well-founded.

The complainants had also argued that the respondent failed to meet the criteria of "openness" under PIPEDA. They were concerned that the organization did not provide details about how it collected, used and disclosed the personal information or its related practices and policies – and was resistant to answering inquiries about these issues.

Assistant Commissioner Denham agreed that the company did not provide enough information on its policies and practices regarding its handling of the personal information that it sold. While the personal information was publicly available, it nonetheless was still personal information.

The company implemented changes to its policies and practices. The openness complaint was well-founded and resolved.

Insurer – Personal Information to a Third Party

The complainant had suffered serious injuries in a car accident. During the four years that followed the accident, she and her insurer had been involved in several formal dispute resolution proceedings related to her long-term benefit entitlement.

The complainant was seeking to be formally recognized as having a "catastrophic impairment" and was awaiting a hearing for binding arbitration, a process which she had initiated.

Before the pre-arbitration hearing with the Financial Services Commission of Ontario, the insurer sought the expertise of third-party medical consultants and shared with them – without the complainant's consent – her medical brief and two previous medical assessments that were the subject of dispute.

When she became aware of the disclosure, the complainant objected based on the grounds that it had been done without her express consent.

Following our investigation, the Assistant Commissioner found that PIPEDA allowed for the disclosure without express consent, in light of the case's specific circumstances.

By initiating an arbitration proceeding before the Financial Services Commission of Ontario in which she put her personal medical information in issue, the complainant gave her implied consent to the collection, use and disclosure of relevant personal

information by the insurer for the limited purpose of defending itself in these particular proceedings.

It would be reasonable for an individual, in these circumstances and for this limited purpose, not to expect the insurer to seek her express consent to disclose her relevant medical information.

The complaint was not well-founded.

ELIMINATING A BACKLOG

One of our Office's accomplishments of 2009 was the virtual elimination of our investigation backlog of cases more than a year old.

In recent years, a shortage of investigators combined with an increasing number of complaints dealing with highly complex issues requiring extensive investigation had led to a backlog that, at its worst, included 376 PIPEDA complaint files.

Adding to the challenge was the fact that many of these old files involved extremely difficult issues – for example, either the complainant or respondent organization was entrenched in a particular position and unwilling to compromise. By definition, no early resolution in these cases had been possible.

The backlog resulted in unacceptable treatment times for many of our investigations in recent years.

Dealing with the backlog has been one of the top priorities of our Office. Our backlog reduction initiative began in earnest in 2008, after we received additional financial resources from Treasury Board.

We implemented a multi-pronged approach that included streamlining our processes; implementing an internal "backlog blitz" aimed at closing old files; hiring and training new investigators; and contracting external resources.

Over the course of 2008 and 2009, we managed to steadily reduce our backlog files. We began the year 2009 with 312 backlog files and ended with 46. By the end of March 2010, we had eliminated our backlog.

AVOIDING ANOTHER BACKLOG – EARLY RESOLUTION

Our focus now is to ensure efficient processing of complaints to avoid future backlogs.

Part of our strategy is ensuring that all concerns about privacy issues don't needlessly turn into formal investigations. As discussed earlier, we are emphasizing to would-be complainants the importance of trying to resolve an issue directly with an organization before filing an official complaint.

When individuals are not able to reach an acceptable solution by speaking with an organization, our inquiries officers help them to formulate the complaint. We also have an online complaint form which explains in detail the information that our Office will need. This can help save time after the file is assigned to an investigator.

The creation of a new position in our Office – Complaints Registrar – is another important change in the way we handle an incoming complaint. The Registrar assesses the complexity of the case; whether it should be handled as a high priority; and whether it can be resolved quickly.

Following the priority-setting process undertaken by the Complaints Registrar, complaints involving a serious, systemic or otherwise complex matter – for example, uncertain jurisdictional matters, multiple allegations or complex technical issues – are immediately streamed to an investigator.

However, complaints that could potentially be resolved quickly now go to our new early resolution team. These complaints could, for example, involve cases where our Office has previously 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.

While we have always tried to encourage complainants and organizations to reach an early resolution, we instituted a more formal early resolution process in the fall of 2009. The purpose of the early resolution process is to address more complaints rapidly by relying on negotiation and persuasion and a solid knowledge of past complaint findings.

Our goal is that complaints sent to early resolution are resolved within 45 working days. If they are not, they are sent to an investigator for completion.

While it is early days, indications are that it will be a useful process to address complainants' concerns.

We are seeing that organizations often initiate immediate corrective action after we have provided guidance about their obligations under PIPEDA. As well, many complaints related to access to personal information have been resolved because the complainant is reassured that an objective third party has confirmed that a denial of access is for a legitimate reason.

DATA BREACHES

Our Office has been encouraging organizations to voluntarily report breaches to us for the last few years.

We have been strongly advocating for legislative amendments that would make it mandatory to report significant breaches to our Office and individuals. We are pleased that Industry Canada has consulted on and developed a breach notification model that contains thresholds for reporting to the Commissioner and to affected individuals.

In 2009, 58 private-sector data breach incidents were voluntarily reported to us. This represents a drop from a year earlier, when 65 breaches were reported, although the 2008 figures included a large number of incidents related to a systemic problem in the mortgage broker industry. In 2007, we received 48 voluntary data breach reports from organizations.

While larger organizations accounted for the majority of reported breach incidents in 2009, we are starting to hear from more mid- and small-sized companies.

When we receive a notice of a breach, we follow up, provide advice where appropriate and prepare an internal

Examples of Reported Breaches

- A U.S.-based credit and debit card payment processing company reported that malware had been installed in its computer systems, potentially compromising the personal information of an unknown number of people – possibly including Canadians. We recommended the company continue to develop end-to-end encryption and comply with the Payment Card Industry Data Security Standard.
- An unencrypted computer hard drive containing the personal information of more than 800 bank clients was stolen during a break-in at a bank. We were satisfied with the bank's actions following the break-in, which included notifying affected clients and reminding branch managers to encrypt the personal information of all clients.
- An envelope-stuffing error while an organization was preparing to send out a mass mailing of pension statements resulted in the statements of an estimated 140 employees being sent to the wrong people. The company discovered the error when the organization received a few calls from employees who had received more than one pension statement. It followed up promptly, identifying the cause of the error, sending out a second mailing with a covering letter advising of the inadvertent breach, and inviting employees concerned about the incident to contact a service centre representative. We agreed the company had taken appropriate measures.

report. We don't normally open a formal investigation if we see the company is taking reasonable steps to address a breach.

However, we will take action where we see a systemic problem. For example, after receiving numerous breach notifications from mortgage brokers, we decided to conduct an audit in order to determine whether these organizations had adequate procedures and practices in place to protect personal information.

For the most part, the breaches reported to us appear to be isolated incidents. Human error remains a consistent theme and we see many cases where the breach is the result of an employee's failure to follow company procedures.

Lost and stolen laptops also continue to be a perennial issue – but what's changing is that now, much of the time, those missing computers and the personal information they hold are protected by strong security measures such as encryption.

When we first published our privacy breach checklist in 2006, we found that many chief privacy officers seemed reluctant to contact us following a breach. Since then, however, we have seen a shift and we now see many major organizations calling or writing to us very soon after a breach.

Most of these companies are promptly notifying affected people in cases of a serious breach.

Privacy officers have expressed a willingness to work with us because they know that by reporting a breach they are demonstrating due diligence and transparency. Companies also see the benefit of involving us because it provides some reassurance to customers that the matter is being treated seriously and with some oversight.

