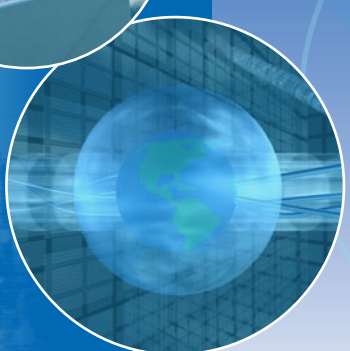
Office of the
Privacy Commissioner
of Canada

Privacy

ANNUAL REPORT TO PARLIAMENT

2008

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) 995-8210, 1-800-282-1376
Fax (613) 947-6850
TDD (613) 992-9190

Cat. No. IP51-1/2008
ISBN 978-0-662-06851-8

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

August 2009

The Honourable Noël A. Kinsella, Senator
The Speaker
The Senate of Canada
Ottawa

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, 2008.

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

August 2009

The Honourable Peter Milliken, M.P.
The Speaker
The House of Commons
Ottawa

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, 2008.

Yours sincerely,

Original signed by

Jennifer Stoddart
Privacy Commissioner of Canada

TABLE OF CONTENTS

MESSAGE FROM THE COMMISSIONER

For people who remember slipping each other notes when the teacher's back was turned, communications among young people today must seem worlds apart.

But what's striking is not that electronic missives have replaced paper, or even the variety of ways young people keep in touch. Rather, it's the apparent attitude of some young people towards privacy that seems so different – at times even *indifferent*.

Many young people are choosing to open their lives in ways their parents would have thought impossible and their grandparents unthinkable. Their lives play out on a public stage of their own design as they strive for visibility, connectedness and knowledge.

And so they text and message, blog, chat, surf and post anything that comes to hand, whether it's a picture or a video, a song, an opinion, an endorsement or even their own location.

Such openness can lead to greater creativity, literacy, networking and social engagement. But putting so much of their personal information out into the open can also expose young people to cyber-bullying or leave an enduring trail of embarrassing moments that could haunt them in future.

What's more, unguarded personal information is just low-hanging fruit for unscrupulous marketers, illegal data brokers and even identity thieves.

That is why the Office of the Privacy Commissioner of Canada is so committed to helping to safeguard personal information. In the private sector, our principal tool for this purpose is the *Personal Information Protection and Electronic Documents Act*, PIPEDA.

This annual report recounts the work of our Office, under the strong and skilful leadership of Assistant Privacy Commissioner Elizabeth Denham in overseeing the private-sector privacy law.

Through our work in inquiries and investigations, audit and review and legal services, we have sought to ensure that PIPEDA is a dynamic, modern and effective tool to strengthen the privacy rights of Canadians.

Our Office has also been busy with many other types of activities, aimed variously at raising awareness of the law among the public, Parliamentarians and businesses; providing guidance; advocating for positive change, and building effective relationships with the provinces, territories and other stakeholder groups.

And, by year's end, it was apparent that there is much to celebrate.

The sheer volume of calls and letters we receive demonstrates the extent to which Canadians recognize and cherish their right to privacy.

We are also gratified by the fact that many organizations are implementing robust privacy policies to safeguard the personal information of their customers and clients.

Even so, our mission remains incomplete.

Some organizations continue to flout the spirit, if not the letter, of PIPEDA. Personal information continues to leak from secure custody through data breaches. Many of the breaches were preventable, underscoring an urgent need for stronger policies and better employee training.

And technology, for all its indisputable benefits, continues to pose new privacy challenges – whether through novel surveillance and tracking capabilities, innovative communications applications or the modern computer's limitless capacity to collect, manipulate, store and transfer personal information.

And so, as 2009 unfolds, we are examining the impact on privacy of covert surveillance cameras, the location-mapping functions of Google Latitude, the image-capture and mapping technology of new applications such as Google Street View and Canpages, and the privacy settings and policies of social networking sites such as Facebook.

Youth are the segment of the population most likely to embrace technology, yet some seem unmoved by the impact on their privacy. Or perhaps they're just not fully aware of the potential risks.

This is why our Office made youth privacy in this fast-changing technological era a key priority in 2008. Through contests, communications materials and a dedicated new youth privacy website, we have worked hard to reach out to young people and to encourage them to reflect on the issues.

We're not suggesting the clock be turned back; we just want to ensure Canadians have the information they need to make more privacy conscious decisions.

As Canada's privacy guardian, it is our role to create awareness of privacy risks, show people how to address those risks, and make it easy for them to make informed decisions.

EXECUTIVE SUMMARY

The need for strong private-sector privacy laws has never been more acute. Advances in computer technology have enabled the accumulation, manipulation and exchange of once inconceivable amounts of personal information.

At the same time, we are seeing massive shifts in how people can use new technologies to distribute information.

Past generations have embraced a steady stream of communications technologies – the telegraph, radio and television, for example. Options for receiving information grew, but the means to distribute it were limited.

This has changed dramatically in the Web 2.0 world. Today's young people are the first generation with the ability to distribute information quickly, cheaply and to large groups of people.

They have embraced these new tools – instant messaging, social networks, texting and photo- or video-sharing sites.

As a result, we are seeing a communications revolution – and these profound changes in technologies and communication patterns are also affecting our concepts of privacy.

The challenge for our Office is to develop tools and resources to help young Canadians manage this transition while maintaining control of their identity.

A second important challenge is figuring out how to apply legislation designed for more traditional models of collection and use of personal information.

In the traditional relationship between a consumer and a bricks and mortar organization, the business directly collects personal information it requires in order to provide a service. However, with a social networking site, for example, individuals proactively put their personal information online for the purpose of sharing it with others.

Meanwhile, behavioural advertising – which we're only beginning to see – is already and will continue to be a very challenging issue for data protection authorities to address.

Deep packet inspection – an Internet traffic management tool which allows network providers to peer into the digital packets that compose a message or transmission over a network – raises all sorts of implications for us. At present, we have no evidence that Canadian ISPs are looking at the content of traffic. However, deep packet inspection offers the capacity to conduct surveillance of content.

While these new models of collection and use of information do raise challenges in applying PIPEDA, the architects of this legislation had the foresight to create a law which is technologically neutral.

In our opinion, it would be impossible to change the law every time a new technology pops up.

Overview

This report describes the activities of the Office of Privacy Commissioner of Canada in overseeing PIPEDA during 2008. As 2008 marked the fifth year since the law has been in full effect, providing us with five years of complete statistics, we include in this report some historic trends.

The work of our Office is guided by the conviction that the more businesses understand their obligations, the more effective PIPEDA will be.

And so our Office created in 2008 a Research, Education and Outreach Branch to complement the work of our Communications Branch in helping to raise public awareness of PIPEDA and the role it can play in enhancing the privacy of Canadians.

It is increasingly critical that we not work in isolation. Rapidly growing transborder data flows mean that the only way we will be able to protect Canadians' privacy rights in the future is by working with other countries to ensure adequate levels of protection for personal information around the globe.

We have been engaged in a number of initiatives at the international level, including, for example, at the Organisation for Economic Cooperation and Development (OECD) and at the Asia-Pacific Economic Cooperation (APEC) and at the International Organization for Standardization.

Our goal should be an equivalent level of basic protection around the world – one that reflects legal and cultural differences.

While there has been progress, we still have a way to go on the international front.

Another important part of our role is to oversee compliance with PIPEDA. Much of our efforts are geared toward ensuring organizations understand their obligations and are equipped to fulfill them. Toward that end, we developed information publications and guidance documents on several issues, for businesses generally as well as for specific industry sectors.

Sometimes, though, a more targeted approach was required. And so we received 422 new complaints for investigation in the private sector and prepared some 68 legal opinions for internal use over the course of the year.

Technology and Privacy

The pervasive and ever-changing nature of technology is one of the major trends influencing the work of the Office of the Privacy Commissioner of Canada.

There is, for example, a growing recognition and concern about surveillance, whether by overt security cameras or more covert means. With every innovation – global positioning systems, radio-frequency identification (RFID) tags or micro-miniature cameras – people find new ways to watch, monitor and track the activities of others.

And so, in March, the Office issued a consultation paper on the use of RFID systems in the workplace. Although the technology can improve productivity and enhance security, such surveillance can also undermine the dignity and autonomy of workers. Results of the consultation will be made public in early 2009.

In conjunction with the Information and Privacy Commissioners of Alberta and British Columbia, the Office also issued guidelines for companies installing video surveillance systems. The guidelines, for example, state that surveillance should only be considered for reasonable and appropriate purposes.

Recognizing that people's privacy is often compromised by their own online activities, our Office commissioned a research paper that explored privacy issues in massive multi-player online games such as Second Life. The paper examined the application of Canadian law to the U.S. company that operates this virtual universe.

Indeed, for the broader privacy community, the challenge is to spot real or potential risks in this era of fast-paced change and to devise ways to mitigate them. In that context, the University of Ottawa's Canadian Internet Policy and Public Interest Clinic (CIPPIC) asked us to investigate, among other things, whether Facebook, the popular

social networking site, violates PIPEDA by not informing members how their personal information is disclosed to third parties for advertising purposes.

CIPPIC also filed a complaint with us about the use of deep packet inspection technology, through which Internet service providers have the technical capability of collecting data about online users.

Our findings in both cases are expected in 2009.

Inquiries and Investigations

Our Inquiries Branch, Canadians' initial point of contact with our Office, handled 6,344 new inquiries about issues that fall under PIPEDA in 2008, an average of more than 500 per month. That's down 17 per cent from the 7,636 inquiries we received in 2007.

The Branch has had considerable success in helping complainants to help themselves by urging them to deal directly with the company to resolve concerns. With this approach, issues are usually resolved before they become formal complaints.

Even so, the Office received 422 new PIPEDA-related complaints for investigation in 2008, ending a downward trend that had lasted for several years. During 2008, we closed 412 complaints.

The challenge of reducing a mounting number of older cases was tackled head on this year. Under the leadership of the Assistant Commissioner and a new Director General, with new resources we hired investigators, launched a concerted effort to clear up the backlog of case files and devised streamlined procedures to handle cases in a way that will ensure that Canadians are well served into the future.

Data Breaches

While our last PIPEDA annual report looked back on 2007 as the year of the data breach, 2008 afforded us an opportunity to more formally explore and address the phenomenon.

We conducted an in-depth analysis of data breaches voluntarily reported to the Office between 2006 and 2008 in an effort to identify key issues leading to breaches. It pointed to inadequate system security

More detailed information about the work of our Inquiries and Investigations Branch is included on page 21. Statistical information is also provided in Appendix 2.

and employee awareness and training as some of the major issues for organizations to address.

While we continue to press for a mandatory breach notification regime, our Office continued to emphasize that organizations need solid policies and sustained and comprehensive training to lessen the chances that data are accidentally disclosed.

A new handbook for businesses reviews the 10 privacy principles underlying PIPEDA, explains how to identify, manage and report a breach, and underscores the importance of reducing the risk of future breaches.

We also created a self-assessment tool that informs organizations of their obligations under PIPEDA, and includes checklists they can use to gauge their own compliance.

Leading by Example

With five full years behind us since PIPEDA came into force for *all* organizations, the Office has had considerable experience with interpreting the law. We have also had an opportunity to reflect on its effectiveness.

In May, the Office published a report on the impact of PIPEDA. Titled *Leading by Example: Key Developments in the First Seven Years of the Personal Information Protection and Electronic Documents Act* (PIPEDA), the report highlighted some of the precedent-setting cases and issues that had helped shape the interpretation and application of the law. In particular, the report noted evolving trends such as surveillance, trans-border data flows, data breaches and the collection of personal information for secondary marketing purposes. A key aim of the report was to help businesses comply with PIPEDA as it has been interpreted.

More detailed information about the work of our Legal Services branch is included on page 45.

Reaching out to Canadians

Given the scope and urgency of today's privacy challenges, our Office believes there is a shared responsibility for safeguarding personal information. Private-sector organizations should be proactive in ensuring they meet the requirements of PIPEDA, and individuals ought to understand their privacy rights and take steps to safeguard their personal information as well.

