TABLE OF CONTENTS

MESSAGE FROM THE COMMISSIONER

The year 2007 will no doubt be remembered in the privacy world as the year of the data breach.

The size of some of the data spills reported around the globe was staggering: An estimated *94 million* credit and debit cards were exposed when hackers broke into the system at TJX Companies Inc., the U.S. retail giant which owns Winners and HomeSense stores in Canada. In the United Kingdom, two computer discs holding the personal details of some *25 million* child benefit recipients vanished.

Those were only the two most high-profile data security disasters. Scores of other major data breaches affecting millions of people around the world were also reported.

Data breaches here in Canada kept our team extraordinarily busy in 2007.

Of particular note, we investigated the TJX/Winners breach, as well as the disappearance of a hard drive containing the personal information of close to half a million clients of Talvest Mutual Funds, a subsidiary of the Canadian Imperial Bank of Commerce (CIBC).

An Obligation for Business

It's clear that organizations of all sizes can – and must – do more to prevent data leaks.

The *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) imposes a legal obligation on businesses to adequately safeguard the personal data they collect. Too often, however, we see breaches occur as a result of human error or a cavalier approach to security.

Our Office has been working with the business community in Canada to improve privacy practices and encourage the use of strong information technology safeguards.

Recent headlines about massive data breaches are also prompting some businesses to rethink how they handle privacy and security. No one wants to have to call clients to tell them that their personal information has been lost.

I hope 2008 will mark a turning point in the protection of personal information. It is time for businesses to recognize that personal information is valuable – and it needs to be well protected.

Unfortunately, the challenge of safeguarding personal information is greater than ever. The amount of personal data being collected, stored and shared is ever-growing – and so too is the ingenuity of fraudsters and hackers.

A Busy Year

Our Office will also remember 2007 as the year we:

- Hosted the 29th International Conference of Data Protection and Privacy Commissioners;
- Expanded our work in the international arena;
- Contributed to efforts to improve *PIPEDA*; and
- Welcomed a new Assistant Privacy Commissioner.

A few thoughts on each of these key events and issues of the year….

Hosting the Privacy World

The success of the 29th International Conference of Data Protection and Privacy Commissioners – held in Montreal in September and following through on our initial 2002 engagement – was beyond our highest expectations.

We welcomed more than 600 commissioners, academics, privacy professionals, advocates, government officials, IT specialists and others from around the globe – making it the largest-ever conference of its kind. Most importantly, the positive reviews and kudos from participants justified the time and resources invested in this event.

The conference theme was Privacy Horizons: *Terra Incognita*. Early cartographers marked unknown lands that had yet to be mapped with this Latin term. One of the earliest known terrestrial globes from Europe labels an uncharted edge of the ocean "*hic sunt dracones*" – or "here be dragons."

This notion of an unknown landscape with lurking dragons seemed the perfect metaphor for the future of privacy.

Privacy issues are changing rapidly, with powerful new technologies and the international war on terror acting as potent forces which threaten the privacy of people around the world.

The goal of our conference was to begin to chart what the privacy world of the future might look like and also to equip privacy advocates with some strong dragon-slaying tools.

During a series of plenaries, workshops and information sessions, we considered the best strategies for defending privacy rights in the face of constant change.

Participants heard from the who's who of the privacy world, including security technology guru and author Bruce Schneier; Simon Davies, a pioneer of the international privacy arena and founder of Privacy International; consumer privacy advocate Katherine Albrecht; Marc Rotenberg, executive director of the Electronic Privacy Information Center; Peter Fleischer, Google's global privacy counsel; Peter Hustinx, the European Data Protection Supervisor; as well as Peter Schaar, now past-chair of the EU Article 29 Data Protection Working Party and France's Alex Türk, who is now chair of the working party.

Our guest of honour, on hand to help open the conference, was the Honourable Peter Milliken, Speaker of the House of Commons.

Our keynote speaker was U.S. Homeland Security Secretary Michael Chertoff, who bluntly argued his thoughts on balancing privacy rights in the context of national security to a somewhat skeptical audience – and sparked plenty of discussion throughout the conference!

A member of our external advisory committee, University of Ottawa law Professor Michael Geist, who holds the Canada Research Chair of Internet and E-commerce Law, later responded by describing Chertoff's case for greater surveillance by governments to hundreds of privacy advocates as a "confrontational challenge."

" … His vision of a broad surveillance society – supported by massive databases of biometric data collected from hundreds of millions of people – presented a chilling future. Rather than *terra incognita*, Chertoff seemed to say there is a known reality about our future course and there is little that the privacy community can do about it," Geist wrote in his popular blog.

Hopefully, Chertoff's comments will serve as inspiration for privacy advocates to make an even stronger case for privacy rights in the post 9-11 world.

The conference program underscored the wide range of issues which will have an impact on privacy in the coming years as well as the increasingly global nature of privacy issues.

We prepared 14 workbooks before the conference. Most included a commissioned paper by a subject-matter expert and a variety of other resources, such as bibliographical materials, to satisfy the curiosity of participants who might be new to a particular subject, as well as the more rigorous requirements of key policy and decision-makers to locate trustworthy information about the privacy implications of our conference topics. These are available on our conference website at www.privacyconference2007.gc.ca and are an important legacy of the conference.

We have posted details about the cost of the conference on our website. We stayed well within our overall financial targets.

Feedback from conference participants was extremely positive. In fact, one of the few frustrations expressed by delegates was that there were too many sessions of interest occurring at the same time!

A Global Concern

The impact of globalization on privacy is a growing preoccupation of my Office. The fact that more and more personal information is crossing borders means data breaches often affect people in multiple countries – as we saw in the TJX/Winners case. The increasing popularity of the Internet also raises many cross-border issues with implications for our Office.

I am pleased to report we are making progress in our work with international counterparts to find global privacy solutions.

Resolutions adopted during the conference by data protection authorities from every continent recognized the increasingly global context of privacy issues.

Commissioners called for international standards for the use and disclosure of personal information collected by travel carriers about passengers. They warned that the transfer of personal information from travel agents, carriers and domestic and foreign governments poses an ongoing threat to the personal privacy of passengers. A global solution needs to be developed with the cooperation of carriers, law enforcement agencies, international organizations, civil liberties groups, and data protection and privacy experts.

Data protection authorities adopted two other resolutions: to improve international cooperation; and to build upon the work of the International Standards Organization to establish shared privacy standards in the area of information technology.

My Office has also been working on transborder issues as part of other international initiatives.

OECD/APEC Efforts

I was pleased to chair an Organisation for Economic Co-operation and Development (OECD) volunteer group examining ways to encourage cooperation between data protection authorities and other enforcement bodies with respect to cross-border complaints and cases arising from transborder data flows.

The group produced a report summarizing the powers of enforcement authorities in OECD member countries and their ability to share information to facilitate cross-border cooperation. The report concluded that, despite differences in national laws, there is considerable scope for a more global and systematic approach to cross-border privacy law enforcement cooperation. In June 2007, the OECD adopted a recommendation on cross-border cooperation which was based on the work of the volunteer group.

The volunteer group's work will also be highlighted during a June 2008 OECD ministerial meeting in Korea, where the theme will be the future of the Internet economy.

My Office has also contributed to the work of the Asia-Pacific Economic Cooperation (APEC) on privacy issues.

Canada has been active in ensuring that core privacy values and principles are reflected in APEC data protection rules – an initiative that will be of clear benefit to Canadians given our increasing data flows with APEC member countries. Our work in 2007 focused on exploring ways to implement an APEC Privacy Framework.

PIPEDA Reform

Here at home, we supported the work of a committee of MPs reviewing *PIPEDA*. Members of the House of Commons Standing Committee on Access to Information, Privacy and Ethics presented the federal government with 25 recommendations for fine-tuning *PIPEDA*. The recommendation which received the most attention was a call for mandatory data breach notification – a concept I strongly support.

In response, the federal government launched public consultations on *PIPEDA* reform late in the year, requesting input on the parameters of data breach notification and other issues.

We appreciate these consultations and look forward to seeing changes to improve *PIPEDA* – and ensure even stronger privacy protection for Canadians.

Welcoming an Assistant Commissioner

I am very pleased that Elizabeth Denham, our new Assistant Privacy Commissioner, will help lead the search for innovative solutions to the significant privacy challenges Canada will be facing in the coming years.

Before her appointment, Ms. Denham was Director of Research, Analysis and Stakeholder Relations in our Office. Previously, she had been the Director, Private Sector, in the Office of the Information and Privacy Commissioner of Alberta.

Ms. Denham's experience in developing relationships with stakeholders, her perspective formed by her work with provincial commissioners and her extensive expertise in the privacy field will undoubtedly be of enormous benefit to the OPC in the coming years. She will be responsible for *PIPEDA*, working alongside Raymond D'Aoust, Assistant Commissioner responsible for the *Privacy Act*.

A Dedicated and Expert Team

I would also like to acknowledge the very hard work of the dedicated team in my Office over this past year. Hosting a major international conference was a huge undertaking – on top of an already intense workload. I am also pleased that our Office is attracting a new generation of personal information experts.

I offer my sincere thanks to all the employees of the Office of the Privacy Commissioner for their immense contribution to protecting the privacy rights of Canadians.

Jennifer Stoddart
Privacy Commissioner of Canada

PRIVACY BY THE NUMBERS IN 2007

Average number of *PIPEDA* inquiries per month:	538
Average number of *PIPEDA* complaints received per month:	28
Average number of *PIPEDA* investigations closed per month:	33
Total investigations closed during the year:	420
Parliamentary appearances:	7
Number of bills/acts reviewed for privacy implications:	15
Research activities commissioned:	19
Speeches and presentations delivered:	92
Media requests:	474
Interviews provided:	301
News releases issued:	44
Publications distributed:	2,043
Average hits to our website per month from Canada:	39,429
Average hits to our website per month from other countries:	86,155
Average hits to our blog per month:	14,173
Legal opinions prepared:	82
Litigation decisions on *PIPEDA* cases rendered:	3
Litigation cases settled:	5
Access to Information Act requests received and closed between April 2007, when we first became subject to the legislation, and the end of the calendar year (all within prescribed timelines):	21
Privacy Act requests received and closed during the same period:	14

NEW STRATEGIC PRIORITIES

The constantly changing world of privacy issues means our Office must find ways to focus our efforts. In 2007 we identified four new strategic priorities which we believe represent some of the most significant threats to the privacy of people across Canada.

