Privacy Commissioner of Canada

Commissaire à la protection de la vie privée du Canada

Privacy

Annual Report to Parliament 2006

Report on the *Personal Information Protection and Electronic Documents Act*

Canada

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

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

ISSN 1910–0051

This publication is also available on our Web site at www.privcom.gc.ca.

Privacy Commissioner of Canada

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

Commissaire à la protection de la vie privée du Canada

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

May 2007

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

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Personal Information Protection and Electronic Documents Act* for the period from January 1 to December 31, 2006.

Sincerely,

Jennifer Stoddart

Jennifer Stoddart
Privacy Commissioner of Canada

Privacy Commissioner of Canada

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

Commissaire à la protection de la vie privée du Canada

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

May 2007

The Honourable Peter Milliken, M.P.
The Speaker
The House of Commons
Ottawa, Ontario K1A 0A6

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Personal Information Protection and Electronic Documents Act* for the period from January 1 to December 31, 2006.

Sincerely,

Jennifer Stoddart

Jennifer Stoddart
Privacy Commissioner of Canada

Table of Contents

Message from the Commissioner

The year 2006 proved there has never been a greater need to take the protection of personal information seriously – new data breaches reinforced our concerns about both security issues and trans-border data flows.

It was also a year to take stock of Canada's private-sector privacy regime and look for ways to create even more effective legislation to govern privacy issues.

Moving information across borders

For several years, the Office of the Privacy Commissioner (OPC) has warned of the serious privacy risks introduced when Canadians' personal information moves across borders. These concerns initially arose when the *USA PATRIOT Act* granted the US Federal Bureau of Investigation new powers to access personal information held by US organizations. They re-emerged in 2006, when the international press reported that the Society for Worldwide Interbank Financial Telecommunication (SWIFT), a European-based financial cooperative that supplies message services and interface software to financial institutions in more than 200 countries including Canada, had secretly disclosed personal information to the US Treasury.

These media reports were alarming and prompted the OPC to launch an investigation. Our conclusions, reached after the reporting period covered in this document, are outlined in my April 2007 Report of Findings. (That report is available on our Web site, www.privcom.gc.ca.)

In brief, we found SWIFT did not contravene the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*), to which it is subject, when it complied with lawful subpoenas served outside the country and disclosed Canadians' personal information to foreign authorities. However, the disclosure process could have been more transparent if the government bodies involved had used existing information-sharing mechanisms, which have privacy protections built in. We have asked Canadian officials to work with their US counterparts to encourage them to use these mechanisms, rather than the subpoena route, to obtain information in the future.

More data security concerns

A separate set of media reports about major data breaches also provoked concern by Canadians toward the end of 2006. A few private sector organizations – notably a mutual fund subsidiary of the Canadian Imperial Bank of Commerce (CIBC) and the US-based owner of Winners and HomeSense stores – acknowledged they had lost huge amounts of sensitive personal information.

While these types of data compromises are not a new phenomenon, the massive volume of these privacy breaches and the media headlines brought them to public light in a dramatic fashion. The media coverage also reinforced for the Parliamentary committee reviewing *PIPEDA* the very serious nature of privacy breaches, as well as the need for further legislative and policy measures to better protect personal information held by private sector companies.

An important Parliamentary review

The launch of that review of *PIPEDA* by the House of Commons Standing Committee on Access to Information, Privacy and Ethics marked an important development for private sector privacy issues in Canada.

The review began in late 2006. This was the first five-year review of the Act, which came into force in stages beginning in 2001. Long before the committee hearings started, my Office was gearing up to identify measures to improve the Act.

Overall, *PIPEDA* has generally proved to be sound legislation. That said, some parts require updating and fine-tuning to better address the effects of intrusive technologies, the increasingly inquisitive private sector environment, and the heightened desire by governments, post 9/11, for access to personal information held by the private sector.

In July 2006, we released a consultation document inviting input about possible amendments. We received more than 60 submissions and presented an analysis of those to the committee in November. The strong response affirmed for us the keen interest among Canadian consumer groups, academics, businesses and citizens to see to it that personal information in the private sector is properly protected. National surveys consistently find that Canadians appreciate the importance of privacy in their daily lives.

The end of an era

Sadly, 2007 will mark the end of an era for this Office. Heather Black, Canada's first Assistant Privacy Commissioner for *PIPEDA*, will retire early in the year.

For almost 25 years, Heather has been a guiding force in Canada on privacy matters. Before joining the OPC, she acted as one of the architects of *PIPEDA* at Industry Canada. She has guided the Act's interpretation in its first five years of application – first as General Counsel to this Office, then as Assistant Commissioner responsible for *PIPEDA*.

The OPC, colleagues elsewhere in government, organizations subject to *PIPEDA* and, most of all, the Canadian public, have all benefited from her extraordinary depth of knowledge, and sage and balanced approach. I thank Heather for her tremendous contributions, and I sincerely hope her voice will continue to be heard on privacy issues.

Looking ahead

We were busy at the end of 2006, laying the groundwork for what will undoubtedly be an exciting time in our Office's history. We are hosting the who's who of the privacy world at the 29th International Conference of Data Protection and Privacy Commissioners in Montreal in the fall of 2007. Our theme, *Privacy Horizons: Terra Incognita* points to the challenge we face as we enter the uncharted privacy ground of the future. Each year brings new challenges for privacy.

Jennifer Stoddart
Privacy Commissioner of Canada

PIPEDA Review

Section 29 of *PIPEDA* requires Parliament to review Part 1 of the Act (the portion dealing with data protection) every five years. As the Act came into force in stages starting in 2001, the initial five-year review was scheduled for 2006.

The House of Commons Standing Committee on Access to Information, Privacy and Ethics began the review in the late fall. In preparation, our Office issued a consultation paper identifying 12 key issues for consideration.

We were delighted to receive more than 60 responses to that paper from a variety of organizations and individuals, which the Commissioner presented to the committee in November. Committee hearings continued into 2007, involving a cross-section of organizations, private sector associations, privacy advocates and individuals. At the time of this report's writing, the committee had just issued its report. We will include our comments in next year's annual report.

Generally, *PIPEDA* continues to prove relevant and effective. It strikes an appropriate balance between the right of individuals to maintain the privacy of their personal information and the need of organizations to collect, use and disclose personal information for reasonable purposes.

Our form of ombudsman model, which includes litigation and audit powers, continues to provide the Privacy Commissioner with sufficient authority to bring organizations in compliance with *PIPEDA;* no specific order-making power is required at this time. Nevertheless, there is room for change in other areas.

As detailed in the Commissioner's appearance before the committee, certain amendments could serve to clarify and enhance the Act.