Within this context, the Office developed guidance to help individuals protect their personal information in retail settings, and conducted public opinion polling on a variety of privacy issues.

The Office also created a Regional Outreach Program with a mandate to talk to Canadians where they live and work. Over the course of the year, members of the Office travelled from Yukon to Nova Scotia to Saskatchewan to offer guidance on the privacy issues that affect people's lives.

We now also have a full-time employee in Atlantic Canada, whose job is to talk to business leaders, lawyers, citizen groups and high school students about privacy, private-sector privacy law, and privacy for children and youth.

In 2008, the Office also announced over $400,000 in funding to support research into privacy issues such as camera surveillance and identity protection. In addition to formal research proposals, the Contributions Program also supported innovative public education, outreach and awareness-raising initiatives. Educational institutions, industry and trade associations, as well as consumer, voluntary and advocacy organizations, were invited to submit proposals for funding of up to $50,000 per project.

Reaching out to Youth

Youth were a key focus of our outreach efforts in 2008.

In conjunction with our provincial and territorial counterparts, the Office launched the youthprivacy.ca website, which offers young people advice about protecting their personal information and taking charge of how their identity is being shaped online. The site, which features a blog and an interactive quiz about privacy, was receiving an average of 3,400 hits per month by the end of its inaugural year.

An in-depth look at the issue of young people and privacy begins on page 15.

At the same time, we launched a first-ever contest to encourage students aged 12 to 18 to create videos about privacy. The winners were announced in early 2009.

Another contest launched in 2008 was aimed at undergraduate students in law schools and legal-studies programs across Canada. They were invited to write essays exploring privacy issues in our four priority areas, including information technology and identity integrity.

In June, federal, provincial and territorial Privacy Commissioners and Oversight Officials, meeting in Regina, resolved to improve the state of privacy for children and youth in the online environment. Their resolution called on governments, educators, industry and other community organizations to develop tools and information to help safeguard the privacy of young people online.

A few months later, the Office brought forward a similar resolution on the world stage. Endorsed by international data-protection authorities at a conference in Strasbourg, France, the resolution acknowledged that many young people lack the knowledge and experience to reduce their exposure to online risks, and called for a global effort to increase awareness of the need for a safe online environment for children and youth.

Reaching out to Business

In keeping with our commitment to raise awareness among organizations about their responsibilities under PIPEDA, the Office in 2008 published a booklet that explains the law to small businesses. It outlines the importance of having a comprehensive privacy policy, and to ensure, through appropriate training, that all employees understand, respect and implement all aspects of the policy.

The Office also created other products to help businesses protect the personal information of their customers. These included a self-assessment tool with an accompanying compliance guide in order to reduce the incidence of data breaches, as well as a handbook to guide businesses on responding to privacy breaches.

In collaboration with the Information and Privacy Commissioners of Alberta and British Columbia, the Office also issued two sets of guidelines: One for private-sector companies considering installing video surveillance systems, and another to advise retailers about the need to exercise caution when it comes to collecting information from consumers' driver's licences and recording the numbers.

We also consulted with various organizations – receiving 15 formal submissions – as we developed guidance on covert video surveillance which were published in 2009.

We were also working on guidance for businesses on transborder data processing in 2008. Those guidelines were published early in 2009.

Collaboration with Provinces and Territories

The year 2008 saw a marked increase in collaboration with our counterparts in B.C., Alberta and Quebec – provinces which also have private-sector privacy legislation. In the spring, our Office issued a Statement of Intent, spelling out how we would work with provincial and territorial commissioners and ombudsmen on privacy matters.

The document, for instance, outlined our commitment to consult with provincial and territorial offices in certain priority areas, such as proposed federal legislation with major implications for the collection, use or disclosure of personal information within a

province or territory.

Under this umbrella, we developed a Memorandum of Understanding with B.C. and Alberta to address how the Commissioners with shared jurisdiction over the private sector will work together.

We were also working more closely with the provinces and territories on several other fronts, such as education, compliance, policy matters and enforcement.

In enforcement, for example, businesses and individuals benefit from consistent application of the law. Working together yields practical benefits as well, such as efficient and effective use of resources between the offices.

This was illustrated by the case of Ticketmaster Canada Ltd., a parallel investigation involving our office and the Alberta Office of the Information and Privacy Commissioner. Our close collaboration ensured a consistent approach to many of the findings and recommendations. (See page 30 for more information.)

The Year Ahead

As this annual report goes to print, we can look forward to new challenges and opportunities ahead.

As an Office, we will continue our efforts to improve our processes to resolve or investigate complaints, with a new case-management system and the elimination of a still too large backlog of cases.

We will continue to monitor developments on the legislative front and in the world around us to determine their impact on privacy. And we will continue to build on what we have learned as we tackle important, complex, and sometimes controversial issues.

We will also remain focused on our four strategic priorities - information technology, identity integrity, national security issues related to privacy and genetic privacy.

What's more, we will continue to reach out to Canadians – individuals, industry and advocacy groups to ensure that privacy is a respected value.

PRIVACY BY THE NUMBERS

Office of the Privacy Commissioner of Canada in 2008

PIPEDA inquiries received	6,344
PIPEDA complaints received	422
PIPEDA investigations closed	412
Legal opinions prepared under PIPEDA	68
Draft bills and legislation reviewed for privacy implications	7
Private-sector policies or initiatives reviewed	24
Policy guidance documents issued	16
Research papers issued	22
Parliamentary committee appearances made	4
Other interactions held with Parliamentarians or staff	79
Speeches and presentations delivered	86
Formal visits from external stakeholders received	53
Contribution agreements signed	10
Research contracts signed	7
Hits to Office website logged	1,422,068
Hits to Office blog logged	282,905
Total:	1,704,973
Publications distributed	8,951
Media interviews provided	282
News releases and fact sheets issued	35
Access to Information Act requests received	26
Access to Information Act requests closed	25

KEY ISSUE: YOUTH PRIVACY

Changes in technologies and communication patterns are affecting how young Canadians develop as individuals and as members of society at large. The Office of the Privacy Commissioner of Canada is developing innovative tools and resources to help young Canadians manage this transition while maintaining control of their identity.

As Canadians, we have learned, generation after generation, to integrate new technology into our lives. We have welcomed the seemingly endless discovery of faster and more powerful media, which have delivered more information, in more detail, into more hands across Canada and around the world.

In the past, innovations such as the telegraph, the telephone and the television changed how Canadians received information from organizations. Today, the invention of the personal computer, the introduction of e-mail and widespread access to highspeed Internet service have signaled a fundamental shift in how information is collected, communicated and shared among individuals, communities, businesses and governments.

Thanks to the development of Internet-based applications, the youth of today are the first generation to have access to tools that allow them to distribute information quickly, cheaply and to large groups of people.

These tools have many functions – instant messaging, social networks, texting, and photo- or video-sharing sites – and are offered under many brand names. Young Canadians can now readily share their personal experiences and their personal information with close friends, classmates, family and larger groups in the community or around the world. Emboldened, some young Canadians have rallied around social and economic issues, broadcast personal or political opinions, and joined activist movements.

The relationship between Canadian consumers and businesses is also changing. Mass media, such as television and newspapers, have seen their markets fragment as Canadians discover they can pick and choose from countless sources of information. Businesses and their marketers must now work harder to find their target market, let alone capture their attention for long enough to close a sale.

This targeting can now be based on demographic data, past purchasing histories, product and attribute preferences identified through market research, or by tracking behaviour online.

Businesses are looking for more opportunities to interact with consumers of all ages in order to accumulate and analyze the information essential to their continuing success. In Canada, the boundaries between the reasonable collection of market intelligence and intrusion into private life are still being established.

As a result, this youngest generation of Canadians has the means to wield more influence and make a greater impact within society than any that preceded it.

"IS MY DAD EVER GOING TO LAUGH WHEN HE SEES HIMSELF ON YOUTUBE!"

To paraphrase the *Cluetrain Manifesto*, a ground-breaking analysis of how relationships and identity have developed online, the conversations generated by young Canadians may appear confused and may sound confusing. Still, they have better tools, more new ideas, and no steadfast rules to slow them down.[1]

This constantly changing environment presents a tremendous challenge for a generation already struggling to understand their environment, identify their own personal qualities and preferences, and shape their own identity.

They are still undergoing the same formative experiences as their predecessors – friends, classmates, community groups and social norms still influence the shaping of their identities. But today, all those influences are more closely bound, thanks to these new tools.

Meanwhile, young Canadians are trying to develop the social skills and cognitive abilities to measure and manage how they interact with society at large. Their growth into adulthood, if anything, may be accelerated by the arrival of these new tools.

---

1 The Cluetrain Manifesto: The End of Business as Usual, Levine, Locke, Searls & Weinberger, accessed on 20 April 2009 at: http://www.cluetrain.com/book/95-theses.html

Noted sociologist and researcher danah boyd has observed that "most teens are engaging with social media without any deep understanding of the underlying dynamics or structure. Just because they understand how to use the technology doesn't mean that they understand the information ecology that surrounds it. Most teens don't have the scaffolding for thinking about their information practices."[2]

This is an important point for the Office of the Privacy Commissioner. Increasing numbers of young Canadians are actively connecting with their friends in the online world, but may not have the time, resources or inclination to consider the impact of how they are sharing information, opinion or gossip.

This is not a caution against using new technologies or integrating new tools into everyday activities. After all, these tools are so prevalent across all media channels that they are now a fact of life, for young and old.

Rather, it is recognition that this generation of Canadians needs help to begin developing appropriate information-management practices – ways to ensure their personal information is collected by organizations only with their permission, distributed only according to their wishes, and used only in ways to which they agree.

In practical terms, young Canadians see their personal information as just one component of their individual identity. That identity finds expression through their interaction with groups of friends or classmates.

Leslie Regan Shade, a professor at Montreal's Concordia University, has noted that when youth express concern about their personal information and privacy, it is within the context of their relationships: They want to control their image, and how they appear to their peers and others.[3]

Research conducted by Ryerson University in Toronto under the auspices of the Office's Contributions Program confirmed this observation, revealing that university students' "expectation of privacy is shaped, not by their sense of autonomy, but by their sense of reputation and dignity, and when they perceive that their privacy is being threatened, it is really their reputation, dignity, persona or online identity that is at stake ..."[4]

---

2 danah boyd, "Living and Learning with Social Media," presented at the Symposium for Teaching and Learning with Technology, Penn State, 18 April 2009, accessed on 20 April 2009 at: http://www.danah.org/talks/pennstate2009.html

3 Notes from 2007 International Conference of Data Protection and Privacy Commissioners, session reference: http://www.privacyconference2007.gc.ca/workbooks/Terra_Incognita_workbook10_E.html

4 The Next Digital Divide: Online Social Network Privacy, Accessed on 20 April 2009 at:

The generation of Canadians that has grown up with easily accessible computing power and always-on Internet access is just beginning to experience the repercussions of living their lives online.

Students have been disciplined by their universities for their use of online social networks to share homework. Young Canadians have been shown the door after their employers discovered indiscrete comments or inappropriate photos taken in the workplace posted on their online social network profiles.

In effect, young Canadians are learning through trial and error to manage how their personal identity is presented and perceived.

The challenge for the Office is to develop tools and information resources that support this natural learning process and encourage privacy-positive behaviour by both consumers and businesses.

Investigations conducted under PIPEDA continue to provide solid examples of how information-management principles should be applied to situations of interest to young Canadians. For example, in 2008, we launched investigations into complaints of impersonation on a social network, as well as a much-publicized complaint about the privacy practices of Facebook, a leading social networking site.

We have also been working with our counterparts in the United States and Europe to understand the privacy implications of increased data collection, data mining and behavioral advertising. This work will eventually help inform and guide young Canadians as they interact with businesses online and offline.