Another encouraging trend is the level of analysis and detail provided in the breach reports we receive. These reports now tend to be very comprehensive and include detailed descriptions of the mitigating measures that the organization plans to put in place.

The federal government has been studying possible legislative amendments that would create a mandatory reporting regime – a step our Office strongly supports.

THE BUSINESS TAKE ON BREACH REPORTING

In 2009, when it appeared that Parliament would amend PIPEDA to oblige companies to report data breaches to our Office, we commissioned research to explore what businesses thought of the existing voluntary notification guidelines and the prospect of a mandatory regime.

(As discussed above, Industry Canada has developed a breach notification model that we hope will be implemented in the near future.)

We hired NYMITY, a global privacy research services firm, to conduct the study. The project involved the preparation and web posting of a background "primer" to ensure that companies were well versed on the issue. This was followed by hour-long telephone interviews with 27 privacy professionals representing companies ranging in size from fewer than 100 to more than 80,000 employees.

The OPC's voluntary breach notification guidelines, titled *Key Steps for Organizations in Responding to Privacy Breaches*, were published in August 2007. They can be found on our website.

Overall, the researchers found a broad level of familiarity with, and acceptance of, voluntary breach notification. All 27 organizations were aware of the existence and general content of the OPC's guidelines, issued in 2007. Six had actually reported one or more incidents to our Office, with the majority describing the experience as positive. Four companies said they had never experienced a data breach, so they had nothing to report.

The study found that the majority of respondents had processes in place to identify, report and address privacy breaches. More than half were formal, written protocols, generally based on our Office's guidelines. Others had more informal procedures, including drawing on the expertise of in-house privacy experts and outside legal counsel.

NO CHANGES EXPECTED

Only a minority (22 percent) of respondents predicted that a mandatory reporting regime would have no impact on their companies. The remaining 78 percent were evenly split on whether the impact would be negative or positive.

On the plus side, respondents expected that under a mandatory regime the company would develop a more structured reporting policy, become more aware of the importance of privacy, focus more on breach prevention, and assign more accountability for privacy

to the business channels. Nearly six in 10 respondents said they were planning additional privacy training and awareness programs in 2010 and 2011.

Respondents' concerns about a mandatory regime were about cost, including the fear that outside legal counsel and more privacy office staff would have to be hired. A quarter of respondents (26 percent) were concerned about being assessed penalties or liability for a failure to report. The opposite effect – a rush to over-report – was also raised as a concern.

Despite these reservations, nearly two-thirds (63 percent) of respondents anticipated that a mandatory regime would not change the way they decide on whether a particular incident is reportable.

Here are other noteworthy findings from the study:

Defining Issues

Many respondents said they would feel more comfortable with mandatory reporting requirements if key concepts were clarified. What, for instance, is the distinction between a breach and an incident? How serious is a "material" breach? Where reporting requirements depend on an assessment of the "sensitivity of the information," the "number of individuals affected," or the risk of "significant harm," respondents were also worried about the potential for misinterpretation and misjudgments.

- The most common cause (51 percent) of breaches reported by respondents were employee errors, such as typing in the wrong e-mail address, faxing a document to the wrong organization, or entering group e-mail addresses in the "To" line, rather than the "BCC" line, thus making them visible to other recipients. "System glitches," including lost laptops or data-storage devices, were blamed in 26 percent of cases.

- Most respondents were confident that if an employee made a mistake, he or she would report it to a supervisor. Respondents generally felt that their staff understood that resolving a breach to the satisfaction of the affected customers is more important than meting out punishment to the employee who made the mistake.

- Only two organizations reported external breaches, including an outsider gaining access to a company's database.

We were pleased to see that, of the six companies in the study that had reported a breach to our Office, five rated the overall experience as either positive or "extremely" or "very" positive. One organization said the experience was "mixed."

Those who rated the overall experience as positive provided the following comments:

"The OPC understood the realities of the situation and were extremely focused on what had been done to stop the situation, what was done to assist the customer, and what measures had been taken to prevent it from happening again."

"The OPC was supportive and not dogmatic."

REACHING OUT TO CANADIANS

An important part of our role is to inform Canadians about their privacy rights and provide information to organizations about how they can respect their obligations under PIPEDA.

Over the course of a normal day, the thoughts of Canadians rarely focus on how their personal information is being handled. They may pause to enter a PIN, or stop to check a box on a financial form, but the average Canadian will likely not linger long before sharing their personal information with friends, family and others on social networks, or with shops, marketers and other commercial organizations.

Similarly, many businesses in Canada find that they collect personal information as part of their daily routine, but do not necessarily have the training or the resources to evaluate the risk posed by poor or non-existent information security practices. This is particularly true of small businesses, where a small team of employees is often relied upon to deliver products or services as quickly and efficiently as possible.

Our Office has put in place a number of programs and activities to encourage Canadians of all ages to spare a few seconds to evaluate the risks and benefits of handling personal information.

These outreach programs try to deliver simple but effective advice on common privacy issues to a variety of community and industry groups, using more traditional tactics as well as technological solutions.

SPEAKING ENGAGEMENTS

In its simplest form, the Office's outreach program coordinates presentations on legal, technical, cultural and legislative topics by staff members to meetings of schools, universities, community groups and industry associations. We are serious about sharing the expertise accumulated by our staff and allowing individual Canadians to personally pose those questions most important to them.

In 2009, we participated in approximately 150 public events across the country. For example, the Commissioner and Assistant Commissioners spoke to a number of events aimed specifically at privacy professionals, as well as other conferences involving experts in security, communications, technologies, the online world and legal affairs.

These included, for example, the Northwind Privacy Invitational Forum, the International Institute of Communications Conference, an OECD committee's Technology Foresight Forum on Cloud Computing, the Ontario Bar Association and the Geomatics Industry of Canada Annual Leaders Forum.

Other officials from our Office also spoke at high schools, colleges and universities, industry associations, local business associations and community groups.

BUSINESS INITIATIVES

Although PIPEDA is nearly 10 years old, our surveys have found that many businesses could benefit from additional training in privacy and data protection. As a result, we try to focus our outreach on providing information and tools that are convenient for executives, managers and employees already facing a busy schedule.

In 2009, that meant a growing number of presentations to monthly meetings of local Chambers of Commerce, economic development offices, provincial and regional industry associations, and conferences targeted at small businesses.

We also meet regularly with major industry associations, including the Canadian Bankers Association, the Insurance Bureau of Canada, the Canadian Life and Health Insurance Association, the Retail Council of Canada, and the Canadian Marketing Association.

We are developing tools that allow small business people to learn in the comfort of their own offices. In 2010, our popular *A Guide for Businesses and Organizations: Your Privacy Responsibilities* will be supplemented with a refreshed online tool that will walk a manager or employee through an evaluation of their information handling practices, and provide advice on how to strengthen them.

We have also developed a number of other guidance documents for the private sector. In 2009, for example, we issued guidance on covert video surveillance in the private sector and the processing of personal data across borders.

While we publish all of our guidance documents and other publications on our website, we also distribute them at many conferences and other events. In 2009, we distributed close to 14,000 printed versions of our publications.

HARMONIZATION OF PRIVATE SECTOR OVERSIGHT

The provinces of Quebec, Alberta and British Columbia have provincial private sector privacy legislation that has been declared to be substantially similar to PIPEDA. Businesses operating in several jurisdictions are often required to comply with more than one private-sector privacy law.