These priorities – information technology; identity management; national security; and genetic information – will help guide our policy, research and investigative work over the next three years.

Information Technology

Information technology was an obvious choice for our list because virtually every current privacy issue and privacy complaint we receive contains an IT component.

Information and communications technologies have become integral to our daily lives. Technological advances mean more and more personal information can be gathered, stored, analysed and potentially accessed from anywhere in the world.

These developments provide undeniable benefits in terms of convenience and efficiency, but also carry great risks for privacy. Governments and businesses can now collect and use personal data on a scale that was until recently unimaginable.

Our Office will continue to develop the capacity to assess the privacy impact of new technologies. We will also work to help Canadians understand and, where possible, mitigate those privacy impacts.

We demonstrated in 2007 how our Office can make a difference in this area after identifying privacy concerns stemming from the integration of street-level photography with web-based mapping technology. This type of photography involves the use of high-resolution video cameras, often affixed to vehicles as they drive along city streets. The images – including images of people who may be identified – are then made available on the Internet.

It has become something of an Internet sport to find pictures of people captured in embarrassing or personal moments – a man leaving an adult video store or young women sunbathing, for example – and then share them on websites.

Google's Street View is one of several services that have been rolled out. To date, Street View has produced photographs taken in U.S. cities. We were concerned that street level photography, as currently deployed in the U.S., may not meet the basic requirements of privacy laws here in Canada. I wrote to Google outlining these concerns and we have received assurances from Google officials that they will ensure Street View will be compliant with Canadian legislation if it is deployed in Canada.

Identity Management

The issue of identity integrity and protection stems from the fact that massive amounts of data are continually circulating.

Personal information has become a hot commodity, not only for legitimate organizations, but for criminals as well. We have seen an explosion of identity theft in recent years – a crime which carries both economic and emotional costs.

Improving personal information management practices can go a long way to reducing the possibility data will make its way into the hands of identity thieves. Our goal is to increase awareness of the importance of handling personal information with great care. Our public education efforts will be aimed at both organizations and individuals.

An important focus will be on the online world, where personal information is increasingly dispersed across commercial sites, social networks and personal blogs. People are finding the personal information they've posted online being used in ways they never imagined. In some cases, entire profiles – name, photo and other personal details – have been hijacked by impostors. We are developing tools to help people manage their online identity.

National Security

National security measures introduced in the wake of the attacks of Sept. 11, 2001 have transformed the privacy landscape in Canada and around the world.

Too often, these measures have focused on the collection and sharing of personal information with little oversight and scant consideration of privacy and other individual rights. A growing list of private-sector organizations – airlines, banks and accounting firms, for example – have been deputized to collect personal information for the state.

The way we address security needs to reflect our society's fundamental values – including the right to privacy. We must constantly ask ourselves why we accept the growing shift towards security at the expense of privacy. Is it always justified? Is it irreversible?

These are messages we will continue to press as we work to ensure that national security initiatives adequately protect privacy.

Genetic information

Advances in genetics are creating an array of new and complex challenges for privacy protection.

Interest in obtaining genetic information is increasing swiftly. Genetic testing for employment, criminal matters, research, medical care, access to insurance and to determine family relationships all raise significant and deeply sensitive privacy issues.

There's a need to increase public awareness about how genetic information can be used. We must also explore some of the new challenges for protecting privacy in a world where our genes reveal so much about us.

KEY ACCOMPLISHMENTS IN 2007

Proactively Supporting Parliament

- Appeared before parliamentary committees on issues such as identity theft and amendments to the *Canada Elections Act*.
- Worked with the Standing Committee on Access to Information, Privacy and Ethics on the statutory review of *PIPEDA*; responded to Industry Canada's consultation on *PIPEDA* review.
- Joined provincial and territorial counterparts in passing a resolution calling on the federal government to suspend its new no-fly list program until it can be overhauled to ensure strong privacy protections for Canadians.

Serving Canadians

- Responded to more than 7,500 *PIPEDA*-related inquiries.
- Investigated hundreds of privacy complaints in the public and private sectors.
- Created a blog to help build links and stimulate discussion on privacy issues of interest to Canadians.
- Began work on a social marketing campaign aimed at encouraging awareness and prompting action on children's privacy online.
- Appeared in numerous court cases in order to help develop privacy-conscious jurisprudence in Canada.

Supporting Business

- Launched an e-learning tool to help retailers ensure their privacy practices and policies meet their legal obligations and provide customers with the privacy protections guaranteed under *PIPEDA*.

- Published guidelines to help organizations take the right steps after a privacy breach, including notifying people at risk of harm after their information has been stolen, lost or mistakenly disclosed.

- Initiated a regional outreach program to extend and tailor compliance education to small and medium-sized businesses.

Global Initiatives

- Hosted the largest-ever International Conference of Data Protection and Privacy Commissioners, honouring a 2002 commitment.

- Chaired an OECD group working to enhance cooperation between data protection authorities and other privacy rights enforcement agencies around the world. OECD adopted a recommendation on cross-border cooperation which was based on the work of the volunteer group.

- Contributed to an APEC data privacy group's efforts to implement a new privacy framework for APEC member countries.

- Worked with the Standards Council of Canada on the development of international privacy standards.

- Joined the International Standards Organization (ISO) and became a member of an important ISO Working Group tasked with developing and maintaining standards and guidelines addressing security aspects of identity management, biometrics and the protection of personal data.

- Participated in the International Working Group on Data Protection in Telecommunications, which has recently focused on Internet privacy.

- Played a lead role in the creation of an international association of data protection authorities and other enforcement agencies from francophone states.

- Became a member of the Asia Pacific Privacy Authorities Forum

Other Highlights

- Prepared a submission and appeared before the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182.

- Provided research grants to eight organizations through our contributions program – bringing the total funding provided for privacy research projects under the program over the last four years to over $1 million.

- Co-hosted an Internet Privacy Symposium with the University of Ottawa's Law and Technology Group to explore new threats to online privacy, emerging trends and ways to better protect personal information in the future.

- Hosted a conference for investigators in Winnipeg in February 2007. The conference was attended by 56 investigators from our Office and 11 provincial and territorial offices.

KEY ISSUE: DATA BREACHES

Gambling with Personal Information

2007 was a year of data privacy disasters, highlighting the need for companies to recognize the value of personal information and take more care in securing it

Not so long ago, a group of executives was debating the merits of delaying an upgrade of their company's out-of-date computer security system.

One of them cautioned his colleagues in an e-mail:

"It must be a risk we are willing to take for the sake of saving money and hoping we do not get compromised."

Those words were prescient.

They were written by a vice-president at TJX – a name which has become synonymous with data breach. The e-mail was released during legal proceedings against TJX.

In fact, hackers had already broken into the international discount retailer's computer system and were busy pilfering the personal information of people who had shopped at Winners, HomeSense and other TJX-owned stores. The company's obsolete encryption technology was not up to the job of protecting this sensitive data.

TJX was one of many companies gambling with Canadians' personal information.

Too often, large corporations underestimate both the value of personal information and the risk that thieves will target it. As a result, we see deficient safeguards, lackadaisical privacy and security policies and procedures – and, of course, data spills.

The size of the worst of the data breaches we saw in 2007 was staggering.

Some 94 million debit and credit card numbers belonging to people in several countries were affected by the TJX intrusion – the largest personal information breach on record.

In a case in the United Kingdom, an official at Her Majesty's Revenue and Customs department ignored security procedures and put two discs containing the personal details of 25 million child benefit recipients into an envelope, which was then mailed through an internal post system. The discs failed to reach the addressee at another government department.

Here in Canada, a hard drive belonging to a CIBC subsidiary vanished – along with the personal information of close to half a million clients.

Of course, not all of the data compromised in these kinds of breaches winds up in the hands of criminals.

However, it is clear crooks have recognized that personal data is a goldmine. Identity theft is rampant – and lucrative.

NOTE: Information on data breaches voluntarily reported to our Office in 2007 is provided on page 39.

Businesses recognize the value of personal information to themselves – for targeted marketing campaigns, for example. Unfortunately, this perception doesn't always translate into security measures up to the job of protecting the information from criminals.

Just before the TJX breach became public, for example, Visa USA revealed that a little over a third of the very biggest retailers in that country were complying with the industry security standard. The figure for other large merchants was even worse – just 15 per cent.

We understand the picture in both the U.S. and Canada has been improving in the wake of TJX. Visa Canada has told us that virtually all major retailers were well on their way to compliance with the payment card industry data security standard.

One word – TJX – is no doubt going a long way when security experts ask senior executives for money to pay for upgrades.

All organizations must use strong security to protect personal information. It is not good enough to offer the excuse that, "We were moving as slowly as other companies."

Good security is expensive, but it is significantly less expensive than mopping up after a major data spill. Security experts have calculated that recovering from a significant data breach costs several times more than installing adequate safeguards in the first place.

Good privacy practices also go a long way to protecting personal information.

PIPEDA sets out 10 fair information principles that businesses must follow. These principles – sometimes called the "golden rules" of privacy – include such basics as seeking consent for the use of personal information; limiting the use, disclosure and retention of personal information; and using appropriate security safeguards.

The starting point for implementing these fair information principles is to critically examine the personal information being collected. Organizations should only collect personal information which is absolutely essential. After all, if you don't have this kind of information in the first place, it can't be lost or stolen.

A second critical step is to recognize the value of personal information which is collected and protect it properly.

By following this bottom-line advice, an organization should wind up with a relatively small and well-protected target.

The OPC has developed more detailed online training on how retailers can put fair information principles into practice. The e-learning course is available on our website.

Employee training is also critical to preventing data breaches. In many of the breach reports we receive from companies, the cause of the compromise is an employee's failure to follow company procedures.

For example, laptop theft is a common type of breach. We see employees leaving the office with laptops containing customers' sensitive personal information – contrary to company security policies.

Policies and procedures are only as good as the training that reinforces them.

