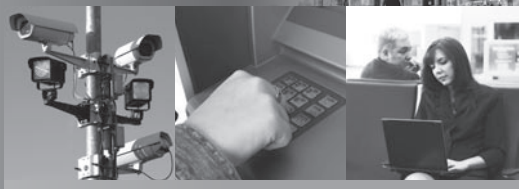
Privacy Commissioner of Canada

Commissaire à la protection de la vie privée du Canada

Privacy

Annual Report to Parliament 2005



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

Cat. No. IP51-1/2005-1
ISBN 0-662-69647-6

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 2006

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

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Personal Information Protection and Electronic Documents Act* for the period from January 1 to December 31, 2005.

Yours sincerely,

Original signed by

Jennifer Stoddart
Privacy Commissioner of Canada

Privacy Commissioner of Canada

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.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 2006

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

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Personal Information Protection and Electronic Documents Act* for the period from January 1 to December 31, 2005.

Yours sincerely,

Original signed by

Jennifer Stoddart
Privacy Commissioner of Canada

Table of Contents

Foreword

I would like to report much good news about privacy in Canada. But it's not all good news. Concern among Canadians about their loss of privacy and the misuse of their personal information has never been greater. This concern stems from the growing threats to personal information in an electronic environment of massive and continuous data circulation.

Current private sector data protection legislation takes us only part way towards offering adequate privacy protection. The *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) has now been in full force for two years. This law has brought Canadians outside Quebec a comprehensive suite of informational privacy rights. (Quebec adopted its own private sector privacy legislation in 1994.) It has introduced a corresponding range of obligations for organizations that collect, use and disclose personal information.

In the wake of *PIPEDA*, several provinces have moved to adopt their own legislation, which were later declared to be "substantially similar" to the standards in *PIPEDA*. British Columbia and Alberta did so in 2003, and Ontario (in health privacy matters) in 2005.

PIPEDA is slated for review by Parliament in 2006. This review is vital. It will present a unique opportunity to examine the Act's effectiveness in protecting one of our cherished Canadian rights, informational privacy. It will also give Parliamentarians and the Canadians they represent the chance to respond to growing attacks on personal information through identity theft, spam and fraudulent on-line activities.

Despite their limitations, *PIPEDA* and the substantially similar provincial laws have promoted a sea change in attitudes toward personal information protection in Canada. Canadians now expect organizations to justify collecting and using personal information. They are becoming increasingly vocal and articulate about the handling of their personal information.

The last few years have also created challenges for organizations covered by *PIPEDA* as they have moved, at different rates and with varying degrees of success, to implement the privacy principles of *PIPEDA*. Overall, the information handling practices brought to our attention show Canadian organizations demonstrating a high level of compliance with *PIPEDA*. Businesses, large and small, have demonstrated goodwill, commitment to community values and openness to change when it comes to protecting privacy. But I am concerned that apparent compliance does not always result in truly effective privacy and security practice. Goodwill needs to be translated into practice.

Technology, consumer trends and national security concerns continue to introduce novel uses for personal data and, indeed, require ever greater amounts of it. We must revisit how we define and apply our operating rules. How adequate are these rules in the world of the Internet, mini-computers in cars, tracking tags in clothing, satellite-assisted surveillance of neighbourhoods, and the outsourcing of data processing to countries lacking effective data protection standards? Even if we have a reliable framework for privacy protection in Canada, these protections do not always extend beyond our borders. Nor do they effectively control actions that, via the Internet, reach into Canada and use our personal information in ways that do not respect the principles of *PIPEDA*.

At the Office of the Privacy Commissioner of Canada (OPC), we continue to support privacy values through education, outreach, complaint resolution and other preventive measures. As an ombudsman, I promote voluntary compliance with privacy principles, and their adaptation to specific industry and consumer needs. I am pleased that the recent trend towards settling the privacy complaints made to my Office is continuing. Almost half of all complaints are settled to the apparent satisfaction of all parties.

As familiarity with privacy standards increases, so does the expectation that they will be observed. It is no longer acceptable that violations of personal information protection norms do not lead to direct remedial action. In 2005, I began asking organizations that are the subject of well-founded complaints to state the corrective measures they would take. I would then decide whether to seek a remedy for the

complainant in Federal Court. To date, in the few situations where I have used this approach, almost all organizations have rapidly committed to providing redress and making systemic changes.