Given this diverse legislative landscape, cooperation between jurisdictions is a very important component of provincial and federal privacy legislation.

This is because there are circumstances where privacy offices have concurrent or overlapping jurisdiction over organizations operating across Canada. In addition, businesses operating across the country are looking for harmonization and clarity in their responsibilities to protect personal information, and Canadians are looking for effective privacy protection.

Effective and efficient private sector oversight requires coordination and regular communication between jurisdictions.

Failure to take full advantage of these cooperative opportunities will only serve to frustrate business owners and individuals and, ultimately, will be detrimental to the privacy rights of Canadians.

Our Office, along with our counterparts in Alberta and British Columbia, have established the Private Sector Privacy Forum, which includes senior staff from each jurisdiction, to coordinate and harmonize, wherever possible, federal and provincial privacy oversight of the private sector in Canada.

The forum's work has allowed our Office to collaborate with Alberta and British Columbia in a number of areas, including joint investigations, parallel investigations, joint guidance documents and joint letters on issues of mutual concern.

The three offices have signed a Memorandum of Understanding in order to set out a framework to support federal/provincial collaboration and cooperation.

OUTREACH ACROSS CANADA

While we have a specific relationship with our counterparts in Alberta and British Columbia due to the similar private sector privacy regimes, our Office believes it is important to have a strong collaborative relationship with all provincial and territorial privacy commissioners.

By acting collectively and collaboratively, we can have a more positive impact on the federal government, on organizations and on the public.

An important aspect of this cooperation is regular pan-Canadian meetings, which allow commissioners to come together to discuss issues of mutual interest, share information and identify opportunities to work together.

Commissioners have started to work on a joint youth engagement strategy designed to generate awareness among Canadian youth of the privacy risks resulting from social networking on the Internet.

We've also launched a number of other initiatives in various jurisdictions aimed at both providing individuals with information and tools necessary to protect their privacy and to help organizations understand their obligations under privacy legislation.

A key goal is to talk to Canadians where they live and work. Our regional outreach program is intended to create stronger links between our office and different parts of the country and to help us better understand local issues.

The program has been established to build citizen awareness and self-protection capacity through targeted privacy awareness training and education for individuals and businesses.

ATLANTIC CANADA OUTREACH

In Atlantic Canada, we have entered into a two-year interchange agreement with the former Assistant Information and Privacy Commissioner for Newfoundland and Labrador. As a senior research and outreach advisor with our Office, he is based in Newfoundland and Labrador, but regularly travels to the other Atlantic Provinces.

This initiative has significantly increased our profile in Atlantic Canada. We are now able to accept a large number of speaking invitations – and initiate other presentations ourselves – to business and other groups as well as high schools.

SASKATCHEWAN PROJECT

We have also launched an outreach project in Saskatchewan which centres on developing privacy tools for credit unions and small businesses in the province.

As part of the project, we are working in partnership with the Saskatchewan Office of the Information and Privacy Commissioner to develop a website to deliver content and interact with Saskatchewan credit unions and small- and medium-sized enterprises.

The website will include a question and answer section so that privacy questions can be submitted to our Office and shared with the public.

We are also updating our e-learning tool for retailers to provide credit unions and small- and medium-sized enterprises with a user-friendly online diagnostic tool to address privacy management practices.

A major goal of the Saskatchewan project is to use the lessons learned there and apply them to future initiatives in other provinces and territories.

TORONTO INITIATIVE

Ontario – and more specifically Toronto – is a significant jurisdiction for our Office. Roughly two-thirds of our investigations originate in the province and the majority of these involve organizations located in the Toronto area. As well, a majority of industry associations – a significant target audience for our outreach efforts – are headquartered in the Toronto area.

Given these facts, we have begun to examine options for establishing a presence in the region.

CONTRIBUTIONS PROGRAM

Our Office is also funding public education initiatives through its Contributions Program. In 2009, for example, we provided resources to:

- The International Association of Privacy Professionals (IAPP) to bring free privacy education workshops in several Canadian cities to serve local privacy and information security professionals.

- Coopérative radiophonique de Toronto (CHOQ-FM) to roll out an awareness campaign about the Canadian privacy protection framework aimed at francophone minorities in Ontario and elsewhere outside Quebec.

- The Canadian Association of the Deaf to develop a campaign to inform deaf people about identity theft, privacy rights and Internet scams.

- The consumer group Option Consommateurs to host awareness seminars on identity theft and privacy protection aimed at seniors.

We also announced funding in 2009 for research projects on: information sharing on Facebook by teens and adults; the privacy polices and practices of direct-to-consumer genetic testing companies; deep packet inspection; the attitudes of people in Newfoundland and Labrador about privacy and personal health information; safeguards for health information; and privacy and camera surveillance.

Our Contributions Program was created in 2004 to support non-profit research on privacy and was subsequently expanded to include public education initiatives. It is considered one of the foremost programs of its kind in the world and has allocated close to $2 million to more than 50 initiatives.

The program was renewed in January 2010 after an evaluation determined that it is well-managed and continues to be pertinent. As a result, we announced that we were inviting proposals for projects that would explore privacy in four areas: information technologies; identity integrity and protection; genetic privacy; and national security. Up to $500,000 in funding will be available for research and public awareness initiatives in 2010-2011.

YOUTH PRIVACY

In the past, our Office has highlighted the challenges faced by young Canadians, constantly barraged with requests to join social networks, participate in marketing activities and share their information with commercial organizations. Just as they are struggling to develop their adult identity, they are encouraged to share elements of those identities across countless networks with possibly unintended consequences.

We recognize that young Canadians will make independent decisions about their identity and their participation in a networked society. We feel, however, that they should be aware of their rights, as well as the benefits and risks of sharing their personal information.

Over the past couple of years, our Office has stepped up its activities among young Canadians. Working with the tag line "Think before you click," we have begun to expand our outreach to students, parents, teachers and youth mentors. Just as with the business community, we are creating opportunities for young Canadians to learn about their privacy rights where convenient: at home, at school and online.

Our efforts are anchored by a specialized youth privacy website, youthprivacy.ca, where students, parents and teachers can find information and links to resources prepared by our and other offices. This is also the home to our annual youth privacy video competition, which has grown fourfold since being launched in 2008.

As well, the site hosts a blog written by and for young Canadians, presenting contemporary privacy issues in a voice and context that may be more digestible.

We believe, though, that online tools cannot succeed without more personal interaction. In 2009, the Office began a highly popular schedule of school presentations designed to highlight the risks and benefits of online social networks. At the same time, we began to meet with school leaders, librarians and academics across Canada to identify what other opportunities may exist to connect with young Canadians, and to discuss what themes and issues concern them the most.

CONCLUSION

The Office's outreach efforts are meant to amplify and broadcast the expertise and experience that has been developed by our staff, while encouraging others who might influence their community to examine issues around privacy and data protection.

As a relatively small office, our work seeks to take advantage of those existing activities and channels that have gained the trust and attention of Canadians.

PROTECTING PRIVACY IN A CHANGING ENVIRONMENT

Our 2009 policy development and parliamentary affairs work touched on a broad range of private-sector issues affecting the future privacy rights of Canadians. These issues included everything from anti-spam and identity theft initiatives to deep packet inspection.

In a world where the privacy landscape is constantly changing, it is critical that Canada's laws keep up.