Incorporating provincial concepts

Many of the more complex complaints received by the OPC deal with the disclosure of employees' personal information. The notion that free and informed consent is required from an employee before an organization can collect his or her personal information is out of synch with the realities of the employment environment. Employees in a weak bargaining position may be pressured to consent to the collection, use and disclosure of their personal data.

The OPC proposed that the Parliamentary committee explore as an example, Alberta's private sector legislation, the *Personal Information Protection Act*, which establishes a reasonableness test for deciding when the collection of personal employee information is acceptable. We also suggested *PIPEDA* amendments related to this issue incorporate the notion of dignity of the person—an element of Quebec's private sector law.

In addition, we asserted that *PIPEDA* could benefit from adopting other elements of the second-generation private sector privacy laws of Alberta and British Columbia. Those laws include provisions related to the disclosure of personal information as part of the sale or transfer of a business. Both provinces allow prospective purchasers to see client lists and employee information as part of corporate due diligence. Our Office recommended that *PIPEDA* allow for similar disclosures, but under stringent confidentiality agreements.

We also support adding a provision making it an offence to willfully attempt to collect personal information without consent. This is an element included in Alberta's private sector law.

Disclosure with jurisdictions outside Canada

Growing cross-border flows of personal data mean that, from time to time, the OPC receives complaints concerning information-access activities occurring outside Canada.

Many countries face similar challenges and have introduced provisions for limited information-sharing while carrying out investigations of mutual interest. In its current form, *PIPEDA* allows the Commissioner to share information and cooperate in investigations with provincial counterparts who have substantially similar legislation.

While the Act already includes an Accountability Principle to help protect personal information once it leaves Canada, there is room for improvement. With a view to more effective enforcement and to increasing Canadians' comfort with trans-border data flow, we recommended that the Privacy Commissioner be given specific authority to share investigation information with international counterparts while cooperating on investigations of mutual interest.

The Commissioner will continue to address cross-border challenges related to enforcement of privacy laws in her work as Chair of a Working Group of the Organization for Economic Co-operation and Development (OECD) Working Party on Information Security and Privacy.

Disclosure related to national security

In our November appearance before the committee reviewing *PIPEDA*, we reiterated our concern about *PIPEDA*'s provision allowing organizations to collect and disclose personal information for law enforcement and national security purposes. The *Public Safety Act, 2002* amended *PIPEDA* to grant such permission. Our Office had requested that the provision be removed at the time Parliament was reviewing the bill. We contend that it begs removal or, at the very least, restriction to limit its unnecessarily broad scope.

Notification of breaches

Finally, the Commissioner recommended that *PIPEDA* be amended to include mandatory breach notification when personal information is lost. We recognize this does not fit easily into the current *PIPEDA* model, as there is no easy way to penalize organizations failing to notify. As such challenges are considered, the Commissioner is working with relevant and interested stakeholders to develop voluntary guidelines for organizations to follow in the event of a breach.

Review of the *Privacy Act*

We are very pleased that *PIPEDA* mandates that a review of the legislation be conducted every five years and we look forward to seeing the law keep apace with new challenges. Canada's quarter-century-old public sector legislation, on the other hand, called only for one mandatory review after three years. A committee did review the *Privacy Act*, but its recommendations were never acted upon. Subsequent calls for reform have also been overlooked. The *Privacy Act* is now extremely out of date and in urgent need of its own review and overhaul.

Policy

In today's global economy, personal information is constantly flowing – within jurisdictions, across provincial boundaries and between countries.

Trans-border information flows benefit both private sector companies and consumers. They allow multinational corporations to distribute their business centres throughout the world, take advantage of lower-cost labour and regionally specialized expertise, and transcend the limits of the eight-hour workday.

Trans-border flows allow consumers to enjoy exceptional customer convenience. We can now book vacations and shop online, receive customer service 24/7, and tap into bank accounts and credit sources from anywhere in the world.

A FLOOD OF INFORMATION

Thanks to the falling costs of telecommunication and the enhanced processing and memory capabilities of computers, the volume of personal data being generated by this always-on economy is growing exponentially. One needs only to think of the enormous amounts of information shared during online searches or social networking Web site visits. More organizations have access to more information about more people than ever before.

With each transfer of information, the threats posed by hackers, unscrupulous employees and identity thieves increase. Instances of laptop theft or loss, and careless handling of information only intensify the risks.

As the threats become clearer and the potential damage apparent, the security of personal information has taken on new importance and created new challenges for entities such as the OPC.

2006 INVESTIGATIONS

Data breaches are becoming more regular occurrences. At year-end, the OPC was involved in two major data breach investigations. We launched a joint investigation with the Information and Privacy Commissioner of Alberta,

Frank Work, into a breach of the database of TJX Companies Inc., operator of Winners and HomeSense stores in Canada. Hackers allegedly gained access to the company's database, which contained the personal information of Canadian customers.

We also began an investigation into a breach involving the personal information of close to half a million clients of Talvest Mutual Funds, a subsidiary of the Canadian Imperial Bank of Commerce (CIBC). We launched this Commissioner-initiated investigation after the bank notified our Office of the disappearance of a hard drive containing the personal information and financial data of approximately 470,000 Talvest clients.

Jurisdictional considerations

In the post-9/11 world, personal information is often seen as valuable intelligence that can help identify security threats and detect transnational crimes such as money laundering and terrorist financing. When personal information moves across borders, it may become subject to different legal regimes. Individuals may lose some of their privacy rights, such as the ability to request access to the information or seek redress if the information is unlawfully used or disclosed.

Countries around the globe are recognizing the need to make the protection of personal data as it crosses borders as seamless as possible. The importance of international cooperation has been recognized by a number of bodies, including the International Conference of Data Protection and Privacy Commissioners, Asia Pacific Economic Cooperation, and the European Union's Article 29 Working Party on Data Protection. With greater awareness of the threats associated with increased trans-border data flows, consensus is emerging around the importance of promoting closer co-operation among privacy enforcement authorities in different countries.

International investigations

In 2006, the OPC learned that US authorities were obtaining access to Canadians' financial information – without their knowledge – through the Society for Worldwide Interbank Financial Telecommunication (SWIFT). SWIFT is a European-based financial cooperative that supplies messaging services and interface software to financial institutions in more than 200 countries, including Canada. The OPC launched an investigation to determine whether SWIFT was improperly disclosing personal information to foreign authorities.

We also reopened our investigation of Accusearch (also known as Abika.com) following a Federal Court ruling which confirmed our jurisdiction to investigate a complaint against an organization that operates out of the US to service customers from many countries, including Canada, by selling personal information about individuals via the Internet. The Federal Court's decision highlighted the practical difficulties associated with investigating an organization operating outside the country. We have been able to address some of these challenges with the assistance of the US Federal Trade Commission (FTC), which, following the passage of the *Safe Web Act* by the US Congress, has greater freedom to share information with other authorities.