We continue to monitor whether the systemic changes we recommended have occurred in response to complaints made in previous years. Again, the overall compliance rate is high and, once we intervene following a complaint, the level of cooperation by organizations is generally commendable.

However, it is difficult, if not impossible, to complain about misuse of personal information if individuals do not understand how their information is being used. The opaque nature of our technology-driven world means increasingly that only specialists understand the flows and uses of personal information. Because Canadians themselves may not fully understand the handling of their personal information, my Office has to rely on other indicators of privacy problems beyond those that surface through public complaints. We now use a variety of additional approaches including audit, review of information management systems, personal information assessments, public information and education to empower individuals and to help businesses with compliance, research on new issues and, where necessary, legal action.

Our mandate under *PIPEDA* is broad and demanding, and we have been hobbled by perennial uncertainty over funding. We have not had permanent funding to carry out our mandated activities under *PIPEDA*, as funding for the new law was granted initially only until 2003 and then renewed annually. *PIPEDA* has now been in full force since 2004 and the pressures are increasing. We have requested a substantial multi-year increase in our funding base and are planning for significant growth. Adequate funding will enable us to do the job our legislation requires of us. It will allow us to meet the challenge of responding to the ever-growing appetites of commercial and governmental interests for our personal information.

I would also like to commend the Honourable Gérard V. La Forest for his study on the possible merger of the offices of the Information Commissioner and the Privacy Commissioner. He concluded that a privacy-focused structure is the most appropriate framework for enforcing Canada's privacy legislation. Retaining this structure also avoids the inevitable administrative upheaval that would flow from merging the two offices. It is far better at this time that our Office continues to focus our energies on the privacy issues that we now face, and that continue to emerge, in abundance.

Our Strengthened Mandate

To date, our Office has not received permanent funding to carry out its duties under *PIPEDA*. Funding was granted for three years only. *PIPEDA* came into force in stages, beginning in 2001 and reaching full implementation in 2004, and we thought it important to let the dust settle before we attempted to identify long-term financial needs. *PIPEDA* has now been in full force for two years, and the demands made of us under the Act are increasing. Current funding levels leave us unable to carry out our multi-faceted mandate. For example, we face a significant backlog of complaints, and complainants are, quite understandably, becoming impatient. The small size of our team of auditors makes it impossible to conduct effective audits to ensure compliance. Even though we have adopted a risk-based approach, we need to intensify our audit activities. Funding limits also mean that our communications strategy is primarily reactive, when proactive public education about privacy rights and obligations is required instead. Similarly, our Policy and Research Branch and our Legal Services Branch are confined to putting out existing privacy fires, rather than anticipating and therefore more effectively addressing emerging privacy issues.

In the past few years, the Office went through an extremely challenging period. However, every cloud has a silver lining. In this case, the silver lining was an opportunity to review the functioning of the Office, in detail, from top to bottom. The result is an Office of the Privacy Commissioner of Canada that is pointed in the right direction. It is now time to put forward the Office's new vision and we need the full set of tools to implement it.

We are attracting new and highly specialized talent to our team. We have pursued an ambitious agenda to correct deficiencies in management of the organization. Audits and evaluations of our Office – by the Auditor General of Canada, the Public Service Commission and the Canadian Human Rights Commission – have so far been positive. And we have implemented a thoughtful, systematic process to determine

our organizational needs. This Office is now again an institution worthy of the trust of Parliament and the Canadians it serves.

The Vision of the Office of the Privacy Commissioner of Canada

The Office has prepared two analyses of significance – a Vision and Institutional Service Plan, and a Business Case for Permanent Funding. Together, these describe who we need to be, for Canadians and on behalf of Parliamentarians, and what it takes to get us there.

If funded appropriately, the Office can accomplish the following in relation to the activities regulated under *PIPEDA*:

- undertake a meaningful number of audits and reviews to encourage greater compliance, and assist in developing a robust privacy management regime in the private sector;
- conduct legal and policy analyses of bills and legislation to assist Parliament;
- make more proactive, extensive and effective use of the enforcement tools entrusted to us by Parliament, including Commissioner-initiated complaints, court actions and public interest disclosures;
- carry out research into emerging privacy issues and trends to help citizens and policy makers understand current and future privacy challenges;
- engage in extensive public education to better inform individuals of their rights, and organizations of their obligations;
- through a streamlined investigation process, tackle the growing backlog of privacy complaints; and, finally,
- sustain institutional renewal efforts.