Unfortunately, a survey of Canadian businesses conducted for our Office in 2007 found that only one third of them report having trained staff about their responsibilities under Canada's privacy laws. Larger businesses were the most likely to have provided training, with 63 per cent confirming they had done so.

Companies that have not trained employees who deal with personal information are exposing themselves to a significantly increased risk of a data breach. We hope to see more encouraging numbers the next time we conduct a survey on compliance with *PIPEDA*.

During 2007, we developed breach guidelines in consultation with industry and civil society groups. These guidelines outline key steps organizations should take after a breach, such as containing the breach, evaluating the associated risks, notifying the

people affected and preventing future breaches. The guidelines have also been adopted as a model in New Zealand. The Australian Privacy Commissioner is also proposing to adopt the guidelines.

We have been clear that voluntary guidelines do not take away from the need for breach notification legislation.

In fact, we have been urging the federal government to amend *PIPEDA* to add a notification requirement.

We believe mandatory notification will help protect personal information in two very important ways. First, it will provide an incentive for organizations to take privacy and security more seriously; and, second, it will give people the information they need to take measures to protect themselves against identity theft or other forms of fraud.

It is clear that people want this kind of information.

More than three-quarters of Canadians (77 per cent) believe government agencies and affected individuals should be notified if sensitive personal information is compromised as a result of a breach, according to a 2007 poll commissioned for our Office. Meanwhile, 66 per cent wanted to be notified if non-sensitive information was compromised.

One of *PIPEDA*'s tenets is that individuals should have control over their personal information. Breach notification offers people a choice. Individuals can decide for themselves how to respond to a breach. One person could decide that it would be a good idea to check her credit report more often. Another person may feel no action is warranted.

What's important is that the individual retains control.

Our Office believes breach notification is an important part of a comprehensive approach to reducing data breaches.

The TJX debacle, along with headlines about missing computer discs and hard drives as well as other lost data are a wake-up call for all organizations that collect personal information. These incidents starkly illustrate the need for companies to make both privacy and security a top priority.

When Canadians entrust their personal information to an organization, they expect – and the law requires – that this information will be well protected.

A DATA BREACH INVESTIGATION

THE TJX CASE: HOW HACKERS GAINED ACCESS TO 94 MILLION CREDIT AND DEBIT CARDS

The story of what has been called the "largest-ever online burglary" began one summer day in 2005.

It's believed that thieves armed with an antenna and a laptop computer and some specialized software settled in outside a Marshall's in Miami and broke into the store's poorly protected wireless local area networks.

Once inside, they tapped their way into computer servers that process and store customer information from transactions for hundreds of stores owned by discount retail giant TJX, including Winners and HomeSense stores in Canada.

For the next year and a half, the thieves plundered the TJX computer system.

They ultimately gained access to at least 94 million credit and debit cards as well as the names, addresses and driver's licence numbers of people who had returned merchandise at TJX stores.

The crime wasn't particularly sophisticated. Detailed instructions on cracking the encryption protocol used to guard TJX's wireless networks were readily available on the Internet.

It had been well established for some time that this encryption protocol – Wired Equivalent Privacy, or WEP – did not provide adequate network protection because it could be easily bypassed by someone with a bit of computer savvy.

TJX was aware of the concerns about its encryption protocol and was in the process of converting to a stronger technology at the time of the breach. In our view, the conversion was not done within a reasonable period of time.

The OPC's investigation, conducted jointly with Alberta Information and Privacy Commissioner Frank Work, concluded TJX did not comply with either federal or Alberta privacy laws.

KEY FAILINGS

The investigation highlighted a few critical failings:

1. TJX collected too much information and kept it for far too long.

The company should not have collected driver's licence and other identification numbers when merchandise was returned without a receipt. A driver's licence is proof someone is authorized to drive a car – not an identifier for analysing shopping-return habits. As well, a driver's license number is invaluable to identity thieves.

In response to our concerns, TJX proposed an innovative new process to deal with fraudulent returns. Information such as a driver's licence number will still be requested and keyed into the point-of-sale system, however, it will instantly be converted into a unique identifying number. This will allow tracking of unreceipted merchandise returns without keeping original identification numbers.

Prior to the breach, identification information collected from people returning goods was kept indefinitely.

Credit card information was also retained for a long time – some of the stolen information involved transactions dating back several years.

2. TJX failed to update its security systems in a timely way.

TJX's process for converting to an up-to-date encryption protocol took two years to complete, during which time the breaches occurred. As a result, the company did not adhere to the requirements of the payment card industry's data security standard.

3. TJX did not adequately monitor its system for signs of an intrusion.

The thieves were able to continue stealing data for a year and a half before TJX learned that suspicious software had been detected on a portion of its computer system. With proper monitoring, TJX should have detected the incident sooner.

LOOKING AHEAD

TJX has complied with all of the OPC's recommendations on improving security, monitoring and other personal information management issues.

A year after it was discovered, the intrusion continued to have an impact.

Some legal proceedings against the company were ongoing. Investigations by the U.S. Federal Trade Commission, as well as an investigation by the Massachusetts Attorney General on behalf of a group of more than 30 state Attorneys General were continuing.

It's unclear how much the breach will wind up costing the company – but the total bill will certainly be in the hundreds of millions of dollars.

By the end of 2007, TJX had named a chief privacy officer and was advertising for a privacy director to develop and implement a comprehensive information privacy and security program.

How our Office Helps Organizations Prevent Breaches

- We launched an online learning tool offering step-by-step guidance for retailers on how to protect customer information and meet *PIPEDA* obligations.
- We have published various online and printed materials on how businesses can safeguard personal information, including the booklet, *Your Privacy Responsibilities: A Guide for Businesses and Organizations*.
- We developed voluntary data breach guidelines in consultation with industry and consumer groups.
- We advise and assist organizations with their breach response actions, including advice on notification of affected individuals.
- We continue to press the federal government to make breach notification mandatory under *PIPEDA*, a move we believe would encourage businesses to improve security measures.
- We conduct audits of the personal information management practices of organizations covered by *PIPEDA* if we have reasonable grounds to believe the organization is contravening the legislation.
- Our investigations into privacy complaints help identify steps that businesses can take to better protect personal information.

IMPROVING *PIPEDA*: A REVIEW OF OUR PRIVATE-SECTOR PRIVACY LAW

A Parliamentary committee completed a mandatory review of* PIPEDA *in 2007 – an important step towards strengthening privacy protections for Canadians

PIPEDA, along with its public-sector sister legislation, the *Privacy Act*, and provincial legislation provide the foundation for privacy protection in Canada.

The privacy landscape is constantly changing – and our laws need to keep up.

Consider how much the world has changed since a decade ago, when we began talking about what a private-sector privacy law in Canada should look like.

Back then, the Information Highway was a catchphrase; now it is a reality. The trickle of personal information crossing borders has become a torrent. Meanwhile, emerging technologies such as location tracking devices are raising new risks for privacy. And the fallout from 9-11 means governments are asking businesses for more information about our day-to-day lives.

It is critically important that *PIPEDA* remains capable of addressing all of these new challenges. The desperately out-of-date *Privacy Act* – left unchanged for a quarter-century – is evidence of the dangers of failing to modernize privacy legislation.

Fortunately, *PIPEDA*'s architects recognized the importance of regular updating. The legislation requires Parliament to review the part of the Act dealing with data protection every five years.

The House of Commons Standing Committee on Access to Information, Privacy and Ethics took on the task of conducting the first five-year review, beginning their work in the summer of 2006.

Committee members wrapped up public hearings on a wide range of issues in February 2007. They heard from 67 witnesses and considered 34 submissions from individual Canadians, private sector associations, privacy advocates and the Privacy Commissioner.

Overall, we feel the legislation has been well-received, that it is working reasonably well, and that we have most of the tools and powers we need to enforce the Act. The legislation offers Canadians strong privacy protections in the commercial sphere.

In our submissions to the committee, we noted the legislation has only been fully in force since 2004. While experience to date has been instructive, more time is needed before any major changes are made. The full impact of complex legislation takes time to unfold.

That said, some adjustments would be welcome to ensure privacy protections evolve with new trends and technologies.

In May 2007, the committee presented its final report, which included 25 recommendations for the government's consideration or further discussion.

Suggested amendments touched on a broad range of issues, including: business contact information; work product information such as physicians' prescribing patterns; employee-employer relationships; investigative bodies; witness statements; law enforcement and national security; individual or family exceptions; disclosure of personal information before transfer of businesses; added protection for minors; and mandatory data breach notification.

We deeply appreciate the effort of the Parliamentarians, researchers, organizations and citizens who contributed their experiences and expertise to the review process.

The Government of Canada tabled its response in October. In our view, a very significant element of the response was the acknowledgement that an increasingly global response is required to meet privacy threats. The data-processing industry has become increasingly international, and so too have data security risks.

Inter-governmental cooperation, information sharing between jurisdictions and attention to trends emerging in other parts of the world have all become vital strategic considerations as we work to protect the privacy of Canadians.

In October, Industry Canada issued a consultation notice seeking public input on how best to implement certain provisions of the Government response. Views on data breach notification provisions, and the concepts of "work product" and "lawful authority," were

given particular emphasis. As well, Industry Canada sought views on witness statements, minors' consent and investigative bodies.

As part of this round of consultations, the Privacy Commissioner asked the Minister of Industry to closely consider five issues which will significantly impact our work in the years to come:

- We continued to promote a 'contextual' approach to work product information.

- We supported a requirement for breach notification, and stressed the need for clear triggers and thresholds in any new *PIPEDA* provisions.

- We asked that the possibility of *PIPEDA* amendments governing access to documents covered by solicitor-client privilege be left open, pending a decision from the Supreme Court of Canada in *Privacy Commissioner of Canada v. Blood Tribe Department of Health*.

- We urged that any new provisions on privacy in the employer-employee context take Alberta and Quebec legislation into consideration in order to better recognize that the unequal bargaining power in employment relationships means employees may not feel in a position to withhold consent for the collection of their personal information. Our Office sees merit in Alberta's approach of a reasonable purposes-based employee code, combined with the notion in the Quebec Civil Code, which obligates employers to respect the dignity of workers.

- We asked for greater flexibility to refuse and/or discontinue complaints if their investigation would serve no useful purpose or are not in the public interest, thereby allowing us to focus investigative resources on issues of broader systemic interest.