The Office introduced joint resolutions calling for better tools, resources and legislation to safeguard youth privacy, first at a meeting of federal, provincial and territorial privacy

http://www.ryerson.ca/tedrogersschool/privacy/Ryerson_Privacy_Institute_OSN_Report.pdf

commissioners and ombudspersons in Victoria in February 2008, and then again in October at the International Conference of Data Protection and Privacy Commissioners in Strasbourg, France.

Over the past year we have also expanded our public education activities, launching tools and resources useful to young Canadians ranging in age from six to 25.

Anchoring this effort is youthprivacy.ca, a dedicated resource for young Canadians, their parents and teachers. This standalone website features practical guidance on how to discuss privacy issues with young Canadians, an interactive and easily updated Privacy Quiz, a youth-oriented blog, and the winning videos submitted as part of our 2008 Youth Privacy Video contest.

The Office continues to work with academics and not-for-profit organizations to develop age-specific material on youth privacy. We commissioned the Media Awareness Network (MNet) to develop modules that can easily be integrated into lesson plans and curricula for students in Grades 7 and 8 and 9 to 12.[5] They also received funds under the Office's Contributions Program to update their well-received "Kids for Sale: Online Privacy and Marketing" awareness program.[6]

In the coming year, we will identify activities to be launched in partnership with other organizations that work directly with youth, especially in areas such as entrepreneurship, financial literacy, consumer affairs and civil society.

We continue to draw inspiration for these public education activities from the work of our colleagues in the provincial privacy offices in Ontario, Alberta, Manitoba and Quebec, as well as initiatives launched by data protection offices in the United Kingdom, Sweden, Hong Kong, Ireland, Spain and Australia. We continue to explore opportunities to co-operate on future public education initiatives.

5 http://youthprivacy.ca/en/teachers.html

6 http://www.media-awareness.ca/english/teachers/wa_teachers/kids_for_sale_teachers/index.cfm and http://www.media-awareness.ca/english/parents/internet/kids_for_sale_parents/

RESPONDING TO CANADIANS: COMPLAINT INVESTIGATIONS AND INQUIRIES

For our Investigation and Inquiries Branch, 2008 was a year of challenges and transition.

We explored issues at the very frontiers of privacy laws. Indeed, technologies such as deep packet inspection and new social networking applications were uncharted territory for privacy authorities, and working on findings that would stand the test of time sometimes felt like driving a stake into quicksand.

Still, we were addressing some important cases that will continue to touch the lives of Canadians for years to come.

As described in greater detail later in this chapter, we witnessed the pervasive impact of technology on privacy, identity management issues, and the collection of excessive amounts of personal information.

Inquiries

Our inquiries unit is our "front office" – our initial point of contact with Canadians. We received 6,344 new inquiries under PIPEDA in 2008, an average of more than 500 per month. That's down about 17 per cent from the 7,636 inquiries we received in 2007.

Imposters Stalk Cyberspace

Online imposters, it seems, don't just stalk the rich and famous.

In a case investigated during 2008, an individual used the name, personal information and photo of a regular family man with two daughters to create a phony account on a social networking site.

Pretending to be the father, the conman went on to dupe the girls into becoming his "friends," thus gaining access to their personal information.

He soon began harassing the daughters with threatening and obscene postings and e-mails. The victims quickly recognized they'd been tricked, and got the social networking site to delete the offending account.

The incident, however, helps to remind people to learn all they can about the privacy controls available on social networking sites. The controls won't stop imposters, but they can reduce their access to the personal information of their victims.

We have noticed some common concerns centred on the perceived misuse of social insurance numbers and the loss or theft of personal information leading to potential identity theft. People also came to us with concerns that they could not gain access to their personal information held by organizations, or that it took too long to do so. We also received many calls about an insurance industry practice of offering lower premiums in exchange for a credit check.

Privacy Protections Dwindling: Poll

Public opinion research conducted for our Office in early 2009 found that only 12 per cent of the 2,028 respondents felt that businesses take their obligation to protect the personal information of consumers "very seriously."

What's more, nearly nine of 10 (87 per cent) were concerned that toughening economic times are leading businesses to cut spending on measures to protect personal information. Indeed, six in 10 felt their personal information was less well protected than a decade ago.

EKOS Research Associates Inc., March 2009

About 83 per cent of all inquiries last year came to us by telephone and the rest by fax or mail. This may be because we have widely publicized our telephone numbers and have advised Canadians that we do not accept complaints or inquiries submitted by e-mail.

In all, we closed 6,234 PIPEDA inquiries in 2008.

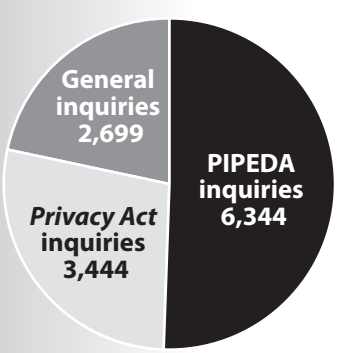
PIPEDA inquiries represented roughly half (51 per cent) of all of the inquiries received over the year. *Privacy Act* inquiries accounted for 27 per cent and general inquiries approximately 22 per cent.

One of the approaches we have been stressing over the past year is to help people help themselves. When individuals come to us with an issue, we encourage them to deal directly with the organizations first, and we help them determine the best way to do that. For example, we maintain a database of contact

Inquiries Statistics
January 1 to December 31, 2008

PIPEDA inquiries received	
Telephone inquiries	5,280
Written inquiries (letter and fax)	1,064
Total	6,344
PIPEDA inquiries closed	
Telephone inquiries	5,281
Written inquiries (letter and fax)	953
Total	6,234

Inquiries of all types received in 2008



information for Chief Privacy Officers of many organizations.

This provides organizations the opportunity to resolve their customers' concerns before we become formally involved. With this approach, issues are usually resolved quickly and do not needlessly become formal complaints.

Complaints

We received 422 new PIPEDA-related complaints for investigation in 2008, ending a downward trend that had lasted for several years. In 2007, there had been 350 complaints, fewer than half the 723 we logged in 2004.

Given our accumulated backlog, however, our workload remains as challenging as ever.

More than six in 10 of the 2008 complaints we received related to the collection, use or disclosure of personal information by companies covered by PIPEDA.

During 2008, we closed 412 complaints, down from 420 the year before.

There are no startling trends in the kinds of complaints that come our way, but certain patterns have emerged with some consistency over the past five years.

For example, although there has been a marked decline in the number of complaints levelled against banks (from 145 in 2004 to 40 in 2008), financial institutions as a whole tend to attract the

Does data matching create personal information?

In one investigation that wrapped up in 2008, we considered whether layering publicly available information about neighbourhoods over personal information about individuals that is publicly available in phone books creates a new type of personal information that is entitled to protection under PIPEDA.

The complaint was lodged against a company that combined anonymized geographic and demographic data from Statistics Canada with White Pages information, such as names and addresses, to create lists that could be sold to direct marketers and other clients.

The complainant argued that the newly created consumer lists constituted personal information, which means that people should have to provide consent for their information to be included and sold on such lists.

The Assistant Commissioner disagreed. She concluded that all the information compiled in the consumer lists came from public sources, and sorting it according to geographic and demographic criteria did not change the publicly available personal information into non-publicly available personal information requiring consent.

Because no information about identifiable individuals was created, no consent was required for its commercial use, the Assistant Commissioner said. However, she also noted that the finding in this instance may not apply to all data-matching processes.

lion's share of complaints. In fact, between 22 and 30 per cent of all the complaints that we investigate annually are levelled against that industry, which also includes collection agencies, credit grantors and financial advisers.

One explanation is the sheer volume of transactions handled by financial institutions on any given day, each involving highly sensitive personal information. Canadians are justifiably concerned that this information be secure, particularly given its value to fraudsters and thieves.

In past years, the telecommunications sector has come in a distant second place, with about half as many complaints as the financial industry, followed closely by sales. Again, the relative volumes of transactions that occur in these sectors suggest the likeliest explanation for the trends.

In 2008, the insurance industry took second place, yielding 71 complaints, or 17 per cent of the total. Most related either to difficulties that complainants had in gaining access to their personal information in the industry's possession, or issues related to the use and disclosure of the information.

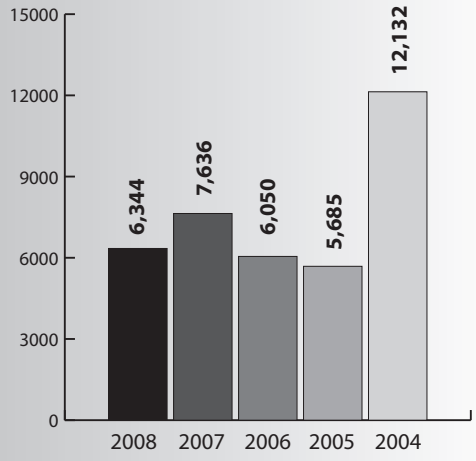
The reason for this spike is not yet apparent, and we do not know whether it will continue in the future. We have noticed, however, that complainants are using PIPEDA in claims disputes with their insurance providers, which is a legitimate and parallel use of the law.

Some complaints have also centred on techniques that insurance adjusters use to evaluate or substantiate claims.

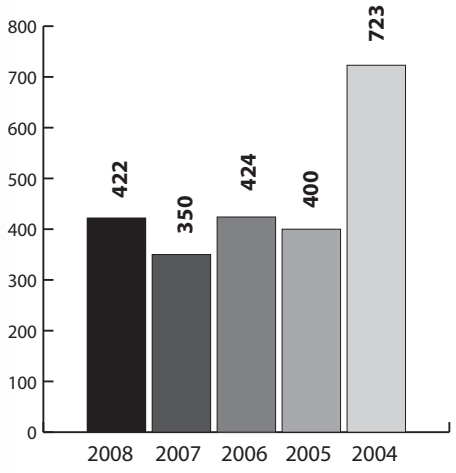
One of those techniques is covert video surveillance - which normally involves a private investigator following a targeted individual and capturing his or her image. By the fall of 2008, having received several complaints about the practice, our Office felt it could be helpful to industry to develop guidelines. We launched a consultation process on the basis of draft guidelines posted on our website. We received submissions from 15 stakeholders, representing the insurance industry, private investigators, unions and employers. Final guidelines were published in 2009.

Our Office is keen to continue working with industry associations to address some of the issues we've seen in our investigations.

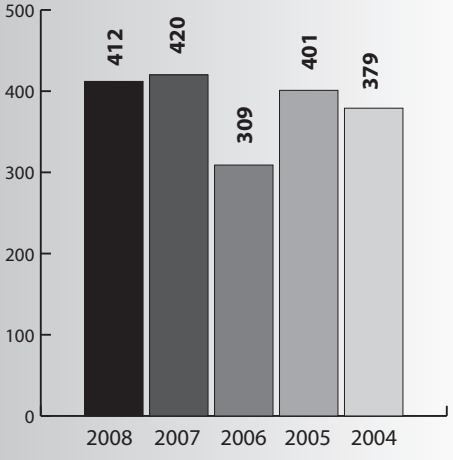
PIPEDA – Five-Year Overview



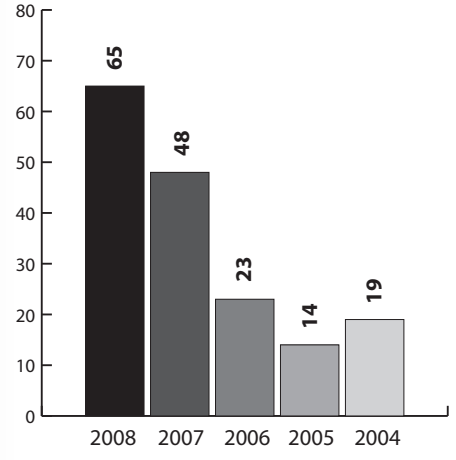
Inquiries received



Complaints received



Complaints closed



Data breaches reported

PIPEDA - Five-Year Overview

Complaints Received by Industry Sector *

Sector Category	2008	2007	2006	2005	2004
Financial institutions	93	105	108	113	212
Insurance	71	35	51	60	82
Sales	63	37	58	44	82
Telecommunications	63	42	55	55	125
Transportation	38	28	37	39	67
Professionals	33	26	11	13	15
Services	21	6	7	2	10
Accommodation	15	21	29	17	18
Other	10	39	56	52	76
Health	9	9	7	4	36
Rental	6	2	5	1	0

* Definitions of industry sector categories are provided on page 27.