Business Case: Resources

After a thorough analysis that included a Business Process Review of the investigations and inquiries functions and an in-depth review of all other functions, the Office requested a greater than 50 per cent increase in resources. The OPC is now planning for an increase within the next two years, to approximately 140 employees and an overall annual budget of approximately $18 million.

Long-term, stable and increased funding is imperative for the OPC, for Canadians, and for the organizations covered by federal privacy laws. The OPC plans to move away from being predominately complaint-driven to a more multi-disciplinary approach, one that is more proactive than reactive, and one that better reflects the mandate given to us by Parliament.

Policy Perspective

Standing on Guard for Privacy

The focus of research and policy activity this year continued to relate to the provision of enhanced ability for law enforcement and national security agencies to obtain personal information. We reported on this extensively in the 2004-05 annual report on the *Privacy Act*, and will do so again in this coming year's annual report on that Act. The issue also merits mention here because legislation discussed or introduced in Parliament this year seeks to compel private sector organizations to release personal information.

The Commissioner appeared before the Senate Special Committee on the *Anti-terrorism Act* (ATA) on May 9, 2005. The accompanying position statement of our Office stressed the growing surveillance powers of the state as it seeks access to private sector repositories of personal data:

> *Since 9/11, the Canadian government has introduced a series of measures to strengthen its surveillance powers over the citizens and residents of Canada. It also has massively invested in the development of integrated information systems that collect, process and share citizens' and residents' personal information, in a wide range of aspects of their economic and civic life: as travelers, investors, consumers, and recipients of social programs, to name a few.*
>
> *These information systems cross organizational and jurisdictional boundaries, and redefine the parameters of time and space. Records can now be kept indefinitely, accessed through delocalized nodes, and combined and aggregated to scrutinize virtually all aspects of private life. Systems to cross-tabulate and data-mine personal information are used to categorize, sort and classify people, and to infer, deduce, and make predictive judgments on individual attitudes*

> *and behaviors. Many of the systems, through the use of biometrics, delve deeply into the personal realm of identity.*

The Commissioner appeared before the House of Commons Subcommittee on the Public Safety Act and National Security on June 5, 2005, to comment on the ATA, and issued similar warnings. While many concerns related to oversight of the agencies which have special powers under the *Anti-terrorism Act*, the Office raised concerns throughout the year that *PIPEDA* was being eroded by government access to private sector databases containing personal information. We are gravely concerned that information gathered for private or commercial reasons is finding its way into government hands. This amounts to a blurring of the public and private sectors, leading to the potential use of private sector companies as agents of the state, often without the safeguards that are elemental in a democracy. We must stand on guard against state access to the databanks of the corporate world. Fears of terrorist attacks or impending pandemics provide superficially attractive justifications for intrusive powers, but the real need for these powers is often not apparent.

Some may argue that the *Privacy Act* can soften the edges of these intrusive powers. However, the Act, which governs government information collection and practices, is more than 20 years old and too antiquated and weak to provide meaningful oversight and redress for those who have been wronged. The Act was drafted even before the advent of desktop computers, let alone the myriad of other advances that enable surveillance at the push of a button.

On November 15, 2005, the Minister for Public Safety and Emergency Preparedness Canada introduced Bill C-74, *An Act regulating telecommunications facilities to facilitate the lawful interception of information transmitted by means of those facilities and respecting the provision of telecommunications subscriber information*. Although the Bill died when Parliament was dissolved for the January 2006 federal election, the Bill or a variant may well be reintroduced.

The Bill would have required telecommunications service providers to establish and maintain certain capabilities to facilitate the lawful interception of information transmitted by telecommunications. The Bill would also have required telecommunications service providers to provide basic information about subscribers to the RCMP, the Canadian Security Intelligence Service (CSIS), the Commissioner of Competition and any police service constituted under the laws of a province. The legislation would have lowered the standard (at present, a warrant) that must be met to obtain disclosure of personal information. Among the main provisions of the legislation were the following:

- the requirement that all wireless, wireline, Internet and other telecommunications service providers be required to maintain existing intercept capabilities, and build in intercept capability as they upgrade their networks. Companies would be audited to ensure they are complying;
- the ability of law enforcement agencies, namely the RCMP and any police service constituted under the laws of a province, CSIS or the Commissioner of Competition, to require telecommunications service providers to surrender certain subscriber data (name, telephone number, address, e-mail address, IP address) upon request, without any judicial authorization. This would represent a change from the present situation where, under section 7(3)(c.1) of *PIPEDA*, companies are permitted to refuse requests unless they are accompanied by judicial authorization. Bill C-74 would have eliminated this discretion.