The deadline for comments to Industry Canada was mid-January 2008. The department received 67 submissions and was reviewing those in early 2008.

We look forward to the next stage of the legislation's review and the important dialogue it serves to generate between privacy advocates, regulators, industry and Parliamentarians.

COMPLAINT INVESTIGATIONS AND INQUIRIES

As Canadians become more knowledgeable about privacy issues, organizations are being challenged to fulfill their responsibilities with respect to personal information. In particular, consumers are increasingly aware of the serious ramifications of identity theft and, as a result, are more insistent that companies meet their obligations when collecting personal information.

People do not want sensitive information such as driver's licence numbers collected and retained without a legitimate reason, nor do they want their credit card numbers and expiry dates printed on receipts.

Many companies do take their privacy responsibilities seriously. But it is also clear – both from the complaints we receive and from the data breaches voluntarily reported to our Office – that many organizations could do more.

Businesses that handle personal information need to update their privacy policies and practices regularly. They must keep their data security up-to-date. And, they must also ensure that employees are kept informed of changes and receive regular training.

Inquiries

Our Inquiries Unit responds to questions from individual Canadians, government institutions, private sector organizations and the legal community. Inquiries officers provide information on a broad range of issues under both *PIPEDA* and the *Privacy Act*.

We received 7,636 *PIPEDA*-related inquiries in 2007, a substantial increase from the 6,050 received a year earlier. We have noticed a marked increase in interest concerning identity theft and social networking sites such as Facebook.

Complaints

We received 350 new *PIPEDA* complaints during 2007. We received 424 complaints in 2006; 400 in 2005; and 723 in 2004.

The year-over-year decrease in complaints is, in part, the result of a streamlined complaint-acceptance process introduced in 2007. Under this process, when an individual brings a complaint which is factually similar to complaints already under investigation, we inform the individual that the issue is already under investigation and will be addressed by the Commissioner in her findings. This approach is also used with complaints for which a finding has already been issued on a similar case.

In such cases, we offer complainants the option of referring to similar findings as a way to resolve the particular issues they may have with an organization.

By way of example, we currently have underway five investigations concerning drug testing for employment, while an additional 27 people agreed not to file official complaints about the same issue.

NOTE: Detailed information about complaints as well as findings and other dispositions are included in Appendix 1 of this report.

In some instances, although an individual's situation may be similar to that of another complaint, the facts may vary enough to warrant a full investigation.

Another possible reason for the decline in complaints is that organizations may be becoming more knowledgeable about their privacy obligations. Moreover, many now have internal complaint-resolution processes in place in order to resolve privacy issues with their customers. Our Inquiries Unit also advises individuals to attempt to resolve their disputes with organizations before they file a formal complaint with our Office.

Complaints by Sector

As has been the case since 2004, when *PIPEDA* was fully implemented, the financial institutions sector was the sector most often targeted in our 2007 complaints. We received 105 complaints involving financial institutions in 2007. This represented almost a third of total *PIPEDA* complaints, which is similar to the proportion of complaints involving this sector over the last few years.

As in past years, the other major sectors for complaints were telecommunications, insurance, sales and transportation. We have, however, seen a decrease in complaints involving companies in these industries over the last few years.

We have seen a steady increase in complaints about professionals and the accommodation sector. However, the number of complaints against these sectors remains small in comparison to others.

With respect to complaints involving the insurance industry, we are seeing more issues involving the covert collection of personal information by private investigation firms.

PIPEDA includes provisions for designating a private investigation company as a "private investigative body" which carries specific responsibilities under the legislation.

We understand there may be a need for covert collection of personal information where other less privacy invasive efforts have failed. However, a key concern about this type of investigation is the risk that innocent third parties may be captured on covert video surveillance tapes. Few of us would like to be videotaped in a bathrobe on our front step simply because we happen to live next to someone under suspicion of insurance fraud.

We are working with both insurance and private investigation organizations to find a balance between their need to conduct their business and individuals' right to privacy. Insurance companies and their contractors should conduct covert surveillance only as a last resort. Businesses should ensure that the decision to conduct covert surveillance is made at a senior level.

Part of the solution may be for insurance companies to establish detailed contracts with investigative firms to ensure that the parameters of surveillance are clearly spelled out. As well, investigative firms need to develop specific polices regarding surveillance, including the videotaping of third parties.

Complaint Trends

Our Office closed 420 complaints in 2007. Of these, the vast majority (39 per cent) concerned use and disclosure issues, a trend which has continued from previous years. Also consistent with previous years, other common types of complaints were collection (19 per cent) and access (16 per cent).

Almost a third (30 per cent) of complaints closed in 2007 were settled during the course of an investigation. These are complaints for which the Office has negotiated an outcome which is satisfactory to all parties and no finding is issued. In 2004, we defined the "settled" category in order to track this outcome.

Closed 2007 Complaints By Finding

	Percentage
Settled	30
Discontinued	21
Not well-founded	15
Well-founded Resolved	15
Resolved	10
Early Resolution	3
No jurisdiction	3
Well-founded	2

In 2004, 40 per cent of our cases were settled. Since then, however, this percentage has steadily declined. The trend may be a reflection of the fact we are seeing more complex cases where an extensive investigation is required.

A significant number of closed cases were discontinued (21 per cent) by the complainant or our Office. This represents an increase over previous years. As in the past, some complainants decide for personal reasons to abandon their complaints. Others do not proceed because they have resolved the issue with the organization before the active investigation has begun. Still others drop their complaints because of lengthy treatment times. Sometimes our Office must discontinue complaints because complainants have not provided us with additional details which we have requested and are necessary to complete an investigation.

Following the completion of investigations, 15 per cent of all complaints were found to be not well-founded and that the organization had complied with *PIPEDA*. Another 15 per cent of complaints were well-founded and resolved. In other words, there was a violation of *PIPEDA*, but the respondent organization agreed to comply with our recommendations.

The determination of whether a fully investigated complaint is well-founded or is well-founded and resolved depends on the level of cooperation we receive from the respondent organization.

A finding that a complaint is well-founded is reached when the Commissioner is of the view there has likely been a contravention of *PIPEDA*. She makes recommendations in a preliminary report with respect to corrective actions the respondent should take. The respondent has 30 days to reply to the preliminary report.

Since this new preliminary report process was established in 2006, it has become an effective means of ensuring that organizations remain accountable.

If the respondent complies with the recommendations, a well-founded and resolved finding is usually reached. In cases where the respondent does not fully comply, the complaint is deemed to be well-founded.

We included preliminary reports in 38 closed complaints in 2007. Of these, 34 organizations complied with the Commissioner's recommendations.

In 2007, only four organizations chose not to implement our recommendations at the conclusion of an investigation. The Commissioner has consistently sought to have her recommendations upheld by the Federal Court in such cases.

As we prepared to publish this annual report, all four organizations that initially declined to adopt our recommendations had finally agreed to comply, either before or after we referred the matters to litigation.

Treatment Times

The average treatment time (calculated from the date the complaint is received to the date the report of finding is mailed) for *PIPEDA* complaints closed in 2007 was 15.7 months – approximately the same as in 2006.

On a more positive note, there were only 44 files in abeyance – unassigned because no investigator is available – at the end of 2007. That's substantially lower than the 76 files in abeyance the previous year.

We are committed to reducing treatment times and eliminating the backlog of cases – without compromising quality. Our Office is actively pursuing innovative steps to that end.

Changes implemented in recent years, including the hiring and training of new staff, have helped revitalize our investigations unit. We plan to further improve service delivery by:

- Continuing to hire more staff;
- Increased automation and the use of technology in processing files; and
- Streamlining our investigation processes.

All of this work is essential to sustaining Canadians' renewed trust in our Office and in our ability to protect their privacy rights. Fair, prompt and effective treatment of complaints also provides a key opportunity for educating both the private sector and individual Canadians.

Commissioner-Initiated Complaints

The Commissioner uses her powers to launch complaints on a wide range of privacy issues. Following are summaries of two significant Commissioner-initiated complaints closed in 2007:

SWIFT Case: Transborder data flows raise new privacy risks

The Privacy Commissioner launched an investigation in August 2006 following newspaper reports that the Society for Worldwide Interbank Financial Telecommunication (SWIFT) had disclosed tens of thousands of records containing personal information to the U.S. Department of the Treasury.

The disclosed materials included personal information originating from, or transferred to Canadian financial institutions. This likely included such information as names, addresses, account numbers and amounts of transfers.

In Canada, SWIFT collects personal information from, and discloses it to, Canadian banks for cross-border payments, securities clearing and settlement, and treasury and trade services. Its presence in Canada is significant. The vast majority of international transfers involving personal information flowing to and from Canadian financial institutions use SWIFT's network.

Following an investigation, the Commissioner concluded in April 2007 that SWIFT was subject to *PIPEDA*, but had not contravened it.

The Commissioner noted that the legislation allows organizations such as SWIFT to abide by the legitimate laws of other countries in which it operates. She also noted that *PIPEDA*'s exception to knowledge or consent applies to an organization disclosing personal information when a lawful subpoena is issued.

In this case, the U.S. Department of the Treasury began issuing subpoenas to SWIFT for data held in its U.S.-based operating centre following the terrorist attacks of Sept. 11, 2001.

In her findings, the Commissioner noted that if U.S. authorities need to obtain information about financial transactions with a Canadian component, they should be encouraged to use existing information mechanisms that have some degree of transparency and built-in privacy protections, such as Canadian anti-money laundering and anti-terrorism financing mechanisms.

Telecommunications Case: Highlighting the importance of authentication

Assistant Privacy Commissioner Raymond D'Aoust initiated complaints against three Canadian telecommunications companies following the publication of a November

2005 article in *Maclean's* describing how the magazine had obtained the Privacy Commissioner's telephone records.

The records were purchased from a U.S. data broker, Locatecell.com, which had obtained them from Bell, TELUS Mobility and Fido.

The investigation revealed that Locatecell.com had used "social engineering" to persuade phone company customer service representatives to divulge confidential information, either in the specific instances alleged and/or subsequent test cases. Social engineering involves manipulating people into divulging personal information, for example, by pretexting – pretending to be someone authorized to obtain the information.