Complaints Received by Complaint Type *

Complaint Type	2008	2007	2006	2005	2004
Use and disclosure	162	120	153	143	286
Collection	93	68	75	68	172
Access	73	67	84	80	112
Safeguards	30	36	34	34	40
Consent	24	16	13	21	37
Time limits	11	13	17	18	9
Accountability	8	8	11	10	9
Accuracy	8	7	11	5	22
Correction/ Notation	5	3	8	5	11
Openness	3	4	1	8	2
Challenging Compliance	2	0	3	1	1
Other	2	0	0	1	4
Fee	1	1	3	3	12
Retention	0	7	11	3	6

* For definitions of terms used, please see Appendix 1.

Breakdown by Industry Sector
Complaints received between January 1 and December 31, 2008

	Count	Percentage
Financial Institutions	93	22
Insurance	71	17
Sales	63	15
Telecommunications	63	15
Transportation	38	9
Professionals	33	8
Services	21	5
Accommodation	15	4
Other	10	2
Health	9	2
Rental	6	1
Total	**422**	

Industry Sector Categories

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

Insurance: Life and health insurance, property and casualty insurance

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

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

Transportation: Air, land, rail, water

Professionals: Accountants, lawyers

Services: Daycare, hairdressers, beauticians

Accommodation: Hotels, landlords, condominiums, property management

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

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

Rental: Car rental, other rental

Complaints about Technology

Technology can be liberating or enslaving, comforting or vexing. For most people, though, it's a pervasive fact of life.

And so it is not surprising that many of our investigations explored some aspect of technology and its impact on privacy and the security of personal information.

One investigation, for example, examined Canwest Publishing Inc.'s outsourcing of its Canada.com e-mail services to a U.S. company. Our investigation found that Canwest had complied with its obligations under PIPEDA because new and existing Canadian e-mail subscribers were adequately informed of the company's intent to transfer their data abroad and had the opportunity to accept or reject the terms of the services.

However, we also noted that, once transferred, the data would be subject to U.S. laws, which could compel the American company to disclose information in its possession to U.S. authorities. We recommended that organizations be transparent about all facets of their personal information handling practices.

The chance that personal information can be lost in a data breach has always existed, but technology has made it easier to collect, store – and occasionally lose – personal information. Because computer memory is so inexpensive and plentiful, technology has also increased the likelihood that data spills, when they occur, are spectacular in scope. Cases on that issue are discussed later in this chapter.

The Canadian Internet Policy and Public Interest Clinic (CIPPIC), based at the University of Ottawa, brought forward two technology-related cases that commanded our attention in 2008.

In one instance, CIPPIC asked us to investigate whether Facebook, the popular social networking site, violates PIPEDA by, among other things, not informing members how their personal information is disclosed to third parties for advertising purposes.

CIPPIC also asked us to examine the practices related to deep packet inspection, through which Internet service providers have the technical capability of collecting data about online users.

Deep packet inspection has been used for several years 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 information sent from one end user to another.

The technology has the potential to give Internet service providers and other organizations widespread access to vast amounts of personal information sent over the Internet for:

- Targeted advertising based on users' behaviour while online;
- Scanning network traffic for undesirable or unlawful content, such as unlicensed distribution of copyright material or dissemination of hateful or obscene materials;
- Capturing and recording packets as part of surveillance for national security and other crime investigation purposes; and
- Monitoring traffic to measure network performance, and plan for future facilities investments.

Our findings in both the Facebook and deep packet inspection cases are expected in 2009.

Complaints about Identity Management

An issue that has preoccupied our Office for some time is the unfettered use of photographic identification for purposes other than what it was intended for. For instance, we often receive complaints about retailers asking customers to provide their driver's licences when they are returning merchandize without a receipt.

A driver's licence contains a great deal of personal information, including the licensee's name, photograph, age, address and gender. Because such information is of great value to fraudsters, a driver's licence should mainly be used by law enforcement officials to confirm that the holder is permitted to drive.

In 2008, we investigated a major home-decorating chain that was recording and retaining the driver's licence information of some customers. We recommended that the organization drop this practice for good, and delete any photo identification numbers stored in its databases. The company agreed to our recommendations and, by November, had wiped its records clean.

Things did not, however, go as well in another case, involving a major video-rental chain. In response to a previous complaint investigation by our Office, the company had agreed to stop collecting the driver's licence information of its customers. In 2008, however, they resumed the practice, prompting our Commissioner to use her powers to initiate an investigation. We will complete this investigation in 2009.

Because the misuse of photo identification had become such a widespread problem, our Office worked with counterparts in Alberta and British Columbia to develop a guidance document to inform retailers about viable alternatives to the collection of driver's licence information.

Other Noteworthy 2008 Cases

Ticketmaster Canada Ltd.

In April 2008, the Privacy Commissioner and the Information and Privacy Commissioner of Alberta concluded parallel investigations into the information-collection and disclosure practices of Ticketmaster Canada Ltd., a major online ticket vendor.

We discovered the company's published privacy policy to be long and difficult to understand. Moreover, online customers had to agree to allow their personal information to be used for marketing purposes as a condition of buying a ticket, a clear violation of PIPEDA.

The concerns uncovered in the investigation were resolved in Canada. Ticketmaster agreed to provide customers with a choice of whether to opt in to receiving marketing material from Ticketmaster and event providers. On-line customers are fully informed and given the opportunity to opt in to receiving marketing material from the event provider by checking off a box before the ticket payment is remitted.

However, Ticketmaster in the United States did not give their customers the option of declining marketing materials.

Law School Admission Council

In May, we published findings of our investigation into a complaint from a person who objected to the requirement that students enrolled at Canadian universities be fingerprinted in order to be permitted to sit the Law School Admission Test (LSAT).

The U.S.-based Law School Admission Council, which developed the test, said the thumb prints are collected to guard against frauds in which professionals are paid to take the test for somebody else.

Our Office upheld the complaint on the grounds that fingerprinting did not effectively meet the stated purpose of deterring imposters. Compared to the difficulty of matching

thumbprints scientifically, there is an increased ease with which photographs may be visually matched to a test taker or to a publicly available image of a test taker. This might result in an improved ability to identify and catch cheaters after the fact, thus enhancing the deterrent effect. In any case, the prints were never actually used for the intended purpose. We concluded that the loss of privacy exceeded any benefit gained.

The Council agreed to drop the thumb print requirement in Canada, although it said it would start collecting photographs of test takers instead. We concluded that collecting photographs is less privacy intrusive and, in this case, did not contravene PIPEDA.

Canad Corporation of Manitoba Ltd. (Canad Inns)

This matter involved 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.

A woman filed a complaint with our Office against the Canad Corporation of Manitoba Ltd., charging that, as a patron of one of the organization's Canad Inns hotel bars, her personal information had been improperly collected.

Our investigation revealed that the bar had placed her driver's licence into a machine that photocopied and then retained the information on her card.

In a preliminary report, the Assistant Privacy Commissioner found that the identification machines were holding more information than was necessary to achieve Canad Inns' stated purposes of verifying the age of patrons and ensuring security. The report recommended that Canad Inns stop collecting and retaining personal information in this manner, and remove the personal information of customers 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.

In early 2009, court-ordered mediation was prescribed in this case, but the case itself remained before the Federal Court. Canad Inns was given time to determine feasible means to limit the personal information it collects. The company was to submit affidavits outlining its proposed efforts. Our Office will then examine its proposals and file for a case management conference to determine future steps in the proceedings.

Data Breaches

Last year's PIPEDA annual report dubbed 2007 the year of the data breach. This year, we can report on a number of initiatives our Office undertook in 2008 to help curb this serious problem.

A data breach means an incident involving loss of, unauthorized access to, or disclosure of personal information as a result of a breach of an organization's security safeguards. It can involve a single customer, or thousands, as when entire computer disks are lost or stolen.

But no matter what the scope of the incident, the consequences can be dire. Personal information that falls into the wrong hands can be misused in any number of ways, from fraudulent credit card purchases to identity theft and criminal impersonation.

Data can be spilled by accidental or deliberate means.

Our Office analyzed private-sector data breach incidents reported to us between 2006 and 2008. We found that the number of reported incidents had more than doubled, from 23 in 2006 to 48 in 2007, the year in which the Office published a privacy breach checklist for businesses. In 2008, there were 65 incidents.

Banking on Staff Training

In December 2006, an employee of CIBC in Montreal couriered off a parcel to the bank's computing centre in Markham, Ont. The package was supposed to contain a portable computer disk drive holding the files of 470,752 clients of a CIBC subsidiary, Talvest Mutual Funds.

The parcel arrived two days later but was empty. To this day, the drive has never been found, and no one is sure what, if anything, happened to the data.

The incident spurred the Commissioner to launch an investigation into such issues as data encryption, technical accountability and supervision in data transfer, and breach notification processes at the CIBC.

In findings issued in November 2008, the Assistant Commissioner concluded that, while robust corporate privacy policies are essential, they must also be backed up by ongoing staff training.

One of the key reasons our Office has been urging organizations to report breaches to us is so that we can develop a better understanding of why spills are occurring and how they can be prevented in the future.

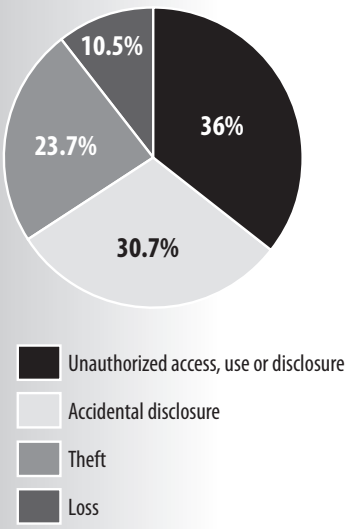
Our analysis focused on 114 data breaches where we had closed the file. (Ongoing investigations were not included in the analysis.)

We categorized the breaches into four different types: unauthorized access, use or disclosure; accidental disclosure; theft; and loss.

Unauthorized access, use or disclosure

We found that unauthorized access, use or disclosure was the most common type of incident – accounting for 36 per cent of total data breaches reported. Unauthorized access, use, or disclosure occurs when someone without authority to do so accesses, uses, and/or discloses personal information (usually for nefarious purposes). And, in more than three-quarters of these cases, the culprit was a rogue employee of either the organization that suffered the breach or a third-party service provider. Fraud was the motive in most of these cases.

Reported Data Breaches – by Type



Accidental Disclosure

The second most common type of incident was accidental disclosure – the key factor in more than 30 per cent of cases. This group of incidents included:

- Mailing foul-ups (40 per cent of accidental disclosures);
- Improper destruction and disposal (20 per cent);
- Online disclosure (14 per cent);
- E-mailing mistakes (11 per cent); and
- Errant faxing (nine per cent).

Human error, mainly on the part of employees, led to the vast majority of these problems. We found that human error was the primary cause of more than 85 per cent of accidental disclosures. Other causes of accidental disclosure included mechanical and technological errors.

Theft and Loss

Our analysis showed that theft was the third most common type of incident, figuring in just under a quarter of incidents. Documents and electronic devices containing personal information were principally stolen from vehicles (41 per cent of cases); from offices or stores (30 per cent) and from courier mailbags (19 per cent).

Loss of personal information accounted for another 10 per cent of breaches. This type of incident included paper documents such as credit card applications and bank

transactional information going missing. Personal information was also put at risk when portable electronic devices such as disk drives and memory sticks were lost.

Our analysis also examined the issues behind all of these types of breach incidents. In many cases, there were multiple factors that led to the breach.