The former Bill C-74 would have also required providers to:

- enable the interception of communications generated by or transmitted through the service provider's network;
- deliver the intercepted communications to law enforcement agencies and CSIS;
- isolate or separate a communication that is authorized to be intercepted from other information/communications;
- enable simultaneous interceptions, by authorized persons from multiple national security and law enforcement agencies, of communications of multiple users. This means, for example, that a telecommunications company would have needed the capability to allow more than one agency to intercept multiple communications at the same time. The maximum capability that the Bill would have required was one intercept for every 5,000 subscribers.

Although this legislation was introduced in late 2005 and was not adopted, it is an excellent example of the growing reliance on private sector companies as "agents" of the state. Electronic surveillance of communications – "wiretapping" – is far from a new phenomenon, but what wiretaps produce in the age of electronic commerce and delivery of multiple services over the Internet is vastly greater than what flowed from tapping a telephone line. We expect that the privacy issues raised in the former Bill C-74 and any successor would preoccupy this Office and many civil liberties groups in 2006.

We also watched with interest the consultation undertaken by the Department of Finance on revising the anti-money laundering/anti-terrorist financing (AML/ATF) regime to meet international commitments. Canada is a member of the Financial Action Task Force (FATF), the international inter-governmental agency that establishes and oversees AML/ATF initiatives. In our letter to the Department, we stressed that not all countries are the same, and that Canada happens to have a well-regulated financial industry with significant privacy legislation governing financial records and institutions. We recognized the need to ensure that Canada does not become a safe haven for money launderers, but also stressed that Canada should not be expected to adopt every measure proposed by the FATF without critical scrutiny of the measure's privacy implications.

The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (*PCMLTFA*) significantly weakens the protections provided by both *PIPEDA* and the *Privacy Act*. An individual's ability to lodge a complaint, and the Privacy Commissioner's power to investigate the complaint, are meaningless, given the secrecy surrounding the collection of personal information by the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). FINTRAC's mandate is to assist in the detection, prevention and deterrence of money laundering, terrorist activity financing and/or threats to the security of Canada. The secrecy surrounding the collection of information by FINTRAC will prevent members of the public from knowing that information is being collected about them or that they are being investigated. We are seeing calls for more information to be scooped up in this net of financial surveillance, all without the knowledge of the individual, and we must protest the lack of attention to the very real privacy issues that flow from this expansion in the surveillance powers of government.

In May 2005, a multi-stakeholder task force struck by the Minister of Industry reported on a one-year study of the problem of unsolicited email, or "spam." Our Office participated on this task force, and we were gratified to see a strong commitment from the Minister to move forward rapidly to combat a pestilence that is undermining trust in the Internet and exposing hapless computer users to scams, identity theft, and even malevolent software or "spyware" that surreptitiously invades and compromises computers and the information they hold. As with many other important issues, the Office has received relatively few complaints on the use of email address information without consent. However, this is a much more significant issue than the limited number of complaints would suggest. We look forward to further government action in 2006.

Most spam originates outside Canada. This is a significant problem, since it is very difficult to investigate and prosecute the originators of spam. A similar difficulty arises with many other Internet scams, and even with legitimate businesses outside Canada collecting and processing personal information. We have struggled with this issue in a number of *PIPEDA* complaints this year. In response, we are now placing greater emphasis on harmonized international solutions and cooperation among data commissioners. In 2004, we reported on the significant concerns raised by the *USA PATRIOT Act* for the personal information of Canadians held both outside and inside Canada, and on the extensive investigation of this issue by the B.C. Information and Privacy Commissioner. Governments at both provincial and national levels need to remain alert to this and other issues related to the outsourcing of personal information.