The Assistant Commissioner concluded that the companies' authentication procedures and staff training were not sufficient to adequately protect customer information or meet *PIPEDA* requirements.

He was also concerned that the companies had not done enough to alert employees about the tactics used by data brokers – even though concerns had already been raised by incidents in the United States.

Although the Assistant Commissioner was pleased that all three companies revised their customer authentication procedures shortly after the disclosures came to light, he recommended further changes to staff training, procedures on authentication and disclosure of personal information.

The companies implemented all of these measures except one, for which they proposed other actions which the Assistant Commissioner found acceptable. As a result, he found the complaints well-founded and resolved.

The Assistant Commissioner noted that organizations must adapt their personal information management policies and practices as threats to personal information continue to emerge and evolve.

Initially, the Assistant Commissioner also opened a complaint against Locatecell.com., however, preliminary results of our inquiries revealed we lacked jurisdiction to continue the investigation.

Following these incidents and legal actions against data brokers in the United States, broker activities have either stopped or been drastically curtailed. Many broker websites are unavailable, and the Locatecell.com site has been inoperative for some time.

CASES OF INTEREST

The following represent a sample of cases we worked on in 2007 which have a systemic significance for privacy issues in Canada.

Court decision prompts cross-border investigation

A Federal Court decision in February 2007 set aside the Privacy Commissioner's decision that she lacked jurisdiction under *PIPEDA* to investigate a complaint against a U.S.-based data broker, Accusearch Inc., operating as Abika.com.

As a result of this decision, our Office is conducting an investigation of a complaint filed by an individual against Accusearch. As part of our investigation, we have contacted the U.S. Federal Trade Commission, and are actively discussing how we can work jointly on issues pertaining to Accusearch.

Credit card number printed on airline ticket

When a travel agency customer purchased an airline ticket, he was upset to discover that his credit card information had been transferred to a travel wholesaler and that the full card number and expiry date were printed on his ticket.

The Commissioner recommended that the travel agent better inform customers of the fact their personal information would be transferred to wholesalers.

As well, the Commissioner recommended that the agency confirm the wholesaler's personal information handling practices, noting that – although there was a related contract between the two parties – the wholesaler was reluctant to reveal its practices.

The agency later informed our Office that it would no longer conduct business with the wholesaler.

Until the issuing of paper tickets ceased altogether (in December 2007), the Commissioner recommended that the agency explain to customers that credit card information would appear on paper tickets. Additionally, it must offer them the option of an e-ticket, which does not contain this information.

Insurance officer discloses information without proper consent

An individual complained that a medical insurance benefits administrator inappropriately disclosed sensitive personal information to his employer, despite the fact he had signed a limited consent form for information disclosure.

When the individual applied for long-term disability benefits, he had negotiated a restricted consent agreement with the insurance company adjudicator, with the express purpose of restricting the insurer's right to transfer medical information to his employer.

Months later, an insurance rehabilitation officer retained by his employer thought she had the complainant's verbal consent to tell his employer that he was ready to return to work.

In doing so, she e-mailed to his employer excerpts of a medical specialist's report – even though the complainant had reminded her of the limited consent instructions.

The Privacy Commissioner concluded the disclosure was inappropriate and written consent ought to have been obtained. The Commissioner recommended that the company update its policies and training. The company followed these recommendations.

Telecommunications company fails to obtain consent to record calls

An individual complained that a telecommunications company was not obtaining proper consent before recording its outgoing calls.

The company had called the complainant's mother, but had not informed her that the call was being recorded. The company's policy required employees to notify individuals of the recording of incoming calls, but not outgoing calls.

According to the company, a statement in its written privacy policy was a sufficient means for obtaining consent for the recording of outgoing calls; however, the Privacy Commissioner disagreed.

She recommended the company inform customers at the beginning of each outgoing marketing call that the conversation would be recorded or otherwise monitored. Customers should also be informed of the reason for doing so.

The telecommunications company agreed to implement the recommendations.

TV station takes steps to secretly record employee calls

A union representing employees of a television station in a small community alleged that a manager had installed telephone-call recording equipment at a customer service representative's work station and had taped her telephone conversations without her knowledge and consent.

The investigation confirmed the allegation. We retrieved a recorded conversation between the employee and her husband from a file in the complainant's computer. The complainant told us she had not been aware that the call was being recorded.

When questioned, the employer claimed the equipment was not yet working and that it had been installed on a test basis, with the intent of recording conversations in case of a billing dispute and also to deter abusive customers.

The Assistant Commissioner recommended that, since the station intended to install equipment at all customer service representatives' work stations, it must inform employees of its plans and their purpose beforehand. It was also required to inform customers that their calls may be recorded and why this was being done.

The complaint was considered well-founded and resolved. The station ultimately decided not to record calls.

Contest rules adequately warned about sharing of e-mail addresses

A subscriber to a company's e-newsletter entered its contest to win a vacation for four people. He provided e-mail addresses of other individuals so that he could receive additional contest entries.

However, he was dismayed when he discovered that the e-mails the company sent to those other individuals were designed to appear as though they came from him. In particular, he was upset that his ex-wife had received an email in which he purportedly suggested the two of them travel together if he won the contest.

He complained his name had been used in the e-mails without his consent.

The Assistant Privacy Commissioner concluded the complaint was not well-founded. The contest rules and wording were clear that e-mail messages to referrals would be personalized as though the contestant had sent them. Given that the prize was a trip for

four, she thought it reasonable to expect the message could include a suggestion that the subscriber and e-mail recipient travel together.

Incident Investigations

Our Office also conducts investigations of incidents that relate to possible contraventions of *PIPEDA*. Reports of incidents are received through self-reporting by organizations; media reports on possible breaches; and information received from individuals who would like an issue to be addressed, but are not necessarily directly affected.

Examples of incidents include issues such at credit card receipts found in dumpsters or reports of information breaches on websites.

When an incident comes to our attention, we work with the responsible organization to correct any deficiencies and resolve outstanding matters such as notifying affected customers; retrieving information; and ensuring appropriate safeguards are implemented.

In 2007, we conducted 12 investigations into incidents brought to our attention from a source other than the organization directly involved in the incident.

Self-reported Data Breaches

Despite the fact that privacy legislation has been in place for a number of years, not all organizations have clear policies and procedures regarding data breaches. That said, we believe there is a heightened awareness of the need to alert our Office of privacy breaches and also to notify affected customers – in part stemming from the development and publication of our breach guidelines.

Organizations voluntarily reported 34 breaches to us in 2007, up from 20 reports the previous year. The self-reported data breaches in 2007 compromised the personal information of some 50,000 people.

Although we began to see reports of breaches from different sectors, including research groups and advertising companies, the bulk of these reports continued to flow from the banking, telecommunications and retail industries.

Of particular note is the fact that half of the breaches reported to us related to electronically stored data – often customer information stored on laptop computers that had been stolen. As well, we found that almost nine in 10 people affected by a self-reported breach were put at risk because their personal information was held in an

electronic format that was either not secured or lacked adequate protection mechanisms such as firewalls and encryption.

We were pleased to note that organizations voluntarily reporting to us did so in a timely way – often within a day or two of the incident. Prompt notification helps us in preparing for media inquiries or complaints that follow notification of affected individuals. Self-reporting also allows us to gather statistics and educate organizations and the public on the causes of data breaches as well as recommended preventive measures.

Brief descriptions of some of the breaches reported to our Office in 2007:

- A laptop being used by the employee of a firm under contract to a financial institution was stolen from the employee's home. The laptop contained the personal information of several hundred employees, but was not considered sensitive. Both the financial institution and the firm under contract had appropriate controls in place to protect personal information, but the employee had not followed them. As a result of this incident, the institution implemented additional controls such as encryption software.

- A laptop containing customer records was stolen from a vehicle belonging to a financial services company employee. More than half of these records included social insurance and account numbers. The company notified individuals and placed alerts on the accounts of affected customers.

- The laptop of an employee of an agency promoting a casino event was stolen from a car. The laptop contained a password-protected database of information on some event participants, but the data was not encrypted. The personal information included participants' names and ages, contact information, driver's licence numbers and, in one case, passport and health card numbers. Following the incident, the agency notified affected individuals and offered credit monitoring. It also introduced several security measures, such as encryption software on laptops and also reminded employees of security policies and procedures. The employee responsible for the breach was relieved of his duties.

We hope the growing awareness about the need to alert our Office and affected individuals about privacy breaches will soon translate into more effective security measures. We continue to urge individuals and organizations to take basic data security precautions such as:

- Limit the amount of personal information collected, used and carried on electronic devices;

- Never leave a laptop unattended where it could be stolen;
- Use technologies which enhance security and privacy such as data encryption and anonymizing services;
- Use hard-to-crack passwords;
- Avoid automatic login features which save user names and passwords; and
- Ensure that personal information is completely overwritten – not just deleted – from a hard drive before discarding or selling a computer.

By following these steps, organizations can significantly reduce the risk that the personal information they hold will be compromised.

AUDIT AND REVIEW

Audits are one of the compliance tools provided under *PIPEDA*. The Privacy Commissioner has the power to audit an organization's personal information practices where she has reasonable grounds to believe there is non-compliance with the Act.

Once an audit is initiated under *PIPEDA*, the auditor has the delegated authority to receive evidence from witnesses; may enter premises at any reasonable time; and may examine or obtain copies of records found on the premises. Where necessary, the Privacy Commissioner may compel individuals to provide evidence.

After an audit is complete, we provide the organization with a report on our findings and any recommendations the Commissioner considers appropriate. The report may be disclosed in the public interest.

Our Office also conducts audits of federal government institutions subject to the *Privacy Act*.

The goal of audits – both in the private and public sector – is to promote accountability and compliance with applicable legislation, policies and standards, and also to contribute to the improvement of privacy systems and practices.