Our active involvement in solving such challenges will continue. In 2006, the Privacy Commissioner was asked to chair an OECD volunteer group that is examining ways to encourage cross-border enforcement cooperation.

The OPC also contributed to work by Asia-Pacific Economic Cooperation (APEC) on privacy issues. In light of our increasing data flows with a number of APEC member countries, Canada has been active in ensuring that our privacy values are reflected in APEC data protection rules. APEC ministers endorsed the new APEC Privacy Framework at the end of 2006.

Research into Emerging Privacy Issues

Our Contributions Program was launched in 2004 to advance independent research in priority areas. The program has been applauded by the research community and privacy experts as vital to galvanizing action around the broad spectrum of privacy issues we face in Canada.

The Contributions Program aims to foster an understanding of the social value of privacy so Canadians may better address emerging issues. Section 24 of *PIPEDA* requires the Privacy Commissioner to:

- *Develop and conduct information programs to foster public understanding of privacy*
- *Undertake and publish research related to the protection of personal information*
- *Promote, by any means that the Commissioner considers appropriate, the purposes of the Act*

Participants and funding levels

A total of 26 research projects have been funded by the Contributions Program in its first three years of operation – 10 in 2004-05, five in 2005-06, and 11 in 2006-07. (Note: The Program follows the government fiscal year, from April 1 to March 31.)

The Office selects research projects through a rigorous competition process through which the very best proposals, which represent the diverse research capacity across Canada, are chosen. While the majority of successful applicants have been from universities, projects led by non-governmental organizations and professional associations have also received funding.

Researchers enter into signed agreements with the OPC and report quarterly so the Office can monitor their progress.

As of March 31, 2007, over $900,000 has been awarded since the program's inception. A fourth call for proposals was issued in January 2007 for the coming fiscal year (2007-08).

Key research themes

Research funded by the OPC in 2006-07 looked at a number of important privacy issues, including:

- protection of personal health information, particularly in a modern context of electronic health records
- strategies for building individuals' awareness of privacy rights
- 'professionalization' of privacy specialists
- storage and retention of personal information
- matters of surveillance – implications of new technologies, workplace surveillance, tracking of individuals' Internet interactions

Contributing to public policy debate

Over the last three years, research funded under the Contributions Program has served to advance public debate on privacy issues in Canada and abroad.

For example, several studies have focused on compliance with *PIPEDA* and implementation of relevant guidelines. Research in this area has fed into the five-year review of the legislation by Parliament. Other studies have helped raise awareness of workplace privacy issues, attracting significant national media attention.

Looking ahead

Priority areas identified for 2007-08 include:

- protection of personal information on the Internet
- challenges inherent to the secure identification and authentication of individuals and entities
- the intersection of the public and private sectors with respect to use and protection of personal information

Program evaluation

Under the federal government's Transfer Payment Policy, contribution programs must be reviewed periodically to affirm their continued relevance, success and cost-effectiveness. The OPC has committed to an independent program evaluation in 2008-09. By year-end, a draft evaluation framework had been developed. It is based on Treasury Board's 2005 Results-Based Management and Accountability Framework. The evaluation, which will involve consultations with various stakeholders, will facilitate any decision to renew the terms and conditions of the program. It will ultimately ensure the accountability and good management Canadians expect.

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 2006 for which they have sought consideration as substantially similar to *PIPEDA*.

Complaint Investigations and Inquiries

In 2006, the OPC observed some interesting and encouraging trends, stemming in part from increased knowledge and understanding of *PIPEDA* by private sector organizations.

Highly publicized data breaches raised the profile of personal-information protection as a public concern. The events made clear that the relationship of trust between consumers and private sector organizations depends on the organizations' responsible handling of customers' personal information. This reinforced *PIPEDA*'s importance as a mechanism for ensuring private sector accountability.

Inquiries

We saw an increase in the number of *PIPEDA*-related inquiries in 2006. The OPC received 6,050 inquiries, compared with 5,685 in 2005 – an increase of 6.4 per cent. However, there has been an overall decline in inquiries since 2003, when our Office fielded 12,132 inquiries. This decline possibly indicates that Canadian organizations and individuals are becoming more familiar with the legislation. *PIPEDA* came into effect in stages, beginning in January 2001. Since January 2004, *PIPEDA* applies right across the board – to all personal information collected, used or disclosed in the course of commercial activities by all private sector organizations, except in provinces which have enacted legislation that is deemed to be substantially similar to the federal law.

Complaints

We received 424 complaints in 2006, compared with 400 in 2005. Complaints against some of the major sectors covered by *PIPEDA* since 2001 (financial institutions, insurance companies and the transportation sector) declined slightly, but industries subject to *PIPEDA* only since 2004 – such as the retail and accommodation sectors – figured in substantially more complaints than in previous years.

Going forward, these companies will need to take steps to ensure greater compliance with the Act. Additional pressure for the private sector to adequately safeguard personal information is coming from individual Canadians, who

are increasingly demanding a high standard of privacy protection. With the proliferation of identity theft and fraud, more and more consumers will seek protection through *PIPEDA* and hold organizations accountable.

The OPC closed 309 complaints in 2006, compared with 401 the previous year. The majority involved three issues: Use and disclosure (111, or 36 per cent); collection (74, or 24 per cent); and, access (51, or 16 per cent).

Disposition of complaints

An analysis of the disposition of complaints completed in 2006 shows that only five per cent were deemed to be well-founded, compared with 10 per cent in 2005. Twenty per cent were resolved, which is an increase of nine per cent over 2005. The total of early resolution, settled and resolved complaints represented 51 per cent of closed complaints. Not well-founded complaints accounted for 21 per cent of the total.

Note: Definitions of types of complaints, findings and other dispositions, as well as detailed complaint figures and a chart describing our complaint investigation process under *PIPEDA*, are available in Appendix 1 and 2 of this report.

Our role as a public advocate for the privacy rights of Canadians is reflected in the large percentage of complaints that are settled during the course of investigation. Many complaints are settled through mediation, negotiation and persuasion, resulting in resolutions that satisfy all parties. In 2006, the number of settled complaints dropped by 13 per cent; yet they still made up the biggest proportion (26 per cent) of closed complaints – the same percentage as in 2005. We will continue to use this approach because settlement is a fundamental aspect of an ombudsman's role of helping organizations change their culture and find solutions to their problems with clients and employees. Furthermore, the willingness of private industry to settle is encouraging as it demonstrates their recognition of the critical importance of protecting customers' personal information.