The rapid technological developments we've seen in the first decade of the 21st century have come with many new risks for privacy. We have also seen a proliferation of identity theft as well as other frauds committed over the Internet – often by using spam e-mails as a weapon against unsuspecting Canadians.

Some changes which will have an important positive impact on privacy protection in Canada became law in 2009 and we hope to see others enacted into law soon. As well, we look forward to the tabling of further legislation in the near future.

PIPEDA REVIEW UPDATE

The House of Commons Standing Committee on Access to Information, Privacy and Ethics began a review of PIPEDA in 2006, which ended the following year with a report making numerous recommendations for the government's consideration or further discussion.

In response to the committee's report, the government agreed to further examine and take action on a number of issues.

For example, the government said that there is a need for a legislative requirement for businesses to alert individuals affected by data breaches in cases where there is a high risk of significant harm. As well, it supported the idea of mandatory reporting of breaches to our Office.

We believe a mandatory breach reporting regime has many benefits: Companies will have another incentive to take security of personal information seriously; people will receive timely information allowing them to protect themselves from identity theft; and our Office will be able to better track patterns and vulnerabilities in order to help the private sector avoid breaches.

Industry Canada has developed a draft model for a mandatory reporting regime and we hope to see legislative amendments introduced in the near future.

Our Office was also particularly pleased with the government's agreement that there is a need for the Privacy Commissioner to cooperate with other data protection authorities, both in Canada and abroad, in order to fulfill her mandate under PIPEDA.

Currently, PIPEDA only allows information sharing with Commissioners who oversee substantially similar laws – British Columbia, Alberta, Quebec and Ontario (where health privacy legislation has been declared substantially similar.)

Increasingly, our Office is receiving complaints that involve more than one jurisdiction and we would like to be able to work more closely with our counterparts in other countries. By sharing information, we can be more effective and efficient in our investigations.

In 2009, we saw the introduction of legislation which would allow us to do this. (This legislation, the *Electronic Commerce Protection Act,* is described in further detail below.)

The second Parliamentary review of PIPEDA would be expected in 2011.

PUBLIC CONSULTATIONS

Our Office is preparing a series of consultations on emerging technological trends in 2010 which will help shape the Office's input into the next parliamentary review of PIPEDA.

These public consultations will focus on two areas: the practice of tracking, profiling and targeting consumers online and issues around cloud computing. These issues are likely to have a significant impact on the privacy of Canadians and we would like to develop a deeper understanding of them.

We issued a call for written submissions or expressions of interest from people who would like to take part in formal discussion panels to be held in Toronto, Montreal and Calgary in 2010. We would like to hear the views of business, government, academics, consumer associations and civil society.

STREET-LEVEL IMAGING

Our Office has been closely following the development and use of online street-level imaging technology for several years.

Street-level imaging applications such as Google Street View and Canpages use various means of photographing the streetscape. Typically, a camera is mounted on top of a car that is driven down a street to capture 360-degree images. The images – which sometimes include identifiable people – are made available online on sites that allow users to take a virtual tour of a particular neighbourhood.

Our ongoing concerns about the commercial use of this technology centre on ensuring that it protects the privacy of Canadians by meeting the requirements of PIPEDA.

The issue also attracted the attention of members of Parliament in 2009.

The adequacy of Canadian privacy law in the face of new technologies was explored during a study on privacy and street-level imaging services by the Standing Committee on Access to Information, Privacy and Ethics.

The study ended when Parliament was prorogued in December 2009, however, the committee has the discretion to come back to the issue when Parliament resumes in 2010.

Our Office began to monitor this issue in 2007, when we learned that Google was photographing the streets of some Canadian cities for the eventual launch of its Street View application in Canada – without the apparent knowledge or consent of the individuals who appeared in the images.

We had a number of discussions with both Google and Canpages to discuss the need to comply with legal requirements such as knowledge and consent, safeguards and retention of personal information.

It is important, for example, that people receive adequate notification that cars will be collecting images in their neighbourhood. We recommended that these companies include visible markings on their camera vehicles and also use press releases, local media and websites to outline dates and locations for filming.

These discussions resulted in improved privacy protection on both sites. Google and Canpages agreed to 'blur' the faces of individuals and also to provide an easy and timely means for people to have images of themselves or their homes removed. We also saw some improvement in the way notifications are provided.

In our view, however, the companies could still be doing more. We would like to see more investment in notification, using various channels to reach more people, and providing more precise information about where filming will be and when. We want people to have more control and choice over whether or not their image is captured in a public place.

Our understanding is that the blurring technology is less than perfect, and we encouraged the companies to continue to look for ways to improve this technology.

Our Office, along with our counterparts in British Columbia, Alberta and Quebec, worked together to develop guidance on our expectations with regard to this new technology. The guidelines, *Captured on Camera,* are on our website.

The Commissioner has often reminded multinational companies that launch online products and services in Canada that they must comply with Canadian privacy laws.

IMPORTANT LEGISLATIVE DEVELOPMENTS IN 2009

FIGHTING IDENTITY THEFT

In 2009, after several years of study, we saw the adoption of legislation to combat identity theft. *An Act to amend the Criminal Code (identity theft and related misconduct)* received Royal Assent in October 2009 and came into force in January 2010.

The legislation amends the *Criminal Code* to make the obtaining, selling or possessing of another person's "identity documents", such as a birth certificate or a driver's licence, an offence. The possession of, or trafficking in "identity information" is criminalized where the information is to be used to commit a crime such as fraud. The Act also expands a number of existing *Criminal Code* provisions dealing with matters such as the theft or forgery of credit cards, mail theft and forging documents.

Our Office appeared before the Senate Standing Committee on Legal and Constitutional Affairs in May 2009 and the House of Commons Standing Committee on Justice and Human Rights in October 2009.

On both occasions, we expressed our support for the legislation. Given the complexity of the problem and the many forms that identity theft can take, we also urged the government to take a coordinated approach to fighting identity theft that draws on the resources of police and regulators, the public and private sectors and federal and provincial officials.

As well, we outlined how reform of the *Privacy Act* and mandatory breach notification would empower Canadians to combat identity theft and motivate companies and government organizations to properly safeguard personal information.

STOPPING SPAM

The Minister of Industry introduced the *Electronic Commerce Protection Act* in April 2009. The bill was primarily aimed at fighting spam, but it also included some legislative amendments which would have a significant impact on our Office.

We've been urging the government to introduce anti-spam legislation for some time. Canada is the only G-8 country without such legislation.

The *Electronic Commerce Protection Act* would prohibit:

- The sending of unsolicited commercial electronic messages without consent;
- The use of false and misleading representations, for example, misleading claims about a product;
- The use of computer systems to collect electronic addresses or other personal information without consent; and
- The unauthorized altering of transmission data so that the message is diverted.

The Act would also require that any electronic message sent must be in a prescribed form, i.e., it must identify the person who sent the message and the person on whose behalf it is sent, provide accurate contact information for these parties, and set out an unsubscribe mechanism.

The Canadian Radio-television and Telecommunications Commission (CRTC), the Competition Bureau and our Office would be responsible for enforcement, with Industry Canada playing a coordinating role. We would be primarily responsible for dealing with complaints with respect to the unauthorized collection, use or disclosure of personal information. The bill also contained a private right of action.