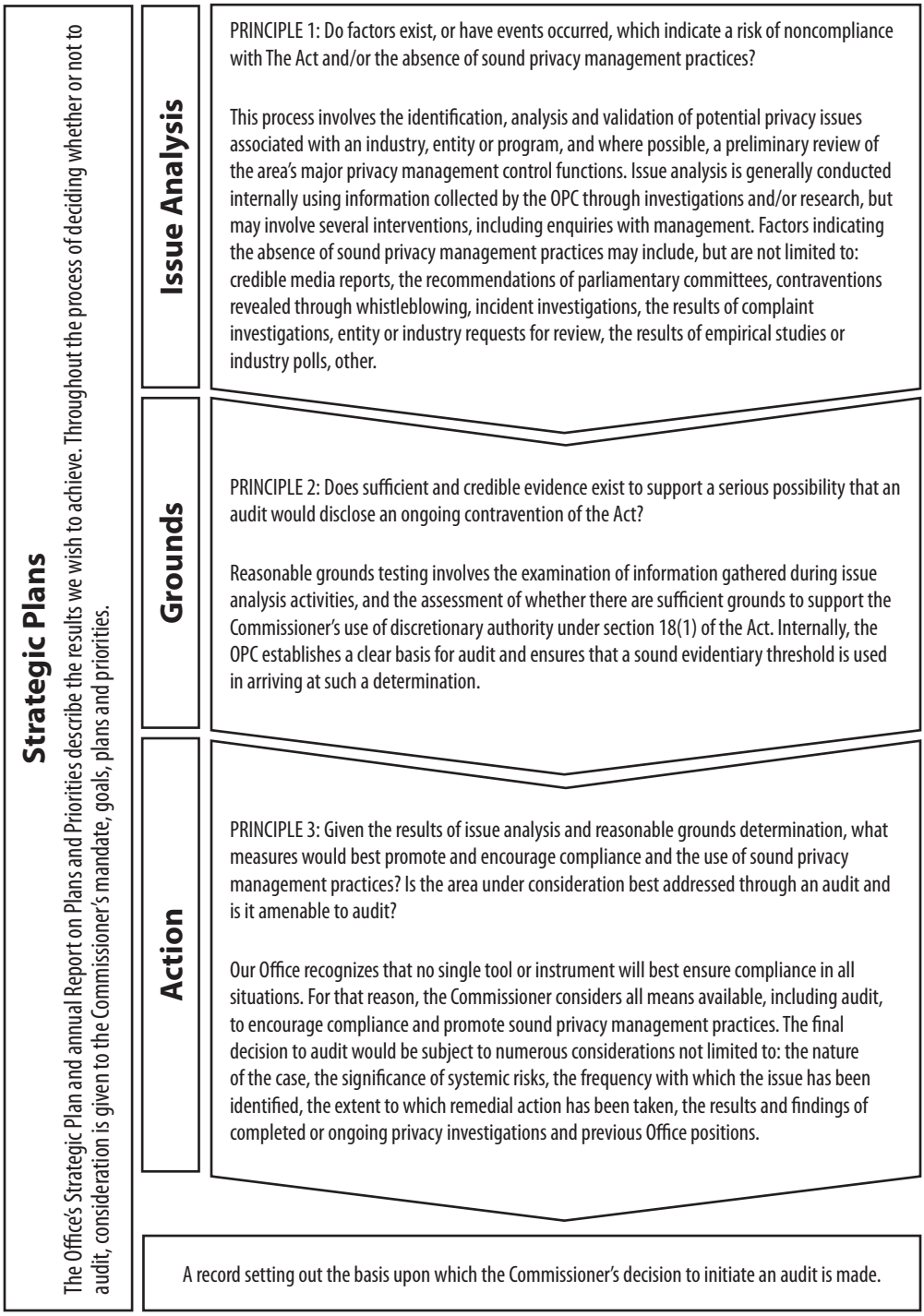
A framework for initiating audits under *PIPEDA*

One of the most frequently asked questions from organizations subject to *PIPEDA* might be: How do you decide whether or not to conduct an audit?

A decision to audit or not to audit is made on a case by case basis. To conduct an audit, the law requires the Commissioner to have reasonable grounds that there is non-compliance with the Act.

In 2007, we developed a framework for initiating audits which provides some insight into the audit selection process.

How do we decide whether or not to conduct an audit under *PIPEDA*



Audits of Equifax and TransUnion

The Privacy Commissioner concluded concurrent audits of the online identification and authentication systems of credit reporting bureaus Equifax Canada and TransUnion.

Equifax initiated legal proceedings challenging the existence of reasonable grounds justifying the Privacy Commissioner's decision to audit. Notwithstanding the position maintained by Equifax throughout the process that the audit was not based on reasonable grounds, the audit was concluded. A report was provided to Equifax and no further steps were required to be taken by Equifax with regard to this audit.

TransUnion also took the position that the Commissioner lacked reasonable grounds, but chose not to take legal action. As was the case in the audit of Equifax, a report was provided to TransUnion and no further steps were required to be taken by TransUnion with regard to this audit.

Self–assessment tool

Our Office is preparing a tool to assist organizations in assessing their compliance with *PIPEDA* and its fair information principles. This tool will help organizations diagnose problems with their privacy systems and practices.

We are seeking comments on this new self-assessment tool from a number of chief privacy officers of large businesses; academics; leaders in management development and training; as well as business and professional associations.

We expect to have a final version available for medium- and large-sized organizations in 2008.

IN THE COURTS

The Privacy Commissioner may initiate 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.

Under section 14 of *PIPEDA*, a complainant or the Privacy Commissioner may, in certain circumstances, apply to the Federal Court for a hearing in respect of any matter referred to in the Commissioner's report.

Section 15 also 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. This section 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.

Since we reported on the status of ongoing court cases in our 2006 *PIPEDA* annual report, new applications have been filed and some ongoing litigation has been settled. These new developments are discussed 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

In 2007, a number of court applications filed against organizations were settled prior to being heard and determined by the Federal Court.

X. v. ING Canada Inc.
Federal Court File No. T-1283-07

A complainant brought an application for judicial review under section 18.1 of the *Federal Courts Act*. The OPC initiated a mediation process, and following a negotiated settlement, the application was discontinued by the complainant.

X. v. Brampton Flying Club
Federal Court File No. T-192-05

A complainant filed an application under section 14 regarding allegations that the Brampton Flying Club failed to provide access to his personal information within 30 days of his written request and tried to charge him an unreasonable amount to answer his request. This case was settled by the parties in January 2007.

X. v. Laidlaw Transit Ltd.
Federal Court File No. T-684-07

An individual filed a section 14 application challenging a form of workplace surveillance that Laidlaw Transit Ltd. had undertaken. The OPC helped mediate the dispute. The individual discontinued the application and the parties reached a settlement.

X. v. The Bank of Nova Scotia
Federal Court File No. T-2126-05

This case concerned a complaint that one or more employees of the Bank of Nova Scotia obtained personal information without consent and shared the information with a third party. The application filed by the complainant in the Federal Court was discontinued by the complainant and settled between the parties.

Privacy Commissioner of Canada v. Air Canada
Federal Court File No. T-342-07

The Privacy Commissioner filed a Federal Court application against Air Canada to have its recommendations implemented in a case dealing with the extent of personal health information collected by the organization to satisfy itself of an employee's ability to return to work.

The parties settled the dispute. Air Canada implemented the Commissioner's recommendations to our satisfaction.

Ongoing Litigation

Ongoing litigation continued in respect of judicial review applications under section 18.1 of the *Federal Courts Act* and complainant-initiated court applications filed under section 14 of *PIPEDA* in which the OPC was involved as an added party or as an intervener.

In one noteworthy case, State Farm Mutual Automobile Insurance Company questioned the Privacy Commissioner's jurisdiction to investigate a refusal to provide access to personal information and power to compel the production of documents during the course of an investigation.

In July 2007, State Farm filed an application in the Court of Queen's Bench of New Brunswick for a declaration that:

- *PIPEDA* did not apply to the disclosure of personal information sought by an individual complainant;
- *PIPEDA* was enacted outside the powers allotted to the federal Parliament;
- The Privacy Commissioner did not have the authority to investigate the complaint in question; and
- The Privacy Commissioner did not have the authority to compel production of the information sought.

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 on the basis that the Federal Court was the more appropriate forum to determine the application, which involved questions of constitutional validity and the judicial review of the Privacy Commissioner's authority. State Farm's appeal from this decision will be heard in early 2008. Further developments will be reported in our next annual report.

Other significant court decisions rendered in 2007 are set out below.

***Judicial review applications under section 18.1 of the* Federal Courts Act**
Blood Tribe Department of Health v. The Privacy Commissioner of Canada et al.
Supreme Court of Canada File No. 31755

Details of this ongoing matter have been reported in our last three annual reports. At issue is solicitor-client privilege and our ability to obtain the information we need to conduct our investigations. The final outcome – yet to come – will have profound implications for how we conduct our investigations.

The case began when a woman dismissed from her job with the Blood Tribe Department of Health asked for her personnel file and was denied access.

The woman filed a complaint with our Office. As part of our investigation, we asked for a copy of the woman's personnel file. The Blood Tribe Department of Health provided some records, but claimed solicitor-client privilege over other documents and refused to provide them.

Our position is that we need these documents in order to independently verify the claim that personal information being sought by a complainant is exempt from disclosure on the basis that it is information over which a claim of solicitor-client privilege has been made.

We issued an order that the organization produce the records. The Blood Tribe Department of Health went to court to challenge the Privacy Commissioner's jurisdiction to issue this order – bringing the investigation to a halt.

The Federal Court dismissed the Blood Tribe Department of Health's judicial review application.

However, the Federal Court of Appeal set aside the Privacy Commissioner's order, finding that language in *PIPEDA* is not clear enough to grant the Commissioner specific power to order the production of solicitor-client privileged documents. The Court proposed that we apply on a case-by-case basis to the Federal Court to examine claims of solicitor-client privilege in the context of complaints involving refused access to personal information.

We appealed from that decision to the Supreme Court of Canada, which scheduled a hearing for February 21, 2008.

The Privacy Commissioner has said she plans to revisit the issue with the Minister of Industry should amendments to *PIPEDA* be needed as a result of the Supreme Court decision.

X. v. Accusearch Inc., dba Abika.com et al
Federal Court File No. T–2228–05

An individual filed a judicial review application seeking an order quashing or setting aside the Assistant Privacy Commissioner's decision that she lacked jurisdiction to investigate a complaint against Accusearch Inc., a U.S.-based organization operating as Abika.com.

Note: This case was also reported in our 2006 annual report.