Preliminary letters of findings

Sending out preliminary letters of findings was a new routine process step introduced in 2006, following policy changes the previous year. These letters are sent to complainants and respondents whenever there is a likely contravention of *PIPEDA*. Each letter contains specific recommendations and requires the private sector organization to respond to the Commissioner within a prescribed timeframe, detailing how it intends to implement her recommendations. In 2005,

the Commissioner adopted a policy of going to the Federal Court in all cases where companies failed to respond within the timeframe.

Last year, the OPC issued 26 preliminary reports, which prompted 21 of the organizations to comply with the Commissioner's recommendations. The other organizations complied after the Office referred the matters to litigation.

The 26 preliminary reports were issued to big and small companies, and were spread across various industries. Six of these reports were sent to financial institutions, and six to insurance companies. The fact that almost one-quarter of preliminary reports involved these two sectors reflects the generally large size of financial and insurance organizations and the significant amount of personal information they collect in the course of their day-to-day operations. Sectors such as banking, telecommunications and insurance, which have been operating under *PIPEDA* since 2001, are often issued recommendations that involve fine-tuning existing privacy policies and procedures, rather than starting such policies from scratch.

Nine of the preliminary reports were sent to businesses, such as law firms, fitness clubs, real estate firms and retail sector companies, which only came under the Act in 2004. The recommendations issued to them generally involved setting up privacy policies and procedures such as designating a privacy officer, training staff, and developing information for customers.

The new process of sending out preliminary letters of finding has been very effective in encouraging both the OPC and the private sector to find innovative solutions to bridge the privacy gaps uncovered during investigations. It has also strengthened commitments made by organizations to comply with *PIPEDA*.

Treatment times

The average treatment time for a complaint (calculated from the moment the complaint is received to the mailing of the letter of finding) was 16 months in 2006. This represents an unfortunate increase of five months over 2005, partly attributable to the increased complexity of some investigations and the new internal process requiring preliminary letters of findings to be sent. However, most of the increase is attributable to the loss of experienced personnel in our *PIPEDA* investigative group through career mobility or leave.

People with investigative skills are in high demand across the government, which means we are seeing a higher turnover than in the past and have a bigger challenge recruiting experienced people. We were significantly below our full complement of 17 *PIPEDA* investigators.

Our backlog of complaint files peaked mid-year, however the hiring of some new investigators allowed us to make impressive strides. By year-end, 57 per cent of those files had been assigned to investigators. As outstanding vacancies are filled and new investigators gain experience, we aim to further reduce and eliminate the backlog.

Case summaries

Case summaries of the Commissioner's findings under *PIPEDA* are available on the OPC Web site, www.privcom.gc.ca.

Of the 309 cases we closed in 2006, 40 are summarized on our Web site. In general, the OPC summarizes complaints that may be of public interest, have some educational value, examine a systemic issue, or deal with a particular issue for which there is no existing case summary. Major sectors, which collect and use a great deal of personal information, such as banking and insurance, have been a steady source of complaints. Therefore, there are a number of case summaries highlighting related issues that may be of interest to the public.

We chose case summaries for complaints against federal works, undertakings or businesses that reflect their experience in working with *PIPEDA*. For example, one particularly complex case we summarized involved complaints that several workers filed against a telecommunications company regarding the use of a global positioning system in its vehicle fleet. We will no doubt be investigating more complaints of this sort as new technologies play a larger role in our everyday lives.

Other summaries include cases from the medical sector, property management companies and law firms, among others.

Not surprisingly, more case summaries focusing on identity theft were added to our Web site during 2006. This trend will likely continue as identity theft continues to be highlighted in the news and as people become more aware of their privacy rights, particularly as they relate to how their personal information is safeguarded. On the one hand, some case summaries illustrate this increased consumer awareness. On the other hand, other summaries also show companies are taking steps to verify customers' identification so that their personal information is well-protected and the possibility of identity theft is reduced.

Self-reporting

In 2006, the number of instances where organizations reported data breaches to the OPC jumped by 41 per cent. This significant increase in self-reporting may illustrate an increased awareness by the private sector of the need to accept the responsibilities that come with maintaining customers' personal information.

It is clear that we are seeing a heightened awareness of privacy rights among Canadian companies. Recently publicized data breaches have no doubt also contributed to consumers' knowledge of their privacy rights.

Audit and Review

Subsection 18(1) of *PIPEDA* gives the Commissioner the authority to audit the personal information management practices of an organization where reasonable grounds exist to believe the organization may be contravening the fair information practices set out in the Act and its accompanying Schedule.

In 2006, the OPC continued to develop its audit capacity in order to apply the audit provision toward the examination of systemic risks. A new organizational structure was developed and a staffing action plan implemented that will allow the OPC to acquire additional audit resources.

Audits initiated in 2006

Two audits were initiated in 2006, pursuant to subsection 18(1) of *PIPEDA*. Complaint investigations raised concerns about certain identification and authentication systems and reasonable grounds were found to believe there was inadequate protection of personal information. Audits were deemed the appropriate means to examine the risk.

In August 2006, the two entities involved were notified of the audit, given information on how reasonable grounds were reached, and provided with an outline of how the audit would proceed. Introductory meetings were held in October 2006. At year-end, the audits were still in process. Results will be included in the 2007 annual report.

Equifax audit

One organization, Equifax Canada Inc., took the position that the Privacy Commissioner did not have reasonable grounds to do an audit. In November 2006, Equifax initiated proceedings in the Federal Court, asking the Court to review the decision that there were reasonable grounds to conduct an audit. It also asked the Court for an interim injunction that would stop the audit. While waiting for a court date, and with the cooperation of Equifax, the audit proceeded to carry out tests of the company's on-line consumer credit reporting system. An out-of-court settlement was reached with Equifax in March 2007 and the audit is proceeding to its conclusion.

Strengthening privacy at CIBC

Between 2001 and 2004, the Canadian Imperial Bank of Commerce (CIBC) misdirected a number of facsimiles containing customers' personal information. The OPC investigated and identified a number of concerns regarding the privacy protection safeguards within CIBC. The results of the complaint investigation were reported to the bank in March 2005.

As a result of the faxing problem, CIBC recognized the need to strengthen its approach to privacy. The bank subsequently informed the OPC of a number of corrective measures it had taken to address privacy issues and concerns. The Audit and Review Branch conducted a review to verify these corrective actions. (This was not an audit pursuant to subsection 18(1) of *PIPEDA*.) Our findings are summarized below:

We concluded that CIBC had addressed the incidents of misdirected faxes by implementing measures to mitigate the risks associated with facsimile data transmission. Such measures included the deployment of a technological solution to ensure internal faxes remain within CIBC, the elimination of fax usage for certain business processes, and the creation of a fax control framework to better manage the dissemination of faxes to internal and external parties. It was suggested to CIBC that compliance with the control framework be addressed in privacy audits undertaken by the bank.