When our Office appeared before the House of Commons Standing Committee on Industry, Science and Technology in June 2009 to comment on the bill, Assistant Commissioner Denham stated: "We believe that it strikes the right balance between giving people greater control over the e-mail and text messages they receive while allowing legitimate businesses to continue to communicate with their clients and customers."

This is important legislation because it has the potential to reduce spam and other forms of unsolicited messages.

In addition, it would increase our ability to share information under PIPEDA with other enforcement agencies – not just with the CRTC and Competition Bureau with respect to spam but more broadly. As a result of the proposed amendments, the Commissioner would have a greater ability to exchange information and cooperate with provincial and foreign counterparts who enforce laws similar to PIPEDA.

As well, the bill would provide the Commissioner with greater discretion in accepting complaints or discontinuing investigations – whether they involve spam or other privacy issues. For example, it would allow the Commissioner to decline to take a complaint which is frivolous, lacking in sufficient evidence or could be dealt with under other federal or provincial laws.

Like many other data protection authorities around the world, we have argued that a better use of our investigative resources would be to focus on privacy issues of a broader, systemic interest.

As a result of the prorogation of Parliament on December 30, 2009, all of the bills introduced during the 2nd Session of the 40th Parliament "died". However, we hope that the legislation, which we believe would help us better protect the privacy interests of Canadians, will be reintroduced in 2010.

SUBMISSIONS TO THE CANADIAN RADIO-TELEVISION AND TELECOMMUNICATION COMMISSION (CRTC)

In 2009, our Office made written submissions to the CRTC on Deep Packet Inspection and Confidential Customer Information.

DEEP PACKET INSPECTION

Our submissions to the CRTC's review of the Internet traffic management practices of Internet service providers focused on the privacy implications of the potential uses of deep packet inspection.

Deep packet inspection is a tool that allows network providers to peer into the digital packets that make up a message or transmission over a network. It is used to maintain the integrity and security of networks, searching for signs of protocol non-compliance, viruses, malicious code, spam and other threats.

This technology raises privacy concerns because it can involve the inspection of personal information – e-mail messages, for example – sent from one person to another.

We urged the CRTC to exercise its jurisdiction to protect the privacy of Canadians under the *Telecommunications Act* and to craft regulatory measures that ensure the personal information of Canadian Internet users is respected. (The submissions are available on our website.)

We were pleased that, following its review, the CRTC created a number of privacy protective requirements for Internet service providers.

These directives included prohibitions on both the use of personal information collected for the purposes of network management for any other purpose and the disclosure of personal information collected for network management purposes – even with customer consent.

As well, Internet service providers must be transparent with their customers about how they use Internet traffic management tools such as deep packet inspection on their networks.

(A summary of an investigation by our Office into a complaint about deep packet inspection is included on page 44.)

CONFIDENTIAL CUSTOMER INFORMATION

We also made a written submission to the CRTC during its review of the appropriateness of continued regulatory measures to safeguard confidential customer information collected, used and disclosed by telecommunications service providers. (The submission is available on our website.)

We called on the CRTC to maintain requirements for telecommunications service providers to obtain express consent from customers when disclosing confidential customer information. As well, we said it was important for the CRTC to maintain its important regulatory role in protecting personal information at a time when the threats to privacy are ever increasing.

The CRTC ultimately determined that implied consent to disclosure of confidential customer information is permissible under some circumstances, such as disclosure to a corporate affiliate involved in supplying the customer with services.

PRIVACY AND THE WIRELESS SECTOR

In 2009, the Senate Standing Committee on Transport and Communications studied the wireless sector and other emerging issues related to communications.

The Commissioner appeared before the committee to discuss the privacy implications of behavioural marketing and the tracking of consumers' online activities; location-based data collection made possible through GPS-enabled mobile devices; and cloud computing, where personal information can be stored on servers in many locations.

STRATEGIC PRIORITIES

Concepts of privacy are changing fast in today's world, and so are the factors that threaten it. Our Office monitors a broad range of challenges, and has identified four emerging issues that we predict will have especially powerful impacts on privacy in the years ahead. We believe that information technologies, identity integrity, genetic advances and national security are the most important challenges for privacy advocates to address.

INFORMATION TECHNOLOGY

Virtually every activity that an individual undertakes nowadays – whether it is keeping up to date with family and friends, purchasing goods and services (online and off) or dealing with government – involves the use of some form of information technology. And that technology is evolving at a rapid pace, with new devices and applications emerging on an almost daily basis.

We monitor and research developments in information technology that could have an impact on privacy – and we consider how to address those developments.

As part of our work in this area in 2009, we held briefing sessions with private industry to gather information about how new technologies work, how these technologies might be used and what the implications on privacy may be. We also initiated an on-going series of "tech talks" – presentations to help improve staff awareness and understanding of subjects ranging from botnets to social engineering.

We also organized workshops on the privacy implications of geospatial technologies. One focused on the privacy implications of merging geospatial and health information, including the risk of re-identifying individuals from supposedly anonymous or de-identified data sets. A second workshop looked at the privacy implications of mobile marketing and other location-based services.

IDENTITY INTEGRITY

Canadians today face demands to share their personal information with a wider group of friends, family, government organizations and commercial enterprises. There is social and financial value in everything from demographic data to brand preference. This information is explicitly shared as part of our membership in loyalty card programs and social networks. We may not realize that information is also being collected as we browse commercial websites or answer questions while paying for purchases in stores.

Information collection, and the breadth of data types being collected, accelerates with the introduction of every new innovation in software and hardware. Canadians are finding it hard to keep abreast of technological innovation, all the while struggling to define their identity in a digital world. They want an element of control in how they are identified and portrayed in both private and public settings.

We are working to better understand the forces that encourage the greater collection of personal information, and how Canadians react to repeated attempts to collect this personal information. We are conducting research into the social and economic motivation for individuals to provide personal information, as well as examining standards and frameworks that provide individuals with greater control over their information. Our Office is also beginning to dig into specific areas of the information economy, such as locational data.

We are developing tools to help young Canadians to make better choices about how they share information and participate in social networks. We are reworking simple guides to help small businesses assess how they collect and protect personal information, and we are providing guidance on the use of technology by public and private sector organizations.

GENETIC INFORMATION

Privacy is often defined in terms of our ability to determine with whom and in what circumstances we will share personal information about ourselves.

Controlling who has access to our genetic information and how it will be used is emerging as one of *the* critical privacy issues of the 21st century.

In 2009, we organized a workshop with external experts in the field of genetics to help us build our in-house expertise and better understand the challenges involved in protecting genetic information. The workshop focused on four issues: "bio-banking," the use of genetic information for forensic (law enforcement) purposes, direct-to-consumer genetic testing, and the use of genetic information for insurance purposes.

As part of a Parliamentary review of the *DNA Identification Act*, we appeared before the House of Commons Committee on Public Safety and National Security as well as the Senate Legal and Constitutional Affairs Committee.

During our appearances, we expressed concerns about expanding the national DNA database by taking DNA from a greater number of offenders for a broader range of offences, allowing "familial searches" and increasing international information sharing.

We also co-sponsored a workshop with Genome Canada on research bio-banks and consent. Senior federal policy-makers and researchers came together to discuss social, legal and ethical issues raised by the growing availability of genetic information. We are involved in planning two related events to be held in 2010.

NATIONAL SECURITY

We often think of national security as strictly a public sector privacy issue, however, as we saw in 2009, there can also be implications for the private sector.