The analysis showed there are several issues that organizations could be addressing more effectively to prevent breaches.

The most common issue was poor system security (46 per cent), followed closely by inadequate employee training (45 per cent).

We see too many organizations underestimating security risks and the need to protect personal information. As well, technologies are constantly changing and it is critical for organizations to ensure their security systems remain up to the task of safeguarding personal data.

In many cases, training of employees is inadequate – despite the fact that this is such an important part of having a robust system to protect personal information. A 2007 OPC poll found that only a third of all businesses reported having trained staff about the practices and responsibilities under Canada's privacy laws, although it was much more pronounced among larger businesses.

Wiping the Slate Clean

Data breaches don't need to be dramatic in order to be traumatic. And nowhere is this more evident than in the reselling of technology.

In a typical scenario, a person buys a mobile communications device, and enters some contact names and other personal information. The device, however, proves unsuitable and is later returned.

Although the device's memory is supposed to be wiped clean, we have investigated many cases where this process failed or was incomplete. The device was then sold to another customer, compromising the privacy of the original purchaser.

Our investigations have found that all sorts of equipment, from phones and computers to printers and cameras, contain memory that must be purged before resale. Retailers and manufacturers share a duty to ensure this is done properly.

Another significant issue identified in our analysis was deliberate employee misbehaviour. One way to reduce this risk is by ensuring that personal information is accessible only on a "need to know" basis.

Other issues for organizations to consider in their efforts to decrease the threat of data breaches include: administrative procedures, including destruction and disposal practices; third-party service providers and their capacity to protect personal information; and security and procedures related to employees taking data out of the office.

Issues Leading to Breaches

System Security - Inadequate – or absent – security systems were the privacy issue that most commonly surfaced in incidents reported to our Office. (46 per cent of closed incident cases.)

Employee Awareness/ Training – A lack of employee knowledge about how to protect the privacy of customers was a factor in 45 per cent of cases.

Employee Misbehaviour - Rogue employees, most often involved in fraudulent activities, were the culprits in close to a third of the incidents (31 per cent). This figure includes both employees of the organizations that suffered the breach and third-party service providers or processors.

Administrative Procedures – Shortcomings related to administrative procedures such as mailing, e-mailing, faxing and database maintenance were at fault in 31 per cent of cases.

Third-party Service Providers – Almost 30 per cent of the time, the breach occurred while personal information was in the custody of a third-party service provider or processor.

Employees Leaving the Office with Data - Security and procedures related to employees taking data out of the office – for example, to do work at home or while travelling – were factors in 18 per cent of incidents.

Disposal/ Destruction Procedures – Getting rid of personal information in a secure manner remains a challenge for some organizations. Disposal and destruction procedures were a factor in eight per cent of incidents.

NOTE: In many instances, we found there were multiple issues which led to the breach of personal information.

While our Office continues to advocate for mandatory breach notification laws, we have been working to raise awareness among industry about the need for robust internal policies and employee training to lessen the chances of data spills.

In 2008, our Office issued new breach tools for business.

We also took steps to make it easier for companies to notify us proactively about an actual or suspected breach. In particular, we created an online breach notification form for our website. We also centralized the reporting point within the Office. This person aids in breach-related investigations, and tracks and reports on data-spill incidents.

Our analysis showed that the proportion of breaches that we monitored and were reported by the organizations themselves – versus those coming to our attention in other ways such as media reports – rose from 75 per cent in 2006 to nearly 90 per cent in 2008.

At the same time, organizations notified all the people affected by the data spills in three-quarters of the cases, and notified some affected individuals in another nine per cent.

Becoming More Efficient

The complaints we receive are becoming increasingly complex and require extensive investigation. Over time, our complaints-handling processes became overwhelmed and treatment times for complaints were getting longer.

On average in 2008 it was taking nearly 20 months for a case to be closed, whether that meant it was discontinued, resolved, settled or became the subject of reported findings. That was up by nearly one-third from the previous year. Our backlog grew to an unacceptable level.

To tackle this challenge, we opted for a proactive, multi-pronged approach that included drafting guidance documents, outreach to business organizations and a wholesale re-engineering of our case-management processes.

By the end of the year, we were making gratifying progress and our case backlog of complaints over a year old had begun to decrease.

Proactive Approach

In addressing our workload issues, it was apparent that a big part of the solution would be to solve problems before they turned into complaints. Toward that end, our Office has been more actively engaged in outreach.

We are talking to industry, business and professional organizations across Canada to ensure they fully understand and abide by their obligations under PIPEDA. Over the year, we also published several information and guidance documents that explained the law, as well as what to do in the event of a data breach.

We were also reaching out to Canadians with a new online complaint form that has simplified the filing process, while giving us more complete and standardized information from which to launch our investigation.

And we have strengthened our ties with provincial and territorial privacy offices because we recognize we have much to learn from each other. In February 2008, for instance, we hosted our annual investigators conference in Ottawa, bringing together Information and Privacy investigators from across Canada. The two-day conference allowed investigators and inquiries officers to make new contacts, share experiences and exchange best practices.

In the shadow of our growing case backlog, we recognized the urgent need to re-engineer our internal processes in order to cope with the workload.

The effort, which was designed in 2008 but is being rolled out over 2009, has several components, including more hands on the job, a concerted effort to eliminate the backlog of unfinished business, and some new complaint-handling processes, backed by an improved computerized case-management system. These initiatives are described below.

More Human Resources

A new and experienced Director General joined the Investigations and Inquiries branch in August 2008 and provided continued leadership for the re-engineering process.

Ten new investigators were hired to join the four already working on PIPEDA files. These new investigators took part in a newly created intensive two-month training program at the beginning of 2009. We also hired four new inquiries officers.

A shortage of investigators has been a significant challenge for our Office. We lost a number of experienced PIPEDA investigators over the last three years and they have been difficult to replace. Many organizations are vying for a small pool of access and privacy professionals, making recruitment and retention difficult.

At times during 2008, we were operating with only four experienced PIPEDA investigators with very large caseloads.

In the absence of trained investigators, consultants and lawyers were retained to deal with files. And, in a pilot project, a contract investigator was engaged in Calgary to handle certain files with a Western focus, particularly if there was shared interest by the Office of the Information and Privacy Commissioner of Alberta. While helping to address an acute personnel shortage, this decentralization exercise also enabled the Branch to perfect strategies for secure and effective tele-working.

The Backlog Blitz

In June, we changed the definition of when a file is in backlog to more accurately reflect how long a complainant was actually waiting for service. In the past, we considered a file to be backlogged if it could not be assigned to an investigator. Under our new definition, a file is considered to be in backlog if more than a year has passed since the date of receipt. With this change in definition, the 96 files in "backlog" in May ballooned to 361 in June.

The new number, though higher, reflects levels of service to Canadians more accurately.

With a comprehensive re-engineering process already underway as described below, we also launched in June a 16-part "backlog blitz" to try to shrink the numbers in an orderly fashion.

For example, we grouped cases that shared similarities in terms of the industry sector involved, the complaint subject or the respondent organization, and dealt with them together. We also shortened the chain of command for signoff on cases. And we committed to dealing with cases in the backlog before tackling any new ones.

By the end of the year, even as new cases continued to arrive at a rate of about 32 per month, we had managed to whittle the backlog down by 14.3 per cent, to 312 cases. We are on track to eliminate it as soon as possible..

Re-engineered Processes

We have long recognized that we needed to retool our processes in order to keep on top of the thousands of complaints and inquiries we expect to continue to receive in the years ahead.

Toward that end, we are re-engineering our inquiries and complaint-handling processes in order to make them more streamlined and efficient. The retooled processes will be supported by a new computerized case-management system. The case management system was implemented for our inquiries work in 2008 and will be rolled out for investigations in 2009.

The re-engineering initiative is being implemented in phases, and we expect it will be fully operational by fall 2009.

A key first step in the re-engineered process will be a robust "refer-back" protocol, under which people who contact us with an inquiry or a complaint are encouraged to speak first with the company with which they have an issue. The company can often resolve

the issue quickly, which is good for all parties. Businesses have, in fact, told us they appreciate a first crack at addressing customer concerns. As is already our practice, we will continue to offer complainants help in contacting companies.

Where direct talk doesn't resolve the issue and a complaint is made to our Office, we want to ensure it is handled efficiently and in a manner satisfactory to all.

Our new online complaint form will help ensure that all the key information is provided, which in turn allows us to assess the complaint more efficiently.

Under our re-engineered procedures, a complaint will be channelled first to our newly created position of Complaints Registrar. On the basis of the nature, complexity or urgency of the issue, the registrar will decide how the complaint will be handled.

Although some cases may be assigned directly to an investigator, the registrar will, wherever possible, try to send complaints for early resolution. Early Resolution Officers use negotiation, conciliation and other expert techniques to try to help the parties resolve their issues expeditiously. Cases that cannot be resolved in that way, however, may also be forwarded to an investigator.

Solicitor-Client Privilege

A decision by the Supreme Court of Canada in July 2008 had an impact on the way we conduct some of our investigations, particularly when it comes to helping individuals gain access to their own personal information that may be held by organizations.

The case related to the situation in which an organization refuses to turn over the requested documents on the grounds that they are protected by solicitor-client privilege.

In *Canada (Privacy Commissioner) v. Blood Tribe Department of Health*, the Supreme Court ruled that the Privacy Commissioner does not have the legal authority to compel the production of documents that are subject to a claim of solicitor-client privilege when it is necessary for her to inspect them in order to independently verify the claim.

Some organizations have interpreted this decision as eliminating altogether the Privacy Commissioner's role in verifying their claims of solicitor-client privilege.

The Office has placed the matter before the Federal Court for further clarification.

We believe the Supreme Court eliminated only one of the tools the Office can use to ensure that individuals' rights to access their own personal information are respected

– the authority to compel production of records for inspection if they are subject to a claim of solicitor-client privilege.

However, we remain committed to investigating solicitor-client privilege claims with other tools at our disposal, in a manner consistent with both our statutory mandate and the Supreme Court of Canada's guidance.

Investigative Discretion

In early 2009, the federal government introduced long-awaited anti-spam legislation, the *Electronic Commerce Protection Act*, which also included important amendments to PIPEDA.

If passed, the legislation would provide the Privacy Commissioner with greater discretion in accepting complaints and conducting investigations – whether they involve spam or any other privacy issues.

Under the legislation, the Commissioner may decide not to accept a complaint if she determines:

- The complainant has not exhausted other available grievance or review procedures. (For example, with a body which exercises supervisory or oversight responsibilities over an industry or professional group.
- The complaint could be dealt with, initially or completely, under other federal or provincial laws.
- The complaint is not filed within a reasonable period of time from the date when the issue arose.

Other amendments would allow the Commissioner to discontinue an investigation where she is of the opinion that:

- There is insufficient evidence to pursue the investigation;
- The complaint is trivial, frivolous or vexatious or is made in bad faith;
- The organization has provided a fair and reasonable response to the complaint;
- The matter is already under investigation or has already been the subject of a report by the Commissioner;

- The matter could be, is being, or has already been, addressed under another grievance or review procedure or another federal or provincial law.

Our Office has previously asked Parliament to provide the Commissioner with the discretion to refuse and/or discontinue complaints the investigation of which would serve little or no useful purpose, and would not be in the public interest to pursue.

At the moment, valuable resources are disproportionately consumed by having to open and investigate all individual complaints on a first-come first-serve basis. We anticipate that greater discretion to refuse and/or discontinue complaints will allow our Office to better focus investigative resources on privacy issues that are of broader systemic interest.

INTERNATIONAL INITIATIVES

In a global economy in which personal information is in constant motion, privacy issues recognize no national borders.

Multinational corporations transfer personal information to other jurisdictions to take advantage of lower wages, economies of scale and to meet the demands of their customers. Individuals, too, are sending their personal information around the globe as they conduct online transactions 24/7 and expect access to their money wherever they are in the world.

Emerging technologies and concerns about international terrorism and transnational criminal activity have created additional challenges for privacy commissioners and other enforcement authorities.