In addition, we found CIBC had introduced notable measures to enhance its privacy management framework and had committed significant resources to increase privacy awareness among employees. These included:

- establishment of a Corporate Privacy Office;
- implementation of procedures to escalate privacy issues;
- root cause analysis to identify and remedy systemic weaknesses;
- creation of a database for privacy issue case tracking and reporting;
- development of customer contact and notification procedures; and
- establishment of a privacy intranet site for employee education and training purposes.

Overall, we found that CIBC had fulfilled its commitments. We offered recommendations to the bank to further reinforce and enhance its privacy practices related to the reporting and classification of privacy issues and to employee privacy training.

We would like to acknowledge the responsible action taken by the bank to strengthen its management of personal information.

Promoting compliance with *PIPEDA*

Audits are by no means the only way to promote compliance. The OPC encourages all organizations to evaluate their own privacy management systems and practices. To this end, in 2006, we made presentations to various associations, including the Chief Privacy Officers Council of Canada, the Canadian Bankers Association, the Canadian Alliance for Business Travel and the International Association of Privacy Professionals.

The OPC also developed a self-assessment tool, now slated for release in July 2007.

In the Courts

The Privacy Commissioner initiates court action whenever an organization refuses to adopt her recommendations in well-founded cases. This policy, consistently applied since 2005, has helped to establish a high level of compliance.

Settled Cases

All recommendations made by the Commissioner in 2006 had been adopted by year-end. Resolution occurred: through an organization's timely efforts to resolve issues before the Commissioner issued her final report on its case; through negotiated settlements between litigation counsel shortly following her report before the Commissioner proceeded to file a Court Application seeking a compliance order; or soon after Court Application filing.

In 2006, court applications were filed against the Commvesco-Levinson Viner Group (CLV Group) and Air Canada in order to seek their compliance with our recommendations. In the CLV Group case, we went to court in a bid to stop the landlord from collecting personal information from tenants, unnecessarily and without consent, particularly photographs of their apartments. In the Air Canada matter, we applied to the Federal Court to enforce our recommendation that the organization adopt a clear policy recognizing its responsibility to provide access to personal information under *PIPEDA*, independently of what may or may not be its discovery obligations under civil litigation rules. In each case, the matter settled without the need to pursue it through to an actual court hearing.

Although another court application was filed in 2006 against Air Canada, 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 were actively in the course of settlement discussions at the time of publication of this annual report and, therefore, the outcome will be reported on next year.

In regard to our court application against RBC Action Direct Inc., described in last year's annual report, we are pleased to say we reached a settlement with the organization and the action was discontinued as RBC Action Direct agreed to disclose certain additional portions of the requested document to the satisfaction of the Privacy Commissioner.

Ongoing Litigation

Ongoing litigation continued in respect of judicial review applications under section 18.1 of the *Federal Courts Act* examining the extent of the Privacy Commissioner's jurisdiction, and complainant-initiated court applications filed under section 14 of *PIPEDA* in which the OPC was involved as an added party.

Significant court decisions rendered in 2006 follow. In keeping with the spirit and intent of our mandate, we have respected the privacy of individual complainants by not including their names.

Judicial review applications under section 18.1 of the Federal Courts Act

Three cases progressed through judicial review this past year, including the Blood Tribe matter (described below) that has been granted permission to proceed further to the Supreme Court of Canada in February 2008.

Blood Tribe Department of Health v. The Privacy Commissioner of Canada et al
Federal Court of Appeal File No. A–147–05

This was an appeal of a decision by the Federal Court dismissing a judicial review application brought by Blood Tribe Department of Health Inc. The Blood Tribe's application challenged the Privacy Commissioner's jurisdiction to order Blood Tribe Department of Health Inc. to produce certain records under paragraphs 12(1)(*a*) and (*c*) of *PIPEDA*. The Privacy Commissioner issued her order after Blood Tribe Department of Health Inc. refused to supply documents she required to verify Blood Tribe Department of Health Inc.'s claim that personal information being sought by an individual complainant was exempted by solicitor-client privilege.

The appeal was allowed and the Privacy Commissioner's order was set aside. The Court of Appeal found the language in *PIPEDA* not clear enough to grant the Commissioner specific power to order the production of solicitor-client privileged documents – notwithstanding her powers to compel evidence in the course of investigations in the same manner as a superior court of record, and to receive any evidence she sees fit, whether or not it would be admissible in a court of law. In the Court's view, very express statutory language would be required to allow the Privacy Commissioner to review documents claimed to be privileged in the context of her investigation.

Although the Commissioner is bound to keep confidential any information she receives during the course of her investigation and would never provide that

information to an individual complainant, she has the discretion to disclose information to the Attorney General if, in her opinion, there is evidence of an offence. In the Court of Appeal's view, that possibility, however slight, may have an unwanted chilling effect and may undermine the confidence of Canadians in dealing with their lawyers. The Court suggested that the Commissioner apply to the Federal Court, under section 15 of *PIPEDA*, and leave it for judges to examine claims of solicitor-client privilege in the context of complaints involving refused access to personal information.

Given the problematic nature of this decision, from both a legal and practical perspective, and its importance for the future of privacy rights in Canada, the Privacy Commissioner sought leave to appeal to the Supreme Court of Canada. The Supreme Court of Canada granted leave to appeal on March 29, 2007 and a hearing has been scheduled for February 21, 2008.

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

An individual filed a judicial review application in December 2005, seeking an order quashing or setting aside the Privacy Commissioner's decision that she lacked jurisdiction to investigate the individual's complaint against a US-based organization, Accusearch Inc. (otherwise known as Abika). The OPC had taken the position that there was insufficient evidence of real and substantial factors connecting Abika's operations to Canada, so as to bring the company within the scope of application of *PIPEDA*. In a decision dated February 7, 2007, the Federal Court disagreed with the Commissioner's interpretation of the facts and allowed the application on the grounds that the Commissioner did have jurisdiction to investigate the trans-border flow of personal information in this case. Whether and how the Commissioner actually exercises her jurisdiction to investigate this matter are practical issues that the Court acknowledged, but declined to address in detail. Accordingly, the matter was sent back to OPC for investigation.

Equifax Canada Inc. v. Privacy Commissioner of Canada
Federal Court File No. T–1937–06

The extent of the Privacy Commissioner's powers under *PIPEDA* was also challenged in a case involving her decision to initiate an audit under subsection 18(1) of Equifax's personal information management practices, specifically its online authentication system. After the Commissioner delivered her notice of intention to audit, Equifax filed a Notice of Application in the Federal Court asking for a review into whether the Commissioner had the necessary reasonable grounds to initiate the audit. Notwithstanding that Equifax maintained its position that the

Commissioner did not have reasonable grounds to initiate the audit, the audit was nonetheless conducted and a report will be delivered to the credit agency. As a result of the cooperation between the parties to see the audit completed, the organization withdrew its court application.