We must all work more effectively at the international level to find solutions to the privacy issues flowing from outsourcing, just as law enforcement has attempted to address crime and money laundering internationally. Our data protection agencies simply do not have the resources (or the legal authority) to chase perpetrators on foreign soil, so it is in our interest to work towards harmonized international standards and approaches. Canada benefits enormously from outsourcing, so we are good candidates to advance solutions that work for exporters, processors and individuals. And we find it more important than ever to communicate with international bodies that focus on ways of increasing international cooperation in a number of areas. The Commissioner was invited by the Organisation for Economic Co-operation and Development (OECD) to play a significant role in trans-border cooperation, and work started in the autumn of 2005. To this end as well, the Assistant Commissioner for *PIPEDA* has attended meetings in Korea and Hong Kong this year on the Asia-Pacific Economic Cooperation (APEC) Privacy Guidelines. The participation and expertise of the Government of Canada in this exercise has clearly exerted a positive influence on the Guidelines, bringing them closer to the Canadian data protection model. The Assistant Commissioner also attended a meeting on travel documents hosted by the OECD and the International Civil Aviation Organization (ICAO) in Britain.

The Commissioner, the Director General Legal Services and the Director of Research and Policy attended the International Data Protection and Privacy Commissioners Conference in Switzerland in September 2005. Our Office will be hosting the 2007 International Data Protection and Privacy Commissioners Conference. We look forward to welcoming more than 60 data commissioners and their staff, as well as members of privacy advocacy groups and the business community, among others,

from Canada and around the world, and to working on practical ways to implement data protection measures, wherever personal data may be held. A common focus on technological issues such as biometrics, Radio Frequency Identification (RFID), standards for authentication and identity management, and surveillance devices, will hasten implementation of measures to better protect privacy and reduce costs for business.

The Year in Parliament

The Office had a busy year in its relations with Parliament in 2005. A key component of our work involves appearing before Senate and House of Commons committees to provide expert advice on the privacy implications of bills and other policy matters under consideration by Parliament.

The Office was called on to appear before parliamentary committees 16 times this year – a considerable challenge for our small organization. Yet because the Privacy Commissioner is an Officer of Parliament, such appearances are central to her duties.

A key Committee for the Office is the relatively new Standing Committee of the House of Commons on Access to Information, Privacy and Ethics (ETHI). Established in late 2004, this Committee is significant in that with its creation, Canadians now have a standing committee of the House of Commons dedicated to privacy matters. The Privacy Commissioner of Canada and other OPC officials appeared four times before the ETHI Committee in 2005. While one reason for these appearances was to question us on the operations of our Office through examination of our Estimates and Annual Reports, MPs on the Committee also had many questions and concerns regarding some of the key privacy challenges and opportunities facing Canadians. The OPC looks forward to a continued, productive working relationship with this Committee in the 39th Parliament. As privacy issues continue to grow in number and complexity, it is vital that Parliament have a focus to examine these issues and reflect on the concerns expressed by Canadians.

The overwhelming majority of our appearances before parliamentary committees involved bills and policy issues that relate to the *Privacy Act,* but three dealt with issues relating primarily to *PIPEDA*.

❋ *Senate Study of the Financial Services Sector*

On February 16, 2005, we appeared before the Standing Senate Committee on Banking, Trade and Commerce to assist with its study of consumer issues in the Canadian financial services sector. The Senate had asked the Committee to examine the impact of federal legislation and initiatives designed to protect consumers within the financial services sector. The Committee was also asked to review the effectiveness of agencies that play a role in consumer protection and supervision of the financial services sector.

As the complaints statistics set out in this annual report show, we receive more complaints about financial institutions than about any other industry. This has been true every year since 2001, the year the first phase of *PIPEDA* came into force. However, as we advised the Senate Committee, this does not necessarily mean that financial institutions are failing to comply with *PIPEDA*. We suspect instead that it reflects the amount and the sensitivity of personal information that banks and other financial institutions are required to collect, the central role they play in our day-to-day lives, and perhaps the complexity of our relationships with these institutions.

Many complaints we receive do not flow from systemic problems. Instead, they are the result of actions by particular employees who failed to follow company policies and procedures. With complaints that we determine to be well-founded, financial institutions typically are prepared to adopt our recommendations for corrective action. As we indicated to the Senate Banking Committee, our Office generally has a very positive relationship with financial institutions.

The Senate Committee did not have the opportunity to table its final report because of the dissolution of Parliament with the federal election call. We look forward to continuing to work with the Committee on this study when the new Parliament is convened.