In June, the federal government introduced two pieces of legislation aimed at giving Canadian law enforcement, national security agencies and others broader powers to acquire digital evidence from private-sector organizations.

Bill C-46, the *Investigative Powers for the 21st Century Act*, would allow authorities to order telecommunications providers to preserve and turn over the details of their subscribers' communications. Authorities would also have the power to apply for special orders to trace mobile communications devices and, by extension, their owners.

Bill C-47, the *Technical Assistance for Law Enforcement in the 21st Century Act*, would give authorities access to information about subscribers and their mobile devices, even without a warrant. The bill would also oblige all telecommunications companies to build in a capability allowing authorities to intercept communications on their networks.

The provisions of the proposed Acts raised serious privacy concerns. For instance, without a warrant, authorities could gain access to personal information such as unlisted telephone numbers, and e-mail and IP addresses.

Canadians consider much of this personal information to be sensitive and expect it to be kept confidential. Canadians also expect their use of computers and mobile devices to remain private.

The legislation was not limited to investigations of serious criminal offences, but also could be used to target even minor infractions and non-criminal matters.

It died on the order paper with the prorogation of Parliament in December 2009, but could be reintroduced again in the future.

In September 2009, privacy commissioners and ombudspersons from across the country issued a joint resolution calling on Parliamentarians to ensure there is a clear and demonstrable need to expand the investigative powers available to law enforcement and national security agencies to acquire digital evidence. We also urged Parliament to take a cautious approach to legislative proposals to create an expanded surveillance regime that would have serious repercussions for privacy rights.

IN THE COURTS

Our Office continued to be involved in a number of matters before the Courts in 2009. Under Section 14 of PIPEDA, a complainant may, 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.

A number of Commissioner-initiated applications filed under Section 15 of the Act remained ongoing. Section 15 of PIPEDA allows the Privacy Commissioner, with the consent of the complainant, to apply directly to the Federal Court for a hearing in respect of any matter covered by Section 14. It also allows the Commissioner to appear before the Federal Court on behalf of any complainant who has applied for a hearing under Section 14; or, with the permission of the Federal Court, to appear as a party to any Section 14 hearing not initiated by the Commissioner.

The Privacy Commissioner regularly initiates court action where an organization refuses to adopt her recommendations in well-founded cases. We have found this has helped establish a high level of compliance with recommendations.

In some cases, the Privacy Commissioner also files preliminary documents in certain court proceedings to be removed as a party where she is improperly named as one.

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

SETTLED CASES

Privacy Commissioner v. X
Federal Court File No. T-572-09

This case stems from a denial-of-access complaint filed with our Office. In the complaint, the complainant alleges that her psychologist denied her access to her personal information. Specifically, the complainant sought access to her psychologist's peer review file notes which pertained to the psychologist's discussions with her colleagues about the complainant's case.

The psychologist contended that the notes did not contain the complainant's personal information because the notes were "anonymized" in that they referred only to the complainant's case in general terms, and did not refer to the complainant by name.

The OPC disagreed with this point of view and concluded that the notes did contain personal information of the complainant, and accordingly the complainant should have access to her personal information in the notes. The psychologist however continued to deny the complainant access to the notes.

On April 9, 2009 the OPC filed a Notice of Application seeking a declaration from the Court that the notes contain the complainant's personal information and requiring the Respondent to provide the complainant with access to her personal information.

Prior to the matter reaching a hearing, the respondent released to the complainant all of the personal information to which she was entitled under PIPEDA. Accordingly, the Privacy Commissioner discontinued her application against the respondent.

COMPLAINANT-INITIATED COURT APPLICATIONS UNDER SECTION 14 OF PIPEDA

X v. The Bank of Nova Scotia et al
Federal Court File No. T-582-08

An individual complained to our Office that the Bank of Nova Scotia had improperly disclosed his personal financial information to a third party who, he alleged, had substituted her own mailing address for the address he had placed on file with the bank.

An investigation determined that the complaint was well-founded and resolved. It found that the bank had appropriate policies in place that would likely have prevented the contravention of PIPEDA if they had been followed. The incident was the result of an isolated human error. The bank implemented all of the Commissioner's recommendations. It also agreed to apologize to the complainant and provide copies of misdirected account statements.

On April 11, 2008, the complainant filed a Notice of Application with the Federal Court naming the bank and the third party as Respondents. The Applicant sought damages of $400,000, declaratory relief and various orders against the Bank. The Applicant sought similar relief against the third party.

On June 9, 2008, the Privacy Commissioner was granted leave to appear as a party. However, on August 24, 2009, the Applicant discontinued his application against the bank. He is continuing the application against the third-party Respondent.

Given that the third party was not the subject of the Privacy Commissioner's investigation and report, the OPC's view is that the application is no longer a proper Section 14 application (the proper respondent to a Section 14 application is the respondent organization originally subject of the OPC's report). As such, we have informed the Court that we take no position on the matter as between the Applicant and the third party and will no longer be participating in the proceedings.

Note: This case was reported in the 2008 Annual Report.

X. v. J.J. Barnicke Ltd.
Federal Court File No. T-1349-06

The complainant alleged improper collection of personal information by a company's vice-president who had sent out an e-mail asking whether anyone knew which firm the complainant worked for. An investigation by our Office determined that the collection complaint was not well-founded. The complainant filed an application in the Federal Court seeking damages in the amount of $75,000 and a declaration that his rights under PIPEDA had been violated.

As the issue of damages under paragraph 16(c) of PIPEDA was raised in the application, our Office participated in the proceedings as an Added Party in order to set out our view as to how the Court should approach awarding damages sought pursuant to PIPEDA.

On February 18, 2009, the Federal Court dismissed the complainant's application after reaching the same conclusions that the Assistant Privacy Commissioner had following her investigation.

Note: This case was also reported in our 2007 and 2008 Annual Reports.

COMMISSIONER-INITIATED COURT APPLICATIONS UNDER SECTION 15 OF PIPEDA

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 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.*

On January 30, 2009, we filed a Notice of Application seeking a declaration confirming the Privacy Commissioner's statutory jurisdiction to investigate claims of solicitor-client privilege under the exemption from the right of access in paragraph 9(3)(a) of the Act.

The matter was scheduled to be heard before the Federal Court on March 23, 2010.

Note: This case was reported in our 2008 Annual Report.

Privacy Commissioner of Canada v. State Farm
Federal Court File Nos. T-1187-09, T-1188-09, T-1189-09

The applications stem from denial of access complaints against State Farm. The insurance company had refused to provide the complainants with access to their personal information on the grounds that PIPEDA does not apply because State Farm was not engaged in "commercial activities" in relation to the collection, use and disclosure of the personal information requested by the complainants, and on the grounds that any information related to the complainants would be exempt from disclosure under paragraphs 9(3)(a) (solicitor-client privilege) and/or 9(3)(d) (information generated in the course of a formal dispute resolution process) of PIPEDA.

In our Reports of Findings, our Office concluded that State Farm was engaged in commercial activities and that it was up to State Farm to prove any claim of privilege it asserted and/or to justify reliance on PIPEDA's exemptions in relation to information generated in the course of a formal dispute resolution process.

Since State Farm failed to provide sufficient information to satisfy its onus, our Office concluded that the complainants' access complaints were well-founded.

On July 22, 2009, our Office filed three applications which, among other things, seek:

- Declarations that State Farm was engaged in commercial activities;
- Orders confirming or denying claims by State Farm that the documents for which the complainants sought and were denied access were protected by

solicitor-client privilege and/or as being information generated in the course of a formal dispute resolution; and

- Declarations that the Respondent must provide access to any personal information unlawfully withheld from the complainants in breach of PIPEDA.