Complainant-initiated court applications under section 14 of PIPEDA

The Privacy Commissioner was an added party in the Federal Courts in seven cases last year. Examples of such cases are described below.

Alta Flights (Charters) Inc.
Federal Court of Appeal File No. A–184–05

This was an appeal from a decision of the Federal Court dismissing a complaint by an individual under section 14 of the Act alleging that her employer, Alta Flights (Charters) Inc., had collected personal information without her consent or knowledge in breach of her rights under *PIPEDA*. In 2005, the Federal Court found no evidence supporting the individual's contention that her conversations were recorded on a digital recorder her manager had taped to the underside of a table in the employees' smoking room. (The machine had malfunctioned and fallen to the floor.) The Court held that, while the manager had attempted to collect personal information without the employee's consent, there was no "collection" of personal information as defined within *PIPEDA*. The individual complainant appealed the decision. On March 21, 2006, the Federal Court of Appeal dismissed the appeal, confirming the decision of the Federal Court. While the manager's surreptitious activities constituted an unsuccessful attempt to illicitly collect personal information, *PIPEDA*, in its current form, does not prohibit such attempts.

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

This case arose when some Telus employees objected to the company's implementation of a voice-recognition system. The system required employees to create a "voice-print" which would be stored on a Telus server. Every time employees attempted to gain access to certain parts of the Telus network, they would have to authenticate themselves by having their voice matched to their voice-print.

The 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 the consent requirement in *PIPEDA* 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* which allow for the non-consensual collection apply to these circumstances; and (v) Telus properly informed employees of all the consequences that might arise if they refused consent.

Interestingly, the Court of Appeal left for another day the question of whether Telus could impose disciplinary measures on employees who refuse to provide their consent. The Court considered that this issue would be better dealt with by the appropriate "labour law forum."

Dr. Jeffrey Wyndowe (Psychiatric Assessment Services Inc.)
Federal Court File No. T–711–05

At issue was whether an individual could receive access to his personal information contained in notes taken by a physician who had conducted an independent medical examination of his medical condition on behalf of an insurance company. The physician in this case refused to provide the individual with access to his notes. The Federal Court concluded, as the Assistant Privacy Commissioner had, that the doctor's notes contained the individual's personal information and had to be provided to the individual as per his rights under *PIPEDA*. The solicitor-client privilege exception in paragraph 9(3)(*a*) did not apply in this case as the notes were not produced for the dominant purpose of litigation. Nor did the exception in paragraph 9(3)(*d*) apply, as the notes were not produced in the context of a formal dispute resolution process either.

The Court disagreed with the physician's assertion that his notes fall outside the scope of *PIPEDA* on the basis that he was not the individual's treating physician and, therefore, was under no professional duty to provide access to medical records. The Court held that, regardless of the policy considerations argued to the contrary, *PIPEDA* clearly provides a general right of access to one's personal information and does not provide for any exception that would apply to this case. The Court ordered the physician to provide the individual access to his notes. The physician has appealed this decision to the Federal Court of Appeal.

Monitoring Function

As part of our larger court monitoring function, the OPC continued to monitor several court cases involving novel privacy issues. We stay abreast of possible advancements in the law, whether they be advanced through applications under *PIPEDA*, applications under the *Privacy Act*, the federal *Access to Information Act*, or even actions in the superior courts of the provinces under the common law or civil law in Quebec.

Public Education and Communications

According to section 24 of *PIPEDA*, the Privacy Commissioner is mandated to undertake public education, communications and research activities that help organizations both understand and meet their obligations under the Act.

The law specifically states the Commissioner must:

- *develop and conduct information programs to foster public understanding, and recognition of the purposes of Part 1 of PIPEDA, which deals with personal information protection in the private sector*
- *undertake and publish research related to the protection of personal information, including any such research requested by the Minister of Industry*
- *encourage organizations to develop detailed policies and practices, including organizational codes of practice, to comply with sections 5 to 10*
- *promote, by any means the Commissioner considers appropriate, the purposes of Part 1*

In 2006, we worked hard to increase the public profile of the OPC. We adopted a more proactive media strategy, issuing press releases on a wide range of topics, and senior officials gave dozens of speeches and presentations across the country and abroad.

Public opinion research

We commissioned a public opinion survey from Ekos Research Associates entitled, *Revisiting the Privacy Landscape a Year Later*. It was a follow-up to a 2005 poll conducted by Ekos that provided a snapshot of Canadians' views on a number of important privacy issues. Noteworthy findings included the following:

- More than 70 per cent of Canadians feel they have less control of their personal information than they did 10 years ago.
- Two-thirds of Canadians view privacy as one of the most important challenges Canada will face over the next decade.
- Respondents expressed dissatisfaction with how they perceive their information to be handled and are concerned about future threats from increasingly invasive technologies and anti-terrorism measures.

Media relations

We provided a large number of media interviews related to our investigations into the Society for Worldwide Interbank Financial Telecommunication (SWIFT). We also participated in many interviews about our audit of the Canada Border Services Agency (CBSA).

Our investigative work involving workplace surveillance also garnered a great deal of media interest. At year-end, we issued news releases outlining tips for protecting personal information while holiday shopping, and ideas for privacy-related New Year's resolutions. Our suggestions were picked up by news outlets across the country.

Speeches and special events

In 2006, we once again attended a range of conferences, meetings and special events, reaching out to stakeholders in Canada and abroad, and keeping ourselves up to date on the fast-changing data protection world.

In total, OPC representatives made over 70 presentations, several focused on *PIPEDA*. These included addresses to the Retail Council of Canada in Toronto, the Barreau du Québec, and an access and privacy conference organized by the University of Alberta.

We continued our bi-monthly privacy lecture series, offering insights on privacy issues and future trends to audiences that include government representatives, academics, members of the private and non-profit sectors as well as OPC staff.

International activities included attendance at international data protection conferences and meetings of the Asia-Pacific Economic Cooperation (APEC) and the Organization for Economic Co-operation and Development (OECD), and consultations with various US agencies. These opportunities allow us to advocate for strong international privacy standards, with a view to preventing the compromise of Canadians' personal information when being processed in other countries.

As part of our ongoing efforts to stimulate a global discourse on privacy, our Office will host the 29th International Conference of Data Protection and Privacy Commissioners. The event will bring together hundreds of data protection authorities, privacy advocates, privacy practitioners, academics and security professionals from around the world. Called *Privacy Horizons: Terra Incognita*,

the conference will address leading-edge issues in the privacy domain – including biometrics, Radio Frequency Identification (RFID), surveillance, and youth privacy.