❋ *Bill C-37 and the "Do-Not-Call List"*

On June 8, 2005, we appeared before the House of Commons Standing Committee on Industry, Natural Resources, Science and Technology to provide our views on Bill C-37, *An Act to Amend the Telecommunications Act*. The Bill enables the Canadian Radio-television and Telecommunications Commission (CRTC) to establish a national do-not-call list. It also gives the CRTC the power to levy substantial penalties against telemarketers who do not follow the rules, and to contract with a private sector third party to operate the do-not-call service. Once the list is operational, Canadians who do not wish to receive calls from companies offering goods and services will be able to add their telephone numbers to a single, centralized list that telemarketers will be required to download regularly and respect. Both the United States and the United Kingdom have similar systems.

When we appeared before the Committee, we welcomed the establishment of a do-not-call list. However, we advised that the exemptions from the list that the Committee was considering not be introduced until after consultations with Canadians. When we appeared before the Committee, the OPC had the support of some ten privacy commissioners across Canada encouraging consultation with Canadians about these exemptions – for example, exemptions for charities, pollsters or businesses that had prior relationships with the customer.

The revised Bill adopted by Parliament contained several exemptions from the do-not-call list. The revised Bill did not prohibit unsolicited telecommunications made by or on behalf of a registered charity; a registered political party; a nomination contestant, leadership contestant or candidate of a political party; or an association of members of a political party. The Bill also did not prohibit unsolicited telecommunications to a person with whom the caller has an existing business relationship and who has not made a do-not-call request to that caller, and unsolicited telecommunications made for the sole purpose of collecting information for a survey of members of the public.

Bill C-37 received Royal Assent on November 25, 2005. We are pleased with its enactment, but the exemptions unnecessarily weaken the legislation.

❋ *Bill C-57 and Financial Institutions*

On November 15, 2005, we appeared before the House of Commons Standing Committee on Finance to address Bill C-57, *An Act to amend certain Acts in relation to financial institutions*. The Bill made changes to the corporate governance framework of banks, bank holding companies, insurance companies, insurance holding companies, trust and loan companies and cooperative credit associations to bring the acts governing those institutions up to the standards adopted in 2001 for business corporations under the *Canada Business Corporations Act*. The Bill also updated certain governance standards that are unique to financial institutions.

Bill C-57 contained only a few provisions relating to the collection, use or disclosure of personal information. These included a series of provisions requiring the directors or officers of banks and other financial institutions to report any interest they may have had in a material contract or material transaction with the bank or other financial institution. Related provisions allowed shareholders to review these disclosures. C-57 also allowed shareholders to obtain personal information about other shareholders, provided that the information would be used only for the purposes specified in the Bill.

When we appeared before the Committee, we did not have any significant concerns with the Bill from a privacy perspective. We found nothing that directly affected customer information. We argued that the new emphasis on corporate governance in the proposed legislation might even enhance privacy protection because it would force corporations to become more aware of the risks of poor management practices, and it would also result in corporations placing greater emphasis on security considerations.

Bill C-57 received Royal Assent on November 25, 2005.

Research into Emerging Privacy Issues

In 2005, the OPC awarded a total of $148,850 to five organizations through its Contributions Program for research into emerging privacy issues. This program has been part of our annual budget since 2000, but was made operational only in 2004. Studies conducted under the program delve into the thriving data brokerage industry, the use of DNA samples, workplace surveillance, and compliance with and enforcement of *PIPEDA*.

This is the second year of the program, which was launched in June 2004 to support research by not-for-profit groups, including educational institutions, industry and trade associations, and consumer, voluntary and advocacy organizations. Its goal is to further the development of a national research capacity in Canada on the broad spectrum of issues that have an impact on privacy.

The OPC is mandated to undertake and publish research related to the protection of personal information. The program was set up as part of the Office's budget pursuant to its program/legislative authority under *PIPEDA*.

Over the past two years, the Contributions Program has awarded a total of $520,440. Research bodies across Canada are invited to apply for grants to examine various privacy issues. After a thorough screening process, the organizations are then awarded the resources to initiate the research.