On September 29, 2009 the Court, in response to a motion filed by State Farm, ordered a stay of proceedings in all three applications until there is a final determination in the case of *State Farm v. The Privacy Commissioner and Attorney General of Canada* which will resolve a similar issue respecting whether State Farm was engaged in "commercial activities." For more detail, see page 86.

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

This matter involves the collection of personal information of bar patrons through the use of a machine that copies and retains personal information appearing on the front of an identification card such as a driver's licence.

Following an investigation into a complaint filed by a Canad Inns patron, the Assistant Privacy Commissioner 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. She 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, we filed a notice of application for a hearing before the Federal Court to enforce our recommendations.

Following court-ordered mediation in early 2009, Canad Inns was given time by the Court to determine feasible means to limit the personal information it collects. As the parties are reviewing Canad Inns' efforts in this regard, the matter remains before the Court.

Note: This case was previously reported in our 2007 and 2008 Annual Reports.

JUDICIAL REVIEW APPLICATIONS UNDER 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

State Farm filed a judicial review application on April 17, 2009 in the Federal Court. In its application, State Farm asserts that the Privacy Commissioner acted without jurisdiction, acted beyond her jurisdiction and erred in law in making her decision to carry out an investigation of a denial of access complaint against State Farm.

The main issues raised in this application are whether information collected by an insurer for the purposes of investigating, defending or indemnifying a third party insurance claim is collected, used or disclosed in the course of "commercial activity" under PIPEDA. Alternatively, in the event the Court determines that State Farm is engaged in commercial activities, State Farm is challenging the constitutionality of the application of PIPEDA to these activities on the grounds that it conflicts with provincial rules of civil procedure and provincial legislation regulating the insurance industry, and thus is outside the legislative authority of Parliament.

The OPC has raised the argument that State Farm's application for judicial review is premature because it was initiated prior to the OPC having issued its Report of Findings. If the Court supports the OPC's position on this argument, the merits of State Farm's application will not be heard.

A hearing was scheduled for April 13, 2010.

Note: This is a continuation of the matter reported on in the 2008 Annual Report (State Farm Automobile Insurance Company v. Privacy Commissioner of Canada, New Brunswick Court of Appeal)

X v. Karen Rucas and Associates and Privacy Commissioner of Canada
Court File No. T-1092-09

This is a judicial review application commenced by the Applicant to review the Report of Findings issued by our Office in relation to the Applicant's denial-of-access complaint against the Respondent organization. Our Office has filed a motion to strike the application on the grounds that the application was substantially out of time, failed to raise any allegations that could properly be the subject of judicial review, and would be more appropriately addressed as an application pursuant to Section 14 of PIPEDA.

On February 10, 2010, the Court granted our motion and dismissed the application with costs awarded to the Privacy Commissioner.

OTHER

Accusearch, Inc., d/b/a Abika.com, and X v. U.S. Federal Trade Commission

Our Office was granted leave to file an *amicus curiae* brief (a written submission to help guide a court in its decision-making process) in a proceeding before the United States Tenth Circuit Court of Appeals in *Accusearch, Inc., d/b/a Abika.com, and X v. U.S. Federal Trade Commission.* This company, a U.S.-based search services website, had also been the subject of a complaint to our Office. Our Office released the results of its investigation into Accusearch, Inc. in 2009 as well. (See page 44 for details.)

In our view, the case before the U.S. Tenth Circuit Court of Appeals related to transborder data flows between the U.S. and Canada, how data brokers collect, use and disclose personal information without the knowledge or consent of the individual concerned, and how online trade in personal information impacts privacy rights. As such, our Office's *amicus curiae* brief outlined how the Court's decision would have a direct impact on the privacy rights of Canadians and the business reputation of Canadian organizations affected by the actions of data brokers.

In June 2009, the U.S. Tenth Circuit Court of Appeals affirmed a judgment for injunctive and monetary relief that had been granted against Accusearch, Inc. by a judge of the United States District Court for the District of Wyoming.

Note: This case was also reported in our 2008 Annual Report.

SUBSTANTIALLY SIMILAR PROVINCIAL AND TERRITORIAL LEGISLATION

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 which has been declared substantially similar.

In December 2009, we were asked by Industry Canada to review and comment on whether New Brunswick's *Personal Health Information Privacy and Access Act* (PHIPAA) is substantially similar to PIPEDA so it can include our views in its recommendation to the Governor in Council.

The New Brunswick Government has asked that PHIPAA be declared substantially similar to PIPEDA. PHIPAA received Royal Assent on June 19, 2009 and it is scheduled to come into force in 2010.

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

- Incorporate the 10 principles in Schedule 1 of the 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.

At the time of writing this report, we had not concluded our review of the legislation.

THE YEAR AHEAD

As we begin 2010, we expect another busy year filled with new privacy challenges. A taste of what's ahead:

INVESTIGATIONS

New complaints to our Office will mean that we will continue to examine privacy issues related to social networking sites in 2010.

We received a new complaint about Facebook and launched another investigation. This complaint focused on a tool introduced by Facebook in mid-December 2009, which required users to review their privacy settings. The complainant alleged that the new default settings would have made his information more readily available than the settings he had previously put in place.

The complaint mirrors concerns that our Office heard and expressed to Facebook in late 2009. We saw on blogs and chat groups that some Facebook users have been disappointed by certain changes made to the site.

We also received a complaint from a public interest advocacy group about the Edmonton-based social networking site, Nexopia.

CONSULTATIONS

Emerging technological trends will also be the focus of a series of consultations we are planning for 2010.

The public consultations will involve in-depth examinations of the practice of tracking, profiling and targeting consumers online and cloud computing.

The goal is to gather information that will help inform our Office's policy development, and also to prepare for the next review of PIPEDA.

PRIVACY AND LEGISLATION

With the next review of PIPEDA expected in 2011, we will become increasingly focused on whether changes are needed to ensure the law remains capable of addressing emerging threats to privacy.

We have commissioned two leading academics – Lorne Sossin, of the University of Toronto, and France Houle, of the Université de Montréal – to analyze the effectiveness of the ombudsman model under PIPEDA in regulating the personal information handling practices of the private sector. This has been an issue of active interest and debate since PIPEDA first came into force in 2001.

Issues that they will explore include:

- The regulatory context (economic, legal and political) under which PIPEDA was first enacted compared to the current environment;

- How best to evaluate the ombudsman model under PIPEDA (including a comparative analysis with the models in place in selected provinces, as well as a sampling of models used in other countries); and

- A qualitative analysis of our Office's effectiveness.

The report will help inform our position moving forward into the next review of PIPEDA. We expect to make the final report public in 2010.

In terms of Parliamentary issues, we hope to see the reintroduction of the *Electronic Commerce Protection Act*, which aims to fight spam. The legislation is also extremely important to our Office because it includes amendments that would allow us to work more closely with our provincial and international counterparts. As well, it would provide us with greater discretion in accepting complaints.

We also hope to see the introduction of legislation that would make it mandatory for private-sector organizations to report significant data spills.

INTERNATIONAL

We will also continue to be an active participant on the international privacy stage.

The work of the OECD will be a particular focus for us. To mark the 30th anniversary of its *Guidelines on the Protection of Privacy and Transborder Data Flows*, the OECD is planning a series of events to look at how the guidelines have been put into practice.