Spam and unwanted telephone calls often originate from outside of Canada.

In this modern context, it is clear that Canada needs to work with international counterparts toward the seamless protection of personal information around the globe.

Our Office has been working on these transborder issues for a number of years, sharing best practices with countries new to privacy protection, and helping to develop enforcement mechanisms to provide individuals with recourse, regardless of where their information is being processed.

In 2008, we built on the success of the 29th International Conference of Data Protection and Privacy Commissioners, which we hosted in Montreal the previous September. At that conference, commissioners agreed to:

- Work together, and with international organizations, to strengthen data protection worldwide,

- Urge governments to adopt global standards to safeguard passenger data used for law enforcement and border security purposes, and

- Support the development of effective and universally accepted international privacy standards through bodies such as the International Organization for Standardization (ISO).

Our global efforts focused on establishing and maintaining strategic relationships, and co-ordinating and participating in activities such as international policy and standards development.

Here are other international activities we engaged in during 2008:

- Our Office was an active participant in the Organisation for Economic Co-operation and Development's Working Party on Information Security and Privacy. The Commissioner spoke at the OECD's Ministerial Meeting on the Future of the Internet Economy in Seoul, Korea and was a member of the Canadian delegation.

- We were active participants in the Asia-Pacific Economic Co-operation Data Privacy Subgroup, which explored ways to implement the 2004 APEC Privacy Framework. We were also working with privacy commissioners' offices in British Columbia, New Zealand, Hong Kong and Australia, as well as the U.S. Federal Trade Commission, to develop a Framework for Cross-border Privacy Enforcement Co-operation within the APEC economies.

- A member of our Office chaired a working group of the Canadian Advisory Committee to the ISO subcommittee responsible for developing security standards for information technology. He is also the Canadian Head of Delegation to a working group on identity management and privacy technologies at international ISO meetings.

- Our Office, which was instrumental in creating the Association of Francophone Data Protection Authorities, also continued to participate in several other international forums, including the Asia Pacific Privacy Authorities (APPA), the International Working Group on Data Protection in Telecommunication, the London Action Plan, and the Federated States Working Group.

LEGAL SERVICES, POLICY AND PARLIAMENTARY AFFAIRS

In the Courts

A number of new court applications were filed in 2008. Under section 14 of PIPEDA, a complainant may, in certain 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. There were five applications filed by complainants at the Federal Court in 2008.

There was one Commissioner-initiated application filed under Section 15. This section 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, which has helped establish a high level of compliance with recommendations.

The Privacy Commissioner also files preliminary documents in certain court proceedings to be removed as a party when she is improperly named as one.

As well, she participated this year in an appellate proceeding in the United States, which is discussed further below.

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

Settled Cases

Privacy Commissioner v. X
Court File No. T-142-09

This case concerns the failure of an insurance company to provide the OPC with affidavit evidence to support its claim of litigation privilege over documents sought by the complainant in an access request.

Following the issuance of a well-founded Report of Findings, the OPC filed a Notice of Application in the Federal Court seeking an order confirming or denying the organization's claim of litigation privilege and requiring the organization to provide the complainant with the documents should the Court reject the organization's claim.

Shortly after commencing the Application in Court, the organization opted to abandon its claim of privilege over the documents in issue, and released to the complainant all the available information to which he was entitled under the Act. Accordingly, the Privacy Commissioner discontinued the Application.

Ongoing Litigation

State Farm Automobile Insurance Company v. Privacy Commissioner of Canada
New Brunswick Court of Appeal File No. 14-08-CA

On July 27, 2007, State Farm Automobile Insurance Company initiated an application in the Court of Queen's Bench of New Brunswick for a declaration that:

Note: This case was also reported in our 2007 annual report.

- PIPEDA did not apply to document disclosure, privilege or other privacy interests of a complainant in relation to his bodily injury damages claim against a State Farm insured client (because State Farm was not engaged in "commercial activities" when it collects, uses or discloses personal information in the course of defending its insured client against litigation initiated by the complainant);

- If PIPEDA does apply, PIPEDA was enacted outside the powers allotted to Parliament;

- The Privacy Commissioner lacked the authority to investigate the complaint; and

- The Privacy Commissioner has no right to request or compel from State Farm information necessary to conduct an investigation.

The Privacy Commissioner filed a preliminary motion to have State Farm's application dismissed or stayed on the ground that the Federal Court was the more appropriate forum.

The motion was granted in January 2008. The Court of Queen's Bench determined that the Federal Court was the more appropriate forum to determine State Farm's application, which involved questions of both constitutional validity and a judicial review of the Privacy Commissioner's authority. Because the Federal Courts have exclusive jurisdiction over applications for judicial review of the Privacy Commissioner, the Federal Court was found to be the most appropriate forum.

State Farm appealed to the New Brunswick Court of Appeal and a hearing was held on September 10, 2008. The New Brunswick Court of Appeal delivered its judgment on January 22, 2009. In reasons affirming the motion judge's decision, the Court of Appeal dismissed State Farm's appeal.

The Court of Appeal affirmed our position that State Farm's application is, for all intents and purposes, an application for judicial review that falls within the exclusive jurisdiction of the Federal Court. The Court noted that, regardless of how State Farm identifies its claim, it is in substance a challenge to the actions and decisions of the Office that should be heard by the Federal Court.

State Farm sought leave from the Federal Court for an extension of time to file a similar application before the Federal Court in February 2009.

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 the 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 web site, had been the subject of a complaint to our Office. The Assistant Privacy Commissioner initially determined that she lacked jurisdiction to investigate the complaint. However, the complainant filed a judicial review application, and in 2007 the Federal Court allowed it on the grounds that the Assistant Commissioner did have jurisdiction to investigate the transborder flow of personal information in this case.

In May 2006, the U.S. Federal Trade Commission (FTC) charged AccuSearch, Inc. with violating federal U.S. law by selling consumers' telephone records to third parties

without the consumers' knowledge or authorization. According to the FTC, the defendants advertised on their website that they could obtain the confidential phone records of any individual – including details of outgoing and incoming calls – and make that information available to their clients for a fee. To obtain such information, the FTC alleged that the defendants caused others to use false pretences to induce telecommunications carriers to disclose confidential records.

On January 28, 2008, a judge of the United States District Court for the District of Wyoming found that the defendants' obtaining and selling of confidential phone records without consumers' knowledge or consent was "necessarily accomplished through illegal means," and that defendants knew that the phone records were being obtained surreptitiously, that this practice caused harm, and barred Accusearch, Inc. from, among other things, obtaining, purchasing, marketing, or selling consumer personal information unless the information was lawfully obtained. Accusearch, Inc. appealed from this decision to the United States Tenth Circuit Court of Appeals.

Considering our Office's involvement with Accusearch, Inc. as reported in past annual reports (2007, 2006 and 2005) and considering the transborder nature of the issues at stake, our Office prepared and was granted leave to file an *amicus curiae* brief in the appellate proceedings initiated by Accusearch.

In our view, the case before the U.S. Tenth Circuit Court of Appeals relates to trans-border 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, issues all at the heart of our mandate.

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.

Recognition that Accusearch Inc.'s practices and the resulting harms are illegal under U.S. law would support international cooperation between Canadian and United States regulators by enhancing the consistency in approach between the two jurisdictions.

This, in turn, would provide the necessary assurance to organizations that contemplate outsourcing data processing functions in the United States, and help boost the confidence that individuals need in conducting business over the Internet. Our brief particularly highlighted the fact that the unauthorized collection, use and disclosure of personal information over the Internet by data-brokers can cause harm and has extra-territorial effects.

In June 2009, the United States Tenth Circuit Court of Appeals affirmed the injunctive and monetary judgment against Accusearch, Inc.

Judicial review applications under section 18.1 of the *Federal Courts Act*

Canada (Privacy Commissioner) v. Blood Tribe Department of Health
Supreme Court of Canada File No. 31755

NOTE: This case was also reported in our 2006 and 2007 Annual Reports

This was an appeal by the Privacy Commissioner to the Supreme Court of Canada. We appealed the Federal Court of Appeal's decision that PIPEDA did not authorize the Commissioner to compel the production of documents subject to a claim of solicitor-client privilege.

An individual complained to the Office that the Blood Tribe Department of Health improperly withheld her personal information following her access request. The Blood Tribe asserted that some documents it withheld from the complainant were subject to solicitor-client privilege.

The OPC determined that it was necessary for it to view the documents claimed to be subject to solicitor-client privilege in order to independently verify the claim. After several requests, the Blood Tribe maintained its original refusal to provide the OPC with copies of the documents in question. We issued a production order pursuant to s. 12(1)(a) of PIPEDA and the Blood Tribe contested the validity of this order in Federal Court.

The Federal Court ruled that the OPC could compel the production of the records in issue for inspection to verify the claim of privilege. The Federal Court of Appeal disagreed. The Supreme Court of Canada affirmed the decision of the Federal Court of Appeal and found that s. 12(1)(a) did not include the power to compel the production of documents subject to a claim of privilege because this authority was not clearly and expressly authorized.

The Supreme Court held that compelled disclosure of documents subject to a claim of privilege to the Privacy Commissioner would constitute an infringement of the privilege even if the Commissioner did not disclose the information any further.

The Court distinguished the role of the Commissioner from that of an independent and impartial judge (who may inspect documents subject to a claim of privilege) because, unlike a court, the Commissioner may become adverse in interest to the organization if she brings a court action against the organization. The Court was also troubled by the Commissioner's statutory power to disclose information she receives to prosecutorial authorities or in the public interest.

The Supreme Court found that an organization could properly establish the existence of solicitor-client privilege on a *prima facie* basis through the provision of adequate affidavit evidence. Where there is adequate affidavit evidence in support of the claim of privilege, a rebuttable presumption in favour of the existence of the privilege arises. This presumption may be tested through cross-examination or other means.

We are now investigating claims of solicitor-client privilege with the benefit of this guidance from the Supreme Court. (Please see page 39 for more information.)

The Supreme Court agreed that questionable claims of solicitor-client privilege must be independently verified. The Court determined that the Privacy Commissioner has at least two alternative effective and expeditious means of ensuring the requirements of PIPEDA are met where dubious claims are encountered.

First, the Privacy Commissioner may refer a question of solicitor-client privilege to the Federal Court under s. 18.3(1) of the *Federal Courts Act* at any point in her investigation.

Second, the Privacy Commissioner may report an impasse over the issue of privilege in her Report of Findings and bring an application to the Federal Court for relief pursuant to s. 15 of the Act.

Complainant-initiated court applications under section 14 of PIPEDA

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

An individual filed a complaint with our Office alleging improper collection of personal information and inadequate policies to protect personal information. The company's vice-president had sent out a company-wide e-mail asking whether anyone knew which firm the complainant worked for.

NOTE: this case was also reported in our 2007 Annual Report.

As there was no evidence that any J.J. Barnicke employee had responded to the e-mail, the Assistant Privacy Commissioner found that there was no collection of personal information and therefore no contravention of the Act. While the investigation revealed that J.J. Barnicke did not have appropriate privacy policies or procedures in place, the company implemented all of the Assistant Commissioner's recommendations in the course of the investigation and this matter was resolved to the Assistant Commissioner's satisfaction.

The complainant filed an application in the Federal Court seeking damages in the amount of $75,000 and a declaration that his statutory rights had been violated. We participated in the proceedings as an Added Party.

In the course of these proceedings, a procedural issue arose with respect to the relevance of information that could be characterized as "bad character" evidence about the Applicant that J.J. Barnicke was relying on in its defence. In reasons responding to the Applicant's motion to strike those portions of the Respondent's materials that were found to introduce irrelevant "bad character" evidence, the Court adopted the position put forward by the Privacy Commissioner.