The following projects were funded in 2005:

Canadian Internet Policy and Public Interest Clinic **Ottawa, ON**	**The *PIPEDA*: Compliance Testing and Special Report on the Data-Brokerage Industry** *Evaluate organizational compliance with PIPEDA and research the growing data-brokerage industry*	$50,000
Ryerson University **Toronto, ON**	**Workplace Privacy - The Employer's Perspective** *Highlight some of the issues, concerns and interests that motivate employers in their adaptation of new workplace surveillance technology*	$36,150
University of British Columbia **Vancouver, BC**	**A Preliminary Exploration of Workplace Privacy Issues in Canada** *Explore the challenges to privacy in the workplace posed by current and emerging technologies*	$27,000
British Columbia Civil Liberties Association **Vancouver, BC**	***PIPEDA* Enforcement Evaluation** *Comparing PIPEDA's effectiveness to similar regimes in other jurisdictions*	$24,200
University of Ottawa **Ottawa, ON**	**Social Uses of DNA Information in the Context of Developing Policies and Analysis of two DNA related bills** *Exploration of the social uses of DNA by a comparative analysis of two DNA bills*	$11,500

The projects are expected to be completed in 2006. Links to the sites where they are published will appear on the OPC's web site.

Substantially Similar Provincial Legislation

Section 26(2)(b) of *PIPEDA* permits the Governor in Council to issue an order exempting an organization, a class of organizations, an activity or a class of activities from the application of *PIPEDA* with respect to the collection, use or disclosure of personal information that occurs within a province that has passed legislation that is substantially similar to *PIPEDA*.

The intent of this provision is to allow provinces and territories to regulate the personal information management practices of organizations operating within their borders and to promote a common standard for privacy protection throughout Canada and across sectors.

If the Governor in Council issues such an order, *PIPEDA* will not apply to the collection, use or disclosure of personal information by organizations subject to the provincial law. Personal information that flows across provincial or national borders will continue to be subject to *PIPEDA*, and the Act will continue to apply within a province to the activities of federal works, undertakings and businesses that are under federal jurisdiction – for example, banks, airlines and broadcasting and telecommunications companies.

Process for Assessing Provincial and Territorial Legislation

Industry Canada has announced that to be substantially similar, provincial or territorial laws must:

- incorporate the ten principles in Schedule 1 of *PIPEDA*;
- provide for an independent and effective oversight and redress mechanism with powers to investigate; and

- restrict the collection, use and disclosure of personal information to purposes that are appropriate or legitimate.

Substantially Similar Provincial and Territorial Legislation Enacted to Date

Our Office is required by section 25(1) of *PIPEDA* to report annually to Parliament on the "extent to which the provinces have enacted legislation that is substantially similar" to the Act.

In November 2003, the Governor in Council issued an Order in Council (P.C. 2003-1842, 19 November 2003) declaring Quebec's *An Act Respecting the Protection of Personal Information in the Private Sector* substantially similar. The Act, which predated *PIPEDA*, came into effect on January 1, 1994.

British Columbia and Alberta each adopted legislation in 2003 that applies to all organizations within the two provinces, except for those covered by other provincial privacy legislation, and federal works, undertakings or businesses that remain subject to *PIPEDA*. The two laws – both called the *Personal Information Protection Act* – came into force on January 1, 2004.

The Governor in Council has issued two Orders in Council (P.C. 2004-1163, 12 October 2004 and P.C. 2004-1164, 12 October 2004) exempting organizations, other than federal works, undertakings or businesses, in Alberta and British Columbia respectively, from the application of *PIPEDA*.

Ontario's *Personal Health Information Protection Act* (*PHIPA*) came into force on November 1, 2004. *PHIPA* establishes rules for the collection, use and disclosure of personal health information by health information custodians in Ontario. Health information custodians are individuals or organizations listed under *PHIPA* that, as a result of their power or duties, have custody or control of personal health information.

In September 2004, our Office informed Industry Canada that we believe *PHIPA* is substantially similar to *PIPEDA*. In November 2005, the Governor in Council issued an Order in Council (P.C. 2005-2224, 28 November 2005) exempting health information custodians in Ontario from the application of *PIPEDA*. As a result, Ontario health information custodians will not be subject to *PIPEDA* with respect to the collection, use and disclosure of personal health information. The Information and Privacy Commissioner of Ontario will be responsible for ensuring compliance

with *PHIPA*, including investigating complaints about the personal information practices of health information custodians within the province.

The Privacy Commissioner of Canada will continue to be responsible for oversight in relation to the collection, use and disclosure of personal health information that crosses provincial boundaries in the course of commercial activity. As well, our Office will continue to be responsible for personal health information collected, used or disclosed in the course of commercial activities by organizations that are not health information custodians.