Commissioner Stoddart has been asked to head a volunteer group helping the OECD plan these events. Among other things, our Office will help draft an OECD discussion paper that describes the new privacy environment, and identifies the challenges to protecting personal information in the 21st century. We are also participating in the planning of two workshops and a conference that will be held in October 2010 in conjunction with the International Conference of Data Protection and Privacy Commissioners.

APPENDIX 1 – DEFINITIONS; INVESTIGATION PROCESS

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.

INVESTIGATIVE 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 – INVESTIGATION STATISTICS FOR 2009

COMPLAINTS RECEIVED BY TYPE

Complaint Type	Count		Percentage	
	2009	2008	**2009**	2008
Access	64	73	28	17
Use and Disclosure	59	162	26	38
Collection	33	93	14	22
Consent	22	24	10	6
Safeguards	21	30	9	7
Accountability	10	8	4	2
Accuracy	9	8	4	2
Openness	4	3	2	<1
Retention	3	0	1	0
Time Limits	3	11	1	3
Challenging Compliance	2	2	1	<1
Correction/ Notation	1	5	<1	1
Fee	0	1	0	<1
Other	0	2	0	<1
Total	**231**	422		

As discussed earlier in this report, the numbers of complaints we received in 2009 dropped for all types of complaints. Over the last several years, access, use and disclosure and collection complaints have accounted for a significant proportion of all complaints to our Office.

Access complaints accounted for the largest number of complaints we received in 2009. Access complaints deal mainly with allegations that organizations have not responded to requests for personal information or have not provided all of the information to which individuals believe they are entitled.

Access complaints accounted for a significantly higher proportion of complaints received than we saw last year. We have seen a number of access complaints related to the insurance sector. In some cases, lawyers and/or "facilitators" are filing complaints against one or more organizations on behalf of a complainant. These types of complaints are often in relation to a legal dispute between an insurer and an individual.

The second-largest group of complaints related to how organizations had used and disclosed personal information. For example, this type of complaint often involves allegations of personal information being used for purposes other than those for which it was collected, or being disclosed to third parties without an individual's consent.

Collection complaints, the third-largest group, usually concern the collection of information without proper consent, or the collection of more information than required for the stated purpose.

CLOSED COMPLAINTS BY FINDING

Finding	Count		Percentage	
	2009	**2008**	**2009**	**2008**
Not well-founded	142	74	24	18
Discontinued	118	108	20	26
Early resolution	76	19	13	5
Well-founded and resolved	61	30	10	7
Settled	55	108	9	26
Resolved	51	27	9	7
Well-founded	45	25	8	6
No jurisdiction	35	20	6	5
No report prepared pursuant to 13(2)	4	0	1	0
Other	0	1	0	<1
TOTAL	**587**	**412**		

We closed a significantly higher number of cases in 2009 than the year before as a result of a concerted effort to eliminate a backlog of investigation files.

We also saw that there were significant year-over-year changes in the breakdown by type of finding. These shifts can largely be attributed to two factors: first, we were closing many older investigations where finding a quick solution was not possible; and, second, we introduced a formal early resolution process at the end of 2009.

We were very pleased to see a big jump in the number of Early resolution findings, which we hope will account for a larger and larger share of our overall findings as more complaints are sent to our new early resolution team. (See page 55 for details of this new process.)

In the past, many easy-to-resolve cases were determined to be Settled after being sent to an investigator. The growing number of Early resolution findings means we are now seeing fewer Settled findings.

Another reason for the far lower number of Settled cases in 2009 was that we were closing a large number of backlogged cases, which did not lend themselves to being settled.

We also had a higher percentage of Not well-founded cases in 2009. This change also relates to our closed backlog files. A significant number of our backlogged insurance complaints were Not well-founded.

FINDINGS BY COMPLAINT TYPE

	Discontinued	Early Resolution	No Jurisdiction	Not Well-founded	No Report prepared pursuant to 13(2)	Resolved	Settled	Well-founded	Well-founded Resolved	TOTAL	Percentage
Use and Disclosure	50	23	8	59	0	10	15	15	27	**207**	35
Access	19	19	5	17	4	15	12	8	15	**114**	19
Collection	25	12	12	25	0	12	13	8	6	**113**	19
Safeguards	3	5	3	18	0	7	7	6	2	**51**	9
Consent	5	8	1	8	0	2	2	2	1	**29**	5
Time Limits	3	3	1	1	0	2	2	2	3	**17**	3
Accuracy	3	2	2	4	0	2	0	1	1	**15**	3
Accountability	3	1	2	2	0	1	1	1	0	**11**	2
Openness	2	0	1	3	0	0	0	1	2	**9**	2
Correction/ Notation	1	2	0	2	0	0	0	0	2	**7**	1
Challenging Compliance	1	1	0	0	0	0	1	0	2	**5**	< 1
Retention	0	0	0	1	0	0	2	1	0	**4**	< 1
Fee	1	0	0	2	0	0	0	0	0	**3**	< 1
Other	2	0	0	0	0	0	0	0	0	**2**	< 1
TOTAL	**118**	**76**	**35**	**142**	**4**	**51**	**55**	**45**	**61**	**587**	

FINDINGS BY INDUSTRY SECTOR

	Discontinued	Early Resolution	No Jurisdiction	Not Well-founded	No Report prepared pursuant to 13(2)	Resolved	Settled	Well-founded	Well-founded Resolved	TOTAL
Financial Institutions	17	31	8	30	0	12	14	5	26	**143**
Insurance	27	9	2	32	3	6	5	4	7	**95**
Sales	42	9	6	10	0	7	6	5	6	**91**
Telecommunications	8	15	2	15	1	12	6	3	1	**63**
Transportation	6	2	7	15	0	6	5	4	7	**52**
Accommodations	5	1	4	12	0	4	1	8	3	**38**
Other	3	5	2	4	0	2	6	4	7	**33**
Professionals	5	1	1	7	0	1	3	7	2	**27**
Health	1	2	2	13	0	0	0	1	1	**20**
Services	4	1	1	3	0	1	6	3	0	**19**
Entertainment	0	0	0	1	0	0	3	1	0	**5**
Rental	0	0	0	0	0	0	0	0	1	**1**
TOTAL	**118**	**76**	**35**	**142**	**4**	**51**	**55**	**45**	**61**	**587**

INVESTIGATION TREATMENT TIMES BY COMPLAINT TYPE

Complaint Type	Average Treatment Time in Months
Consent	11
Accountability	15
Accuracy	15
Other	17
Retention	18
Time Limits	18
Use and Disclosure	18
Openness	19
Access	20
Collection	20
Correction / Notation	20
Safeguards	20
Fee	32 *
Overall Average	**18.5**

* The Fee category included only three investigation files.

INVESTIGATION TREATMENT TIMES BY FINDING

Disposition	Average Treatment Time in Months
Early Resolution	6
Report not issued under 13(2)	13
Discontinued	14
Settled	16
No jurisdiction	17
Resolved	20
Not well-founded	24
Well-founded Resolved	26
Well-founded	27
Overall Average	**18.5**

Our investigation treatment times remained higher than we would like to see, although they are lower than the year before. Part of the reason we saw long treatment time averages in 2009 was that we were closing so many backlogged investigation files.

With our backlog now gone, we expect to see a dramatic decline in treatment times in 2010.