The Court ruled: "For complainants who are already of the view that their privacy has been violated, the prospect of public proceedings to protect their rights become even more daunting when having to defend their personal character or having irrelevant private facts publicized in order to obtain a remedy for a respondent's breach. Evidence of bad character alone is of no relevance to any privacy matter properly in issue before this Court. Parties to a public hearing should be discouraged from filing such materials." (2009 FC 170, para. 31)

The application on the merits, heard on August 25, 2008, was dismissed after the Court reached the same conclusions that the Assistant Privacy Commissioner had.

With respect to the collection complaint, the Court held that there was no evidence that J.J. Barnicke had collected any of the Applicant's personal information. The Court applied prior jurisprudence to find that PIPEDA does not prohibit attempts to collect personal information.

With respect to the Applicant's claim for damages for the company's initial non-compliance with the Accountability Principle, the Court found the fact that J.J. Barnicke had brought itself into compliance with PIPEDA in the course of the Commissioner's investigation to be compelling. There was no basis for an award of damages on the facts.

Costs were awarded to the company. The Court recognized that litigants should not be dissuaded from exercising their rights for fear of cost awards, particularly because PIPEDA litigation is in its infancy. However, the Court found that awarding costs against an Applicant would be appropriate where a litigant was using PIPEDA litigation as a surrogate forum for unrelated legal disputes and not for the purpose of exercising his or her privacy rights.

The Applicant filed a Notice of Appeal on March 19, 2009 in respect of the Court's decision on the issue of "costs" and "bad character" evidence.

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

An individual filed a complaint with the Office of the Privacy Commissioner against the Bank of Nova Scotia. The individual alleged that the bank had improperly disclosed his personal financial information to a third party, who he alleged had been permitted to substitute her own mailing address for the address he had placed on file in contravention of PIPEDA.

We investigated and determined that the complaint was well-founded and resolved. The investigation confirmed that the bank had appropriate policies in place at the relevant times that, if followed, would likely have prevented the contravention of the Act. The breach of PIPEDA that occurred was the result of an isolated human error. The bank implemented all of the Commissioner's recommendations and agreed to apologize to the complainant and provide copies of account statements that had been misdirected.

On April 11, 2008, the complainant filed a Notice of Application with the Federal Court that names both the bank and the third party as Respondents. The Applicant is seeking damages in the amount of $400,000, declaratory relief and various orders against the Bank. The Applicant seeks similar relief against the third party.

On June 9, 2008, the Privacy Commissioner was granted leave to appear as a party.

Commissioner-initiated court applications under section 15 of PIPEDA

Privacy Commissioner of Canada v. Canad Corporation of Manitoba Ltd.
Federal Court File No. T-586-08

This matter is described on page 31. With the complainant's consent, we initiated legal action in this case in order to enforce recommendations issued in an investigation.

In early 2009, court-ordered mediation was prescribed in this case, but the case itself remained before the Federal Court. Canad Inns was given time to determine feasible means to limit the personal information it collects. The company was to submit affidavits outlining its proposed efforts. Our Office will then examine its proposals and file for a case management conference to determine future steps in the proceedings.

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

NOTE: This case was not before the court until early 2009.

Following an in-flight incident on a short-haul flight, Air Canada collected personal information about the individual involved including statements from crew members, witness statements and in-flight reports. This individual requested access to his personal information. Air Canada refused the access request, claiming solicitor-client privilege.

The individual complained to us. We were unable to resolve the matter in the course of our investigation because Air Canada refused to provide the Office with sufficient particulars concerning its claim of solicitor-client privilege – namely a sworn affidavit in support of its claim of privilege. Air Canada's position was that the Office lacked jurisdiction to investigate claims of solicitor-client privilege following the Federal Court of Appeal and 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 in respect of the application of the exemption from the right of access for solicitor-client privilege recognized under paragraph 9(3)(a) of the Act and various orders.

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.

No provinces or territories enacted legislation in 2008 for which they have sought consideration as substantially similar to PIPEDA.

Policy Development

PIPEDA, which came into force in 2001, included a requirement for a review by Parliament after five years. As such, we have been working with Industry Canada, the House of Commons Standing Committee on Access to Information, Privacy and Ethics

and stakeholders since 2006 to gauge the impact of the law on private-sector privacy, and to recommend improvements.

This very important work continued during 2008. In particular, we had an opportunity to examine the outcome of Industry Canada's stakeholder consultations, and to provide our response.

Both the committee and the government agreed with us that, on the whole, PIPEDA is working well and large-scale reforms are not needed at this time. PIPEDA has only been in full force since 2004, and it takes time for the full impact of such complex legislation to be felt.

Even so, we feel that some adjustments would be beneficial. Here are summaries of our policy positions on key aspects of the PIPEDA review process:

- Mandatory Breach Notification

Our Office feels strongly that private-sector organizations should be obliged by law to inform individuals if their personal information may have been put at risk in a data breach.

We believe this would force companies to take more seriously their obligation to safeguard the personal information of their customers and clients, thus reducing the likelihood of data spills. It would also ensure that the affected individuals are equipped with timely information, so they can move to protect themselves from fraud and identity theft.

Moreover, if a formal breach-notification regime were in place, it would be easier to track patterns and vulnerabilities so that organizations could better learn from the experiences of others.

In particular, we have argued that businesses must promptly notify individuals of a data spill that could pose a "risk of significant harm to individuals or organizations," where harm should be interpreted to mean more than financial damage alone.

We have also said that companies should be required to inform our Office of cases involving "any material breach" of personal information. Such notification should include details of the incident, the steps taken to inform the individuals affected, and the justification, if any, for not doing so.

In the meantime, our Office in 2008 issued guidelines and a step-by-step handbook for organizations dealing with data spills.

- Complaint Discretion

Our Office favours a change to PIPEDA under which we would have greater discretion to discontinue certain complaints early, on the grounds that they are made in bad faith, could be better dealt with in a different forum, or where further investigation would serve no purpose.

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.

There is a case to be made that organizations such as ours can have a bigger impact by examining how rapidly changing surveillance, information and nanotechnologies are affecting people's privacy, often even without their knowledge.

- Schedule III Banks

We have also suggested to the government that it consider amending PIPEDA so that it would clearly apply to Schedule III authorized foreign banks.

Parliamentary Affairs

Parliament and its committees had a reduced sitting schedule during 2008 because of a general election and a prorogation. While Parliament was in session, much of its work in relation to the mandate of this Office focused on amendments to the *Privacy Act*.

Even so, in an appearance before the Commons Standing Committee on Access to Information, Privacy and Ethics in April 2008, the Commissioner reiterated the Office's call for PIPEDA reforms, including in particular a mandatory breach-notification regime.

At the same time, we were weighing in on other legislative initiatives that we felt could have an impact on the privacy of Canadians.

In January 2008, for instance, we wrote to the Ministers of Industry and Canadian Heritage to express concerns about possible amendments to the *Copyright Act*. We argued that one of those amendments, which would authorize the use of certain technical mechanisms to prevent copyright infringement, could result in the collection, use and disclosure of the personal information of Canadians, without their consent. This would have a negative impact on their privacy rights.

AUDIT AND REVIEW

PIPEDA gives the Commissioner the authority to audit the personal information handling practices of organizations if there are reasonable grounds to believe there is non-compliance with the Act.

The Privacy Commissioner has the authority to receive evidence from witnesses; may enter the premises at any reasonable time; and may examine or obtain copies of records found on the premises. The Commissioner can compel individuals in businesses to provide evidence. Audit findings and recommendations are presented to the organization and may be disclosed to the public.

In 2008, the Audit and Review branch started an audit in the financial sector that was still in the early stages as we prepared this annual report. We will provide an update in 2009.

Self-Assessment Tool for Businesses

In August 2008, the OPC launched the PIPEDA Self-Assessment Tool, designed to assist medium to large businesses in evaluating and improving their personal information management practices in compliance with PIPEDA and its fair information principles.

In a world of ubiquitous computing and information sharing it is increasingly difficult to ensure appropriate use and protection of personal information. Strong privacy governance and management within organizations are effective means of mitigating privacy risks and ensuring that fair information principles are applied in business decisions and day-to-day operations.

Privacy self-assessment is a process whereby an organization initiates an evaluation for the purpose of benchmarking and improving its own privacy systems and practices over time. This includes assessing the organization against a set of expectations to determine the degree to which they are met. In measuring compliance, gaps and/or risks may be identified for the purpose of guiding and following up remedial action.

The OPC sees self-assessment by organizations as an efficient and effective means of promoting privacy principles.

The Self-Assessment Tool was developed in consultation with a number of chief privacy officers of businesses, leaders in management training, and professional associations. It includes a compliance guide to inform organizations of their obligations under PIPEDA, and a diagnostic tool to assess compliance with the Act.

This important new tool is on our website.

Truncating Credit Card Numbers

Our Office takes a strong interest in the issue of credit card truncation – the process of blocking out credit card numbers on sales receipts – because exposed credit card numbers can be used to commit fraud.

The OPC has expressed its position that credit card numbers should be masked on sales receipts since 2005, when we first consulted with credit card industry stakeholders. The credit card industry committed to truncate credit card numbers on electronic receipts by April, 2007. We have continued to monitor the situation, and in 2008 took steps to find out why the practice of including complete credit card numbers on customer receipts was still prevalent.

Credit card processors advised our Office that old equipment which does not truncate credit card numbers has been replaced on an ongoing basis and there are now very few retailers who cannot mask credit card numbers on customer receipts.

However, some small businesses continue to use outdated equipment, either because they are unaware of the requirement or because of the expense. This leaves some account numbers exposed and consumers at risk of fraud.

As a result of our discussions with the card processing industry and retailers, we prepared an advisory for businesses and individuals to point out the need to truncate and protect credit card numbers.

The advisory reminds businesses of the obligation to protect consumers' information and to adopt good privacy practices and notes that major credit card companies require organizations to suppress all but the last four digits of a credit card number on customer receipts.

The advisory also informs individuals that they also have a responsibility to protect their own information. For example, they should securely store receipts with complete credit

card information. And when the receipt is no longer needed, it should be appropriately destroyed.

The advisory has been posted on our website.

Canadian Automobile Dealers Association

Following concerns from the media and public about allegations that car sales representatives were improperly using the driver's licence information of people taking cars for test drives, our Office contacted the Canadian Automobile Dealers Association.

The industry association was unaware of any instances where sales representatives were copying driver's licences when customers took cars for a test drive and used information from the licence to run credit bureau reports without the customers' consent. The association explained that the driver's licence information is collected for insurance purposes and to confirm that the individual is licensed to drive and the copy of the driver's licence is returned to the individual or destroyed after the test drive.

Our inquiries did not identify any specific Canadian dealership involved in the alleged actions. However, the Canadian Automobile Dealers Association agreed to take this opportunity to remind its members about the proper collection, use and retention of driver's licence information and to ensure their practices were in compliance with PIPEDA.

THE YEAR AHEAD

With new technologies continuing to come on stream, the year ahead will be filled with challenges for our Office.

We will complete our investigation of Facebook in 2009. The findings and our recommendations will be important given the enormous popularity of Facebook and other social networking sites.

We were also expecting Google Street View, which features panoramic views of major cities, to launch its Canadian site in 2009. Our Office has been in discussions with Google about their rollout since 2007. We've expressed our concerns regarding the privacy of the people photographed in these street-level images. Some of our key concerns relate to notification and consent, the efficacy of the blurring technology Google is using to mask faces and licence plates, as well as the length of time Google keeps original "unblurred" images on file.

We will also be keeping an eye on Google Latitude – a social networking technology that allows cell phone users to broadcast their location through the use of GPS technology. Our concern is that people might not be aware of the potential implications for their privacy.

We have set an ambitious agenda for ourselves for the coming year and we are committed to passionately and persistently defending Canadians' privacy rights as we address crucial issues.

Our major corporate priorities for 2009-2010 are as follows:

Continue to improve service delivery through focus and innovation

- Eliminate the backlog of complaint investigation files.

- Review work processes to increase efficiency through introduction and implementation of alternative approaches to investigations, audits, privacy impact assessment reviews, and other activities.

- Explore collaborative opportunities with provincial/territorial and international counterparts.