Publications and Web site

Each year, our Office disseminates a wide range of information to individuals and organizations inquiring about privacy matters – annual reports, *PIPEDA* guides, fact sheets, and copies of *PIPEDA* and the *Privacy Act*. Increasingly, these documents are being accessed from our Web site.

One noteworthy document published to the Web in 2006 was a *PIPEDA* review discussion paper, *Protecting Privacy in an Intrusive World*. The paper captures several issues identified by the OPC for consideration by the Standing Committee on Access to Information, Privacy and Ethics during its review of *PIPEDA*. Input was invited from individuals and organizations. The feedback we received helped to shape our subsequent submission to Parliament.

In addition, we posted a Questions and Answers document for individual Canadians explaining how they could go about filing a Federal Court application under *PIPEDA*, hopefully de-mystifying the process for them so they can more meaningfully exercise their legitimate rights.

The OPC Web site has seen a steady and significant increase in visits over the last several years. It has become an important mechanism for sharing information with different audiences. In 2006, the site had more than 1.2 million visitors – up dramatically from approximately 500,000 in 2002, the first full year we tracked hits. Throughout the year, we continued to post speeches, fact sheets, news releases, links and *PIPEDA* case summaries, so visitors understand how the law applies in various circumstances.

In 2007, we will add a dynamic tool to the site: an e-learning module for the retail sector designed to clarify the proper process for collection and handling of personal information. Most of the groundwork for this interactive tool, developed in close consultation with the Retail Council of Canada, was completed in 2006.

OPC Administration

In 2006, we focused on implementation of the OPC business case and strengthening of our human resources management capacity.

Planning and reporting

With an eye to ensuring the efficient and effective administration of the OPC, we continue to have complete planning cycles – from our *Report on Plans and Priorities* to departmental performance reports. We also integrated all aspects of planning (financial, human resources, information technology/information management). We will take that a step further in the next fiscal year by incorporating our performance measurement framework into branch plans, and by implementing the required templates and tools to report on results against objectives at the 2007 fiscal year-end.

Finance and administration

The OPC has received clean audit opinions of its financial statements from the Office of the Auditor General (OAG) of Canada each year since OAG audits began in 2003-04. The OPC continuously enhances its financial management practices by reviewing, streamlining and strengthening its financial policies and procedures, and by enhancing communication and training for OPC staff.

Financial information

The OPC's financial framework is based on the government fiscal year, not the calendar year. For *PIPEDA*, we are required to report on the calendar year; for the *Privacy Act*, on the government fiscal year. For this reason, and to avoid confusion, we have not included the OPC financial tables in this report. They are, however, available in our *Report on Plans and Priorities*, as well as our departmental performance reports (www.privcom.gc.ca).

Human resources

The OPC has entered an important phase of institutional renewal, inspired by a leadership philosophy that promotes core public-service values and ethics, and in compliance with the *Public Service Modernization Act* (PSMA), the *Public Service Employment Act* (PSEA), the *Public Service Labour Relations Act*, and the *Federal Accountability Act*.

In May 2006, the Public Service Commission removed the restrictions that had been imposed on the OPC staffing authority in 2003. The OPC subsequently made significant improvements to its staffing management framework, systems and practices, in consultation with central agencies and unions. These included development of:

- new mechanisms for communication between management and employees and the introduction of a self-monitoring process
- an Instrument of Delegation of Human Resource Management – a tool to guide managers with human resource management
- a Strategic Human Resource Plan and a new Staffing Strategy, as well as an Employment Equity Action Plan, to ensure the recruitment of a qualified and diversified workforce representative of Canadian society
- a monthly internal newsletter designed to improve transparency of staffing processes
- briefings delivered at quarterly all-staff meetings and senior management sessions regarding relevant components of the new PSMA and PSEA

The OPC further created a comprehensive organizational Learning Strategy and Curriculum, in collaboration with the Canada School of Public Service. This will allow staff to enhance their expertise and competencies, and position them to take on new responsibilities. The curriculum incorporates training in areas such as values-based staffing, language, performance management, employee appraisals, and harassment awareness in the workplace. It includes management training on the new PSEA.

Information management/information technology

Strong information technology and information management systems are crucial to the operations of the OPC and represent a significant portion of our budget. Several important initiatives were either completed or significantly advanced in 2006. We:

- prepared a Business Continuity Plan and purchased all equipment for the OPC's disaster recovery site to ensure our work could continue in the event of a natural disaster or some other emergency;
- updated our Threat and Risk Assessment framework and began development of measures to strengthen our security posture;
- surpassed the halfway mark in our Information Management project to ensure we are compliant with a Treasury Board information holdings policy and began evaluating potential replacements to our case tracking system;
- secured a research facility for our legal branch;
- completed zoning of our servers, put in place a server backup strategy, and began development of change management procedures for effective and timely server patching; and
- acquired new computers and other IT infrastructure to support new employees.

APPENDIX 1

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.

Case summaries of the Commissioner's findings under *PIPEDA* are available on the OPC Web site, www.privcom.gc.ca.

APPENDIX 2

Investigations Received by Complaint Type

Complaints received between January 1, 2006 and December 31, 2006

Complaint type	Count	Percentage
Access	84	20
Accountability	11	3
Accuracy	11	3
Challenging Compliance	3	<1
Collection	75	18
Consent	13	3
Correction/Notation	8	2
Fee	3	<1
Openness	1	<1
Retention	11	3
Safeguards	34	8
Time Limits	17	4
Use and Disclosure	153	36
Total complaints	**424**	

Breakdown by Sector

Complaints received between January 1 and December 31, 2006

Sector	Count	Percentage
Financial Institutions	108	25
Insurance	51	12
Telecommunications	55	13
Other	56	13
Sales	58	14
Transportation	37	9
Accommodation	29	7
Professionals	11	2
Health	7	2
Services	7	2
Rental	5	1
Total complaints	**424**	

Closed Complaints by Complaint Type

Complaints closed between January 1, 2006 and December 31, 2006

Complaint type	Count	Percentage
Access	51	16
Accountability	5	2
Accuracy	9	3
Challenging Compliance	2	1
Collection	74	24
Consent	11	3
Correction/Notation	4	1
Fee	6	2
Openness	1	0
Other	5	2
Retention	6	2
Safeguards	18	6
Time Limits	6	2
Use and Disclosure	111	36
Total closed complaints	**309**	