The individual sought to review the Assistant Privacy Commissioner's position that she did not have jurisdiction to investigate. In February 2007, the Federal Court allowed the application on the grounds that the Assistant Commissioner did have jurisdiction to investigate the transborder flow of personal information in this case.

This was an important decision for our Office in that it helped strengthen our international outreach activities in order to better protect the personal information of Canadians.

As a result of the decision, we are conducting an investigation into the complaint about Accusearch.

As well, proceedings have been initiated in the United States against Accusearch with respect to its advertising and selling of confidential consumer telephone records to third parties without the consent of the individual concerned. Given our Office's increasing interest in international activities in helping to protect the personal information of Canadians, our Office is closely monitoring these proceedings.

Complainant-initiated court applications under section 14 of PIPEDA
Dr. Jeffrey Wyndowe (Psychiatric Assessment Services Inc.) v. X.
Federal Court of Appeal File No. A–551–06

This is a long-running case, which was also discussed in our 2005 and 2006 annual reports. At issue is whether an individual has the right to access his personal information contained in notes taken by a physician conducting an independent medical examination on behalf of an insurance company.

The Federal Court considered whether such notes contained the "personal information" of the individual examined, and if so, whether any exemptions to refusing access to such information under *PIPEDA* applied. The Federal Court held the notes did contain the individual's personal information and that the claimed *PIPEDA* exemptions did not apply. Accordingly, it ordered the doctor to provide access to the notes.

The physician appealed. At the Federal Court of Appeal, the issues became, first, whether the notes constituted the personal information of the individual examined or the work product of the physician; and secondly, whether notes taken in the context of an independent medical examination occur in the course of a commercial activity covered by *PIPEDA*.

The Federal Court of Appeal issued its decision in February 2008 and held that:

(i) Notes taken by a medical examiner in the course of an independent medical examination made at the request of an insurance company are taken in the "course of a commercial activity" and thus clearly subject to *PIPEDA*; and

(ii) Notes taken by a medical examiner in the course of an independent medical examination clearly contain an individual's personal health information, and, therefore, personal information.

The Federal Court of Appeal held that the individual has a right to access those portions of the notes which contain information he provided, and also to correct any mistakes in what the medical examiner may have noted about him.

However, the Court also concluded that information in the notes could be personal to both the individual and the physician, and that there may be need for a balancing exercise which takes into consideration the private interests of the individual and the physician, as well as the public interest in disclosure and non-disclosure.

The case was sent back to the Privacy Commissioner so that she, together with the doctor's counsel, could determine which portions of the notes contain the individual's "personal information" and should be released.

X. v. Telus Communications Inc.
Federal Court of Appeal File No. A–639–05

This case involved Telus employee complaints about the company's implementation of a voice-recognition system.

Note: This case was also reported in our 2004, 2005 and 2006 annual reports.

In January 2007, the Federal Court of Appeal confirmed that:

(i) The voice-print collected by Telus is personal information;

(ii) On the facts, a reasonable person would find the introduction of voice-print technology for company authentication and security purposes to be reasonable in the circumstances;

(iii) The Telus voice-print authentication system met *PIPEDA*'s consent requirement since employees could not be enrolled in the system without their active consent;

(iv) None of the exceptions set out in section 7 of *PIPEDA* allowing for the non-consensual collection apply to these circumstances; and

(v) Telus properly informed employees of the consequences which might arise if they refused consent.

X. v. Scotia Capital Inc.
Federal Court File No. T-2181-05

In response to the complainant's request for his personal information, Scotia Capital provided the complainant with a copy of his personal information but did not include his pay stubs or records of hours of work.

The complainant alleged Scotia Capital improperly relied on exemptions for third-party information and solicitor-client privileged materials. As a result of our investigation, the company forwarded additional information to the complainant.

The Assistant Commissioner concluded the organization was otherwise justified to withhold information which consisted of other individuals' personal information, or was subject to solicitor-client privilege.

The complainant filed an application in the Federal Court under section 14 of *PIPEDA*. The application was later dismissed.

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

An individual filed a complaint against J.J. Barnicke Ltd. 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.

The Assistant Privacy Commissioner concluded that, as there was no evidence that any J.J. Barnicke employee responded to the e-mail, there was no actual collection of

personal information. Therefore, the complaint regarding the improper collection of personal information was not well-founded.

However, the investigation revealed that J.J. Barnicke did not have appropriate privacy policies or procedures in place, nor was there a designated privacy officer accountable for compliance. Although J.J. Barnicke developed a privacy policy during the course of the investigation, the Assistant Privacy Commissioner recommended that the organization post the privacy policy on its website, disseminate the privacy policy to its employees and provide staff with proper privacy training. J.J. Barnicke fully implemented the Assistant Commissioner's recommendations.

The complainant filed an application in the Federal Court. A hearing scheduled for November 2007 was adjourned on the basis of a preliminary procedural motion and a new hearing date had not yet been set.

Monitoring Function

As part of our larger court monitoring function, we continued to monitor several court cases involving novel privacy issues. This is one of the ways in which we stay abreast of possible advancements in the law, whether they be through applications under *PIPEDA*, applications under the *Privacy Act*, the federal *Access to Information Act*, or actions in the provincial superior courts under the common law or Quebec's civil law.

For example, we were granted intervener status in *X. v. The Minister of Health and Privacy Commissioner of Canada*, even though this matter originated under the *Access to Information Act*.

In this case, a journalist sought access to Health Canada's Canadian Adverse Drug Reaction Information System database, which houses mandatory and voluntary reports of adverse reactions to drugs marketed in Canada.

Health Canada refused to reveal the province in which data had been collected on the grounds that this information, together with the already released information, could permit the identification of individuals when combined with publicly available information. The Information Commissioner agreed, holding that the information was exempt from access.

The journalist sought judicial review of Health Canada's decision.

Our Office decided to intervene given the significance of this case in relation to the interpretation and application of both *PIPEDA* and the *Privacy Act*, as well as the

interpretation of the meaning of "personal information." We argued in favour of a broad definition of personal information.

This case demonstrates the important role we can play as an intervener on issues having a significant impact on *PIPEDA* and/or the *Privacy Act* – and in this way contribute meaningfully towards the development of privacy jurisprudence in Canada.

The Federal Court was to hear the case in February 2008.

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 British Columbia, Alberta, Ontario and Quebec which has been declared substantially similar.

No provinces or territories enacted legislation in 2007 for which they have sought consideration as substantially similar to *PIPEDA*.

THE YEAR AHEAD

Our key priorities for the coming year:

Continue to improve service delivery

- Design and implement new and innovative investigative strategies to make our complaints resolution process more efficient and effective.

Build a sustainable organizational capacity

- On the human resources side, address retention issues and grow our Office in order to balance workload internally and manage increasing demand for our services.
- Continue an information management renewal project; introduce scanning technology; use current technologies to update inquiry and investigation processes; and modernize our case management system.

Support Canadians to make informed privacy decisions

- Develop materials to help Canadians better understand their privacy rights and take action to protect these rights.
- Prepare and distribute publications and guidelines in print and on the web; continue to reach out using new and interactive technologies such as blogs and online videos.
- Implement a social marketing campaign on children's online privacy.
- Put into place education and outreach programs in partnership with provincial and territorial privacy commissioners.

Provide leadership to advance four priority privacy issues

- Information Technology
    - Build sufficient capacity to assess the privacy impact of new information technologies.
    - Increase public awareness of technologies with potential privacy impacts.
    - Provide practical guidance to organizations on the implementation of specific technologies.

- National Security
  - Ensure national security initiatives adequately protect privacy.
  - Ensure proper oversight and accountability of national security agencies' personal information management practices.
  - Raise public awareness of the privacy impacts of national security initiatives.

- Identity Integrity and Protection / Identity Theft
  - Improve organizations' personal information management practices.
  - Raise public awareness of identity protection.
  - Persuade the federal government to adopt a coordinated approach to identity protection.

- Genetic Information
  - Advance research and knowledge to address new challenges posed by genetics in the context of traditional data protection regimes.
  - Raise public awareness about the potential uses of genetic information.

Advance global privacy protection for Canadians

- Seek legislative amendments to *PIPEDA;* co-operate with other data protection authorities to ensure privacy protection measures are comprehensive and harmonious.
- Chair an OECD volunteer group reviewing how cooperation between data protection authorities and other privacy rights enforcement agencies can be enhanced.
- Continue to work with an APEC data privacy group which has developed a privacy framework for APEC member states.

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 valid 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 the complainant's rights under *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.