Provide leadership to advance four priority privacy issues

- Information technology
- National security
- Identity integrity and protection
- Genetic information

Strategically advance global privacy protection for Canadians

- Develop and sustain partnerships with data protection authorities, international associations, global corporations, and other regulators such as the U.S. Federal Trade Commission.
- Share knowledge about privacy standards and other privacy issues and practices with international jurisdictions and partners.

Support Canadians, organizations and institutions to make informed privacy decisions

- Continue to identify issues of privacy risk and expand public awareness to key audiences.
- Work with partners such as the Media Awareness Network and our provincial counterparts to develop and deliver outreach programs and guidance.

Enhance and sustain organizational capacity

- Identify and implement innovative approaches and solutions to capacity challenges (i.e. major recruitment in core functions, privacy training to new investigators and other staff, developmental hiring, interchanges, enhanced departmental orientation).
- Develop and use robust technology and integrative tools to increase knowledge and information sharing as well as collaboration between OPC branches, hence enhancing capacity.

APPENDIX 1 – DEFINITIONS; INVESTIGATION PROCESS

DEFINITIONS OF COMPLAINT TYPES UNDER PIPEDA

Complaints received in 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.

- **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.

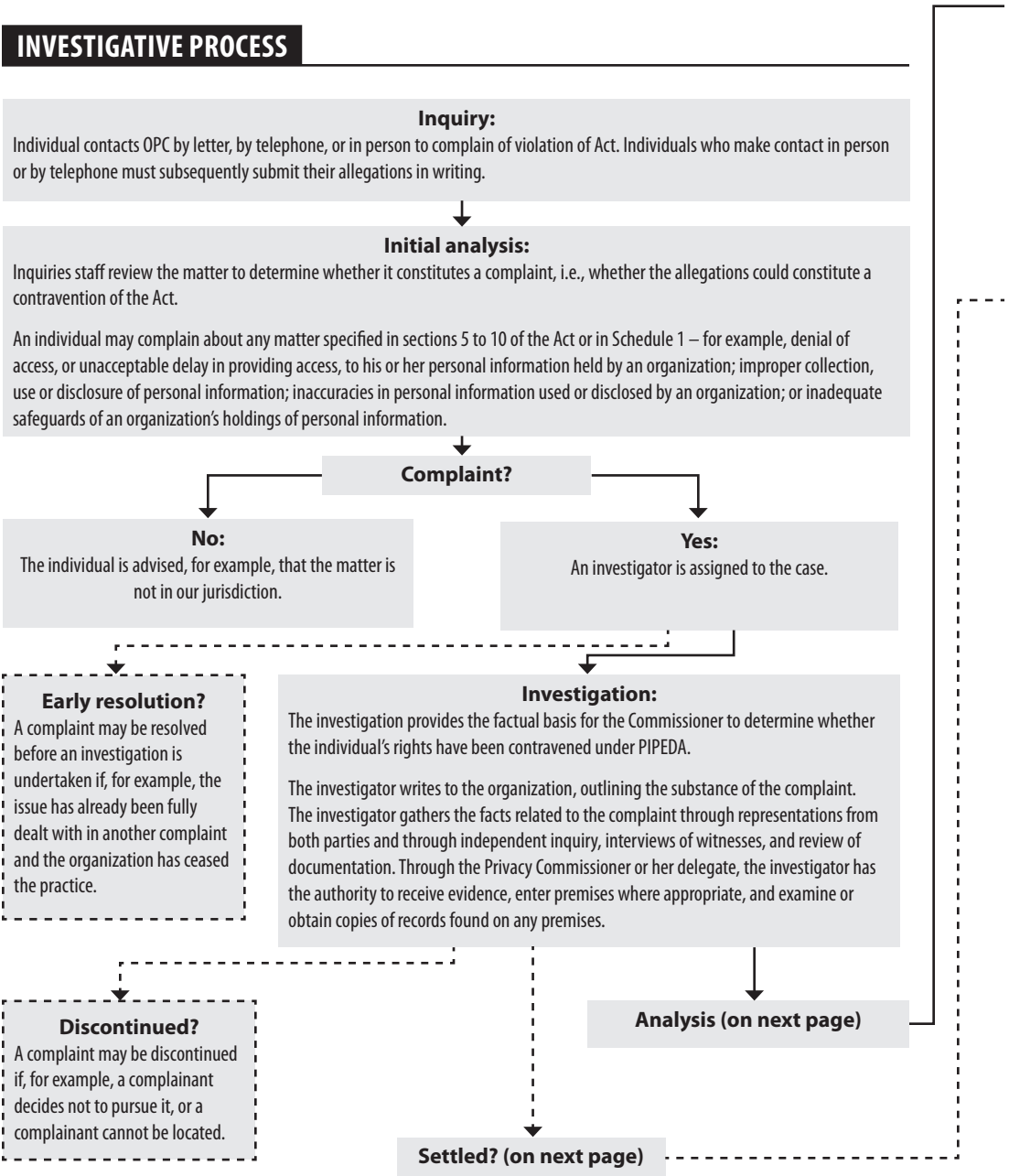
- **Settled during the course of the investigation.** The OPC helped negotiate a solution that satisfies all involved parties during the course of the investigation. No finding is issued.

- **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 the situation where an organization, on learning of allegations against it, addressed them immediately to the satisfaction of the complainant and the OPC.

INVESTIGATIVE PROCESS



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 or Research and Policy Sections, as appropriate.

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.

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.

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.

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 – INVESTIGATIONS STATISTICS

COMPLAINTS RECEIVED BY TYPE

Complaints received between January 1 and December 31, 2008

Complaint type	Count	Percentage
Use and Disclosure	162	38
Collection	93	22
Access	73	17
Safeguards	30	7
Consent	24	6
Time Limits	11	3
Accountability	8	2
Accuracy	8	2
Correction/Notation	5	1
Openness	3	<1
Challenging Compliance	2	<1
Other	2	<1
Fee	1	<1
Total	**422**	

The largest number of complaints we received involved how organizations have used and disclosed information. The most common type of use and disclosure complaint involves an allegation of personal information being used for purposes other than for which it was collected, and being disclosed to third parties without an individual's consent.

Collection complaints usually concern the collection of information without proper consent or the collection of more information than required for the stated purpose.

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.

CLOSED COMPLAINTS BY FINDING

Complaints closed between January 1 and December 31, 2008

Finding	Count	Percentage
Settled	108	26
Discontinued	108	26
Not well-founded	74	18
Well-founded Resolved	30	7
Resolved	27	7
Well-founded	25	6
No jurisdiction	20	5
Early Resolution	19	5
Other	1	<1
TOTAL	**412**	

Settled complaints continue to make up a significant portion (more than one quarter) of our closed complaints. This suggests that we often succeed in finding solutions that satisfy complainants, respondent organizations and our Office.

The percentage of discontinued cases is up slightly – to 26 per cent, compared to 21 per cent last year. There are a number of reasons why cases are discontinued. For example, complainants abandon complaints for personal reasons; an organization resolves an issue before an investigation begins; or a complainant does not provide us with requested information needed to complete an investigation.

INVESTIGATION TREATMENT TIMES — BY FINDING

For the period between January 1 and December 31, 2008

Disposition	Average Treatment Time in Months
Early Resolution	9.42
No jurisdiction	14.20
Discontinued	17.28
Settled	20.28
Not well-founded	23.92
Resolved	25.15
Well-founded Resolved	26.47
Well-founded	29.76
Other	36.00*
Overall Average	**20.73**

* The treatment time for this complaint type represents only one case.

Unfortunately, our average treatment times are longer than last year because of our backlog situation.

A key contributing factor to the backlog was a lack of investigators. We have lost a number of experienced PIPEDA investigators over the last three years. At times during 2008, we were operating with only four experienced PIPEDA investigators with very large caseloads.

A number of organizations are vying for a small pool of access and privacy professionals, making recruitment and retention a challenge. To counter the significant loss of PIPEDA investigators, an intensive recruiting initiative was launched in 2008, which resulted in the hiring of 10 new PIPEDA investigators in early 2009.

Another factor contributing to our lengthy treatment times is that we have been concentrating on completing some of the very oldest files as part of a backlog blitz. Statistically, this increases our average time per complaint file.

Our focus on backlog files and having more trained investigators will result in improved treatment times in the future.

INVESTIGATION TREATMENT TIMES – BY COMPLAINT TYPE

For the period between January 1 and December 31, 2008

Complaint Type	Average Treatment Time in Months
Correction / Notation	16.3*
Time Limits	18.2
Accuracy	18.5
Consent	18.6
Retention	18.6*
Safeguards	19.2
Collection	19.6
Use and Disclosure	21.2
Access	22.0
Accountability	24.7
Openness	25.8*
Fee	27.7*
Other	41.0*
Overall Average	20.7

* The treatment time for these complaint types reflects six or fewer cases each.

Use and Disclosure, Collection and Safeguards typically take longer to investigate because corrective measures are often being sought.

The Openness category included a complex joint investigation with another jurisdiction which took more time. The length of time to complete the Fee and Other Categories cases was partially a matter of scarce investigative resources, but also because negotiations with organizations were required to bring about improvements to their privacy practices.

INVESTIGATION TREATMENT TIMES — BY SECTOR

For the period between January 1 and December 31, 2008

Sector	Average Treatment Time in Months
Rental	12.33
Services	13.53
Transportation	14.77
Financial Institutions	19.61
Telecommunications	19.68
Health	20.00
Professionals	20.88
Insurance	22.85
Accommodations	23.46
Other	23.60
Sales	27.54
Overall Average	20.73

FINDINGS BY COMPLAINT TYPE

Complaints closed between January 1 and December 31, 2008

	Discontinued	Early Resolution	No Jurisdiction	Not Well-founded	Other	Resolved	Settled	Well-founded	Well-founded Resolved	TOTAL	Percentage
Use and Disclosure	43	5	10	27	0	4	34	10	10	**143**	35
Collection	38	5	5	12	0	2	21	5	6	**94**	23
Access	11	3	0	13	0	12	18	2	2	**61**	15
Safeguards	5	2	1	5	0	1	10	5	3	**32**	8
Consent	6	0	3	3	0	2	7	0	4	**25**	6
Accountability	1	0	0	6	0	0	7	1	0	**15**	4
Time Limits	1	2	1	1	0	3	4	1	2	**15**	4
Accuracy	1	0	0	4	0	1	2	0	0	**8**	2
Openness	0	0	0	1	0	0	1	0	3	**5**	1
Retention	2	0	0	0	0	1	2	0	0	**5**	1
Correction/ Notation	0	2	0	1	0	0	1	0	0	**4**	1
Fee	0	0	0	0	0	1	1	1	0	**3**	<1
Other	0	0	0	1	1	0	0	0	0	**2**	<1
TOTAL	**108**	**19**	**20**	**74**	**1**	**27**	**108**	**25**	**30**	**412**	

FINDINGS BY INDUSTRY SECTOR

Complaints closed between January 1 and December 31, 2008

	Discontinued	Early Resolution	No Jurisdiction	Not Well-founded	Other	Resolved	Settled	Well-founded	Well-founded Resolved	TOTAL
Financial Institutions	22	8	2	22	0	6	26	5	12	**103**
Telecommunications	15	2	1	16	1	1	23	6	1	**66**
Sales	9	2	1	9	0	4	16	2	9	**52**
Transportation	28	2	0	5	0	1	7	4	1	**48**
Other	8	0	5	4	0	5	13	3	2	**40**
Insurance	6	0	0	6	0	7	10	1	3	**33**
Accommodations	9	0	4	2	0	1	8	2	0	**26**
Professionals	3	1	4	5	0	1	1	0	1	**16**
Services	8	4	1	1	0	0	0	0	1	**15**
Health	0	0	2	2	0	1	4	1	0	**10**
Rental	0	0	0	2	0	0	0	1	0	**3**
TOTAL	**108**	**19**	**20**	**74**	**1**	**27**	**108**	**25**	**30**	**412**