Closed Complaints by Finding

Complaints closed between January 1, 2006 and December 31, 2006

Finding	Count	Percentage
Discontinued	35	11
Early Resolution	15	5
No jurisdiction	8	3
Not well-founded	65	21
Other	2	0
Resolved	62	20
Settled	81	26
Well-founded	14	5
Well-founded Resolved	27	9
Total closed complaints	**309**	

Findings by Complaint Type

Complaints closed between January 1, 2006 and December 31, 2006

	Discontinued	Early Resolution	No Jurisdiction	Not Well-founded	Other	Resolved	Settled	Well-founded	Well-founded Resolved	TOTAL
Access	6	0	1	7	0	19	14	1	3	**51**
Accountability	0	0	0	0	0	0	3	1	1	**5**
Accuracy	0	0	0	4	0	2	3	0	0	**9**
Challenging Compliance	0	0	0	1	0	0	1	0	0	**2**
Collection	6	3	2	20	0	23	15	3	2	**74**
Consent	1	1	0	5	0	1	3	0	0	**11**
Correction/ Notation	1	0	0	2	0	1	0	0	0	**4**
Fee	0	0	0	0	0	5	0	0	1	**6**
Openness	0	0	0	1	0	0	0	0	0	**1**
Other	1	0	0	1	2	0	1	0	0	**5**
Retention	0	0	0	1	0	2	3	0	0	**6**
Safeguards	4	3	1	1	0	2	4	0	3	**18**
Time Limits	0	0	0	2	0	1	1	2	0	**6**
Use and Disclosure	16	8	4	20	0	6	33	7	17	**111**
TOTAL	**35**	**15**	**8**	**65**	**2**	**62**	**81**	**14**	**27**	**309**

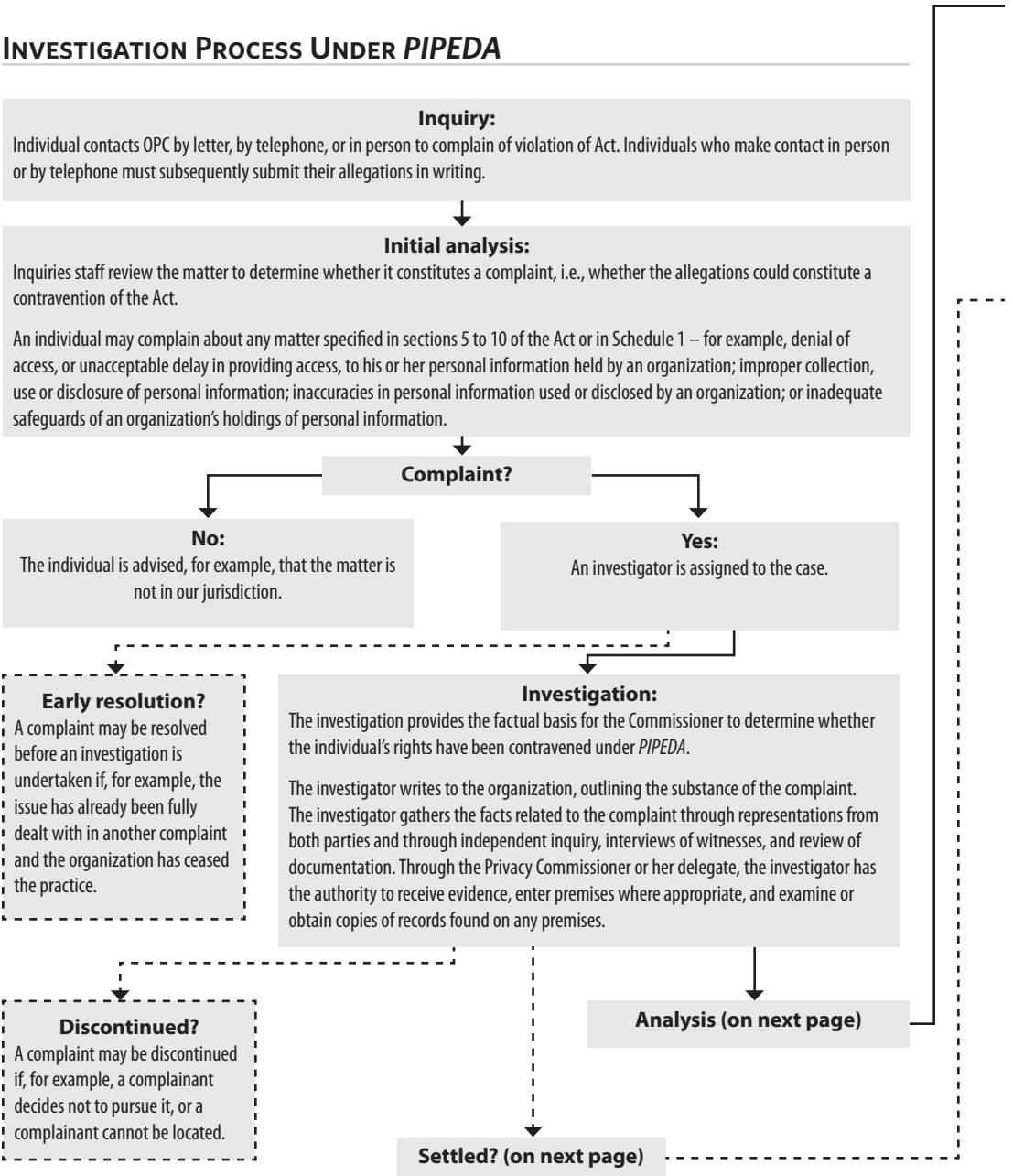
Findings by Private Sector Industry

Complaints closed between January 1, 2006 and December 31, 2006

	Discontinued	Early Resolution	No Jurisdiction	Not Well-founded	Other	Resolved	Settled	Well-founded	Well-founded Resolved	TOTAL
Accommodations	0	1	0	2	0	3	11	2	0	**19**
Financial Institutions	6	1	4	25	0	15	19	7	15	**92**
Health	1	0	1	7	0	5	1	0	2	**17**
Insurance	1	0	0	13	0	9	10	0	2	**35**
Other	5	0	2	6	0	2	10	0	2	**27**
Professionals	1	0	0	0	0	0	0	2	1	**4**
Rental	0	0	0	0	0	0	2	0	0	**2**
Sales	3	11	0	3	0	1	5	0	3	**26**
Services	0	0	0	1	0	0	1	0	0	**2**
Telecommunications	10	2	0	4	0	24	13	1	1	**55**
Transportation	8	0	1	4	2	3	9	2	1	**30**
TOTAL	**35**	**15**	**8**	**65**	**2**	**62**	**81**	**14**	**27**	**309**

Number of complaints in abeyance on December 31, 2006: 76

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 Branches, as appropriate.

Settled?

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

Findings:

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

Preliminary report

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

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.