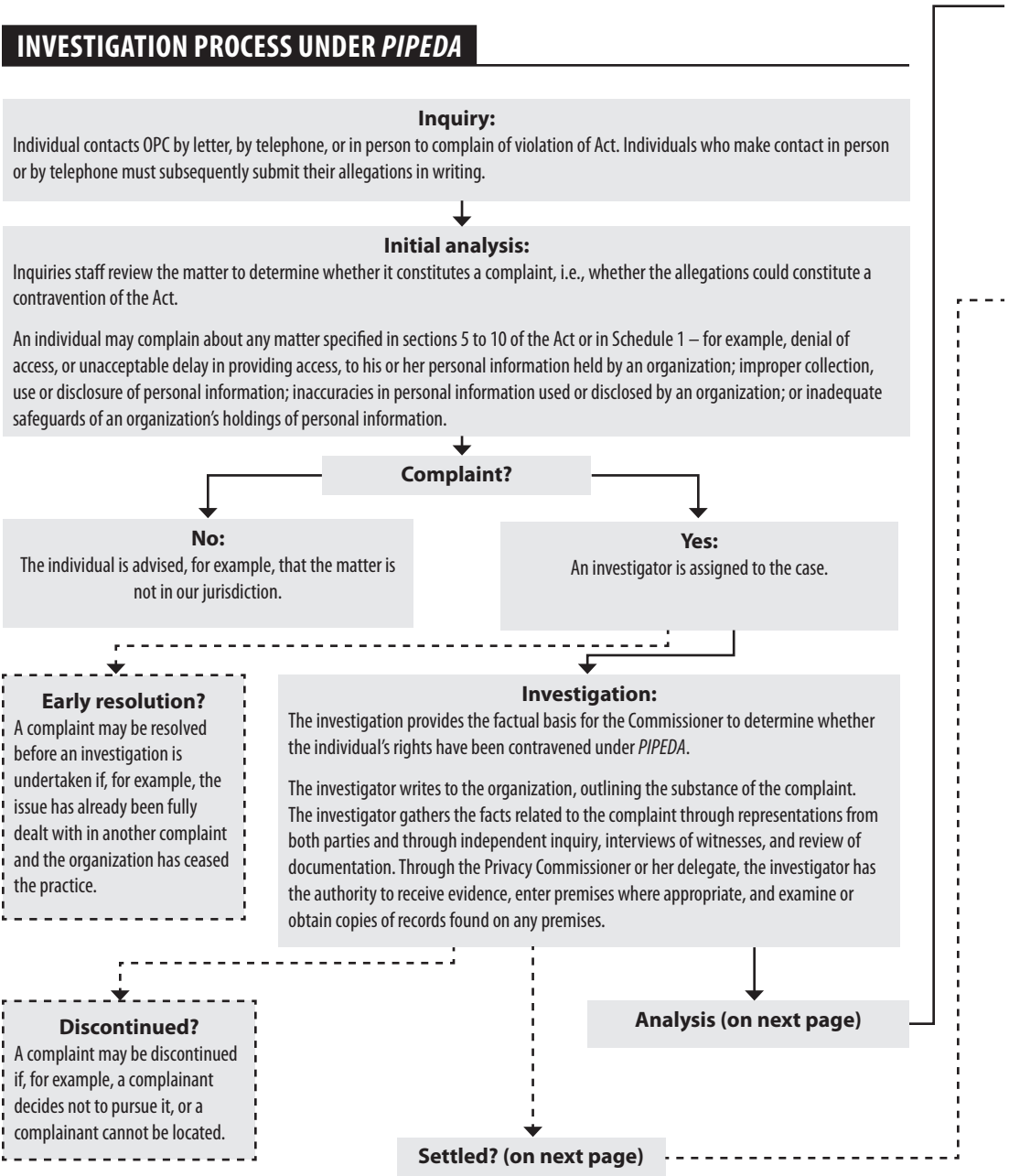
- **Settled during the course of the investigation.** The OPC helped negotiate a solution that satisfies all involved parties during the course of the investigation. No finding is issued.

- **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.

INVESTIGATION PROCESS UNDER *PIPEDA*



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 – INQUIRY AND INVESTIGATION STATISTICS

Inquiries Statistics

Our Inquiries Unit provides one of our most important services to Canadians – quick, direct and personalized information about privacy issues. We received almost 8,000 *PIPEDA*-related inquiries in 2007.

Frequently raised issues include: the collection and use of Social Insurance Numbers; obtaining access to personal data held by financial institutions; and use and disclosure of personal information in the telecommunications and sales sectors. Identity theft is another key issue people contact us about. Police often advise individuals who have filed police reports about identity theft to get in touch with our Office for further information.

We have recently seen heightened interest by organizations about transborder issues.

For the period between January 1 and December 31, 2007

***PIPEDA* inquiries received by the Inquiries Unit**	
Telephone inquiries	6,428
Written inquiries (letter and fax)	1,208
Total number of inquiries received	7,636

***PIPEDA* inquiries closed by the Inquiries Unit**	
Telephone inquiries	6,417
Written inquiries (letter and fax)	1,142
Total number of inquiries closed	7,559

COMPLAINTS RECEIVED BY TYPE

By far, the largest number of complaints we receive involve 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.

Complaints received between January 1, 2007 and December 31, 2007

Complaint type	Count	Percentage
Use and Disclosure	120	34
Collection	68	19
Access	67	19
Safeguards	36	10
Consent	16	5
Time Limits	13	4
Accountability	8	2
Accuracy	7	2
Retention	7	2
Openness	4	1
Correction/Notation	3	1
Fee	1	<1
Total	**350**	

BREAKDOWN BY SECTOR

Complaints received between January 1 and December 31, 2007

Sector	Count	Percentage
Financial Institutions	105	30
Telecommunications	42	12
Other	39	11
Sales	37	11
Insurance	35	10
Transportation	28	8
Professionals	26	7
Accommodation	21	6
Health	9	2.5
Services	6	2
Rental	2	<1
Total	**350**	

CATEGORIES

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

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

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

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

Insurance: Life and health insurance, property and casualty insurance

Transportation: Air, land, rail, water

Professionals: Accountants, lawyers

Accommodation: Hotels, landlords, condominiums, property management

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

Services: Daycare, hairdressers, beauticians

Rental: Car rental, other rental

CLOSED COMPLAINTS BY COMPLAINT TYPE

Complaints closed between January 1, 2007 and December 31, 2007

Complaint type	Count	Percentage
Use and Disclosure	162	39
Collection	80	19
Access	68	16
Safeguards	37	9
Consent	25	6
Time Limits	11	3
Accountability	9	2
Retention	9	2
Correction/Notation	7	2
Accuracy	5	1
Openness	4	1
Other (Retaliation)*	2	<1
Fee	1	<1
Total	**420**	

* We closed two retaliation or "whistle-blowing" complaints. The enforcement of retaliation complaints is included under section 27.1 of *PIPEDA*. The provision is aimed at ensuring that organizations do not retaliate against employees who have, in good faith, brought forward allegations that their employers have contravened *PIPEDA* or will contravene *PIPEDA*, or that an employee has refused to do something that would contravene the legislation. Retaliation could include, for example, dismissal, suspension, demotion, or discipline.

The Commissioner, in her ombudsman role, has an obligation to investigate retaliation cases to determine whether she should forward them to the Attorney General of Canada for possible prosecution under the Criminal Code. While our Office has assessed retaliation complaints, no cases have warranted follow-up with the Attorney General.

Number of complaints in abeyance
(awaiting assignment to an investigator) on December 31, 2007: 44

CLOSED COMPLAINTS BY FINDING

Almost one third of our closed complaints were settled. This indicates that, in a large number of cases, we were successful in finding solutions that satisfied complainants, respondents and this Office.

The next-largest category was discontinued. Cases are discontinued for a number of reasons – complainants abandon complaints for personal reasons or because an organization resolves an issue before the investigation has begun or our Office can't proceed because a complainant hasn't provided us with requested additional details necessary to complete an investigation.

Complaints closed between January 1, 2007 and December 31, 2007

Finding	Count	Percentage
Settled	125	30
Discontinued	89	21
Not well-founded	64	15
Well-founded Resolved	62	15
Resolved	41	10
Early Resolution	14	3
No jurisdiction	14	3
Well-founded	9	2
Other (Retaliation)	2	<1
TOTAL	**420**	

PIPEDA INVESTIGATION TREATMENT TIMES - BY FINDING

Roughly one-quarter of our investigations are completed within a year. More complex cases take longer to complete. For example, cases involving multi-jurisdictional issues or which require extensive research into industry practices usually take more time to complete. In some instances, cases take longer if there are delays in obtaining information.

For the period between January 1 and December 31, 2007

Disposition	Average Treatment Time in Months
Early Resolution	3.36
Discontinued	11.18
No jurisdiction	12.07
Settled	12.17
Not well-founded	20.56
Resolved	20.68
Well-founded Resolved	23.15
Well-founded	24.36
Other (Retaliation)	26.00
Overall Average	**15.71**

FINDINGS BY COMPLAINT TYPE

Complaints closed between January 1, 2007 and December 31, 2007

	Discontinued	Early Resolution	No Jurisdiction	Not Well-founded	Other	Resolved	Settled	Well-founded	Well-founded Resolved	TOTAL
Use and Disclosure	26	8	6	27	0	8	46	3	38	**162**
Collection	18	2	2	18	0	7	25	2	6	**80**
Access	17	2	5	4	0	15	19	1	5	**68**
Safeguards	9	1	0	4	0	3	11	1	8	**37**
Consent	7	1	1	2	0	5	7	0	2	**25**
Time Limits	4	0	0	0	0	2	3	2	0	**11**
Accountability	0	0	0	2	0	1	5	0	1	**9**
Retention	2	0	0	2	0	0	5	0	0	**9**
Correction/ Notation	3	0	0	3	0	0	0	0	1	**7**
Accuracy	2	0	0	1	0	0	1	0	1	**5**
Openness	0	0	0	1	0	0	3	0	0	**4**
Other	0	0	0	0	2	0	0	0	0	**2**
Fee	1	0	0	0	0	0	0	0	0	**1**
TOTAL	**89**	**14**	**14**	**64**	**2**	**41**	**125**	**9**	**62**	**420**

FINDINGS BY INDUSTRY SECTOR

Complaints closed between January 1, 2007 and December 31, 2007

	Discontinued	Early Resolution	No Jurisdiction	Not Well-founded	Other	Resolved	Settled	Well-founded	Well-founded Resolved	TOTAL
Financial Institutions	24	5	3	21	0	14	28	0	18	**113**
Telecommunications	11	2	2	12	1	5	17	4	17	**71**
Sales	7	3	1	2	0	5	34	0	9	**61**
Other	17	0	7	8	0	2	23	0	1	**58**
Insurance	13	2	0	3	0	6	11	1	8	**44**
Transportation	4	1	0	11	1	4	7	2	3	**33**
Professionals	3	1	1	2	0	2	1	2	2	**14**
Services	2	0	0	4	0	1	0	0	4	**11**
Accommodations	7	0	0	0	0	0	2	0	0	**9**
Rental	0	0	0	0	0	2	2	0	0	**4**
Health	1	0	0	1	0	0	0	0	0	**2**
TOTAL	**89**	**14**	**14**	**64**	**2**	**41**	**125**	**9**	**62**	**420**

PIPEDA INVESTIGATION TREATMENT TIMES - BY COMPLAINT TYPE

For the period between January 1 and December 31, 2007

Complaint Type	Average Treatment Time in Months
Accuracy	9.4*
Fee	10.0*
Time Limits	11.3
Retention	12.7
Access	14.5
Openness	15.3*
Correction/Notation	15.4
Use and Disclosure	15.8
Safeguards	15.9
Accountability	16.2
Collection	17.0
Consent	18.0
Other	26.0*
Overall average	15.7

*The treatment time for these complaint types reflects 6 or fewer cases each.