Complaints

The year 2005 was the second year in which *PIPEDA* covered all commercial activities in provinces that do not have substantially similar legislation. We saw a large drop in 2005 in the number of complaints filed under *PIPEDA*. We received 400 complaints in 2005, compared with 723 in the previous calendar year.

Complaints received between January 1 and December 31, 2005 Breakdown by Sector	Count	Percentage
Financial Institutions	113	28.25
Insurance	60	15.00
Telecommunications	55	13.75
Sales	44	11.00
Transportation	39	9.75
Accommodation	17	4.25
Professionals	13	3.25
Health	4	1.00
Services	2	0.50
Rental	1	0.25
Other	52	13.00
Total	**400**	**100.00**

We can only speculate about the reasons for fewer complaints. The volume of incoming complaints in 2004 was itself an increase over previous years, largely due to the full implementation of the Act and its coverage of new activities such as insurance, retail and accommodation, and professions such as law. The 400 complaints we received in 2005, while only 55 per cent of the number we received in 2004, were still considerably more than we received in 2001, 2002 or 2003.
We hope that the decrease in complaints indicates greater awareness by organizations of the need to comply with *PIPEDA*. That awareness would be expected to produce at least two benefits. First, organizations would bring their personal information management practices into compliance with *PIPEDA*. Second, if compliance problems arose, the organizations' privacy officers would be more conversant with *PIPEDA* and better able to resolve problems directly with individuals.

Greater awareness and understanding of *PIPEDA* may simply come with time. The reduction in complaints in 2005 was generally greater in sectors covered since the first phase of *PIPEDA* came into force in 2001. *PIPEDA* has applied since 2001 to financial institutions, telecommunications and interprovincial or international transportation. Financial institutions – which handle by far the greatest quantity of personal information – were once again the most frequent object of complaints, but the number of complaints was just over half (53 per cent) what it was in 2004. The decline was of a similar scale in the transportation (58 per cent of the total for 2004) and telecommunications (44 per cent) sectors. In the health sector, which has been covered since 2002, the decline was precipitous; we received only 11 per cent of the number of complaints we received in 2004 (although these statistics may be unreliable as indicators of trends because of the small number of complaints).

Complaints in the more recently covered sectors declined as well, except for the accommodation sector, where the number remained roughly the same as in the previous year. In the retail sector, complaint numbers were 54 per cent of the 2004 total; this may indicate a very quick uptake of *PIPEDA* principles by the retail sector. In other cases, the decline was less dramatic. The number of complaints involving insurance companies was 73 per cent of what it was in 2004, and complaints about professionals declined to 87 per cent of their previous level (although here again, the apparent trends may not be statistically significant, given the small numbers).

Definitions of complaint types under *PIPEDA*

Complaints received in the Office 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.

Complaints received between January 1 and December 31, 2005

Complaint type	Count	Percentage
Use and Disclosure	143	35.75
Access	80	20.00
Collection	68	17.00
Safeguards	34	8.50
Consent	21	5.25
Time Limits	18	4.50
Accountability	10	2.50
Openness	8	2.00
Accuracy	5	1.25
Correction/Notation	5	1.25
Fee	3	0.75
Retention	3	0.75
Challenging Compliance	1	0.25
Other	1	0.25
Total	**400**	**100.00**

This year, the most common matter raised in complaints was the inappropriate use or disclosure of personal information. These complaints, along with those about refusal of access to personal information and inappropriate collection of personal information, comprised nearly 73 per cent of the complaints received. Last year, the picture was similar, with these categories of complaints constituting 79 per cent of the total.

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 our Office.
- **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. This finding category does not appear in the statistical tables, as it was introduced towards the end of 2005. It will appear in our statistics next year.
- **Settled during the course of the investigation.** The Office helped negotiate a solution that satisfies all involved parties during the course of the investigation. No finding is issued.
- **Discontinued. T**he 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 Office 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 this Office.

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

Findings by Complaint Type

What do complaints tell us about business organizations' compliance with *PIPEDA*? We should be cautious about reading too much into the number of complaints received, since an investigation may reveal that a complaint is not well-founded. It may be more appropriate instead to look at the findings in complaints. The chart below shows the outcome of our investigations of the different types of complaints in 2005.

Complaints closed between January 1 and December 31, 2005

	Discontinued	Early Resolution	No Jurisdiction	Not Well-founded	Resolved	Settled	Well-founded	TOTAL
Use and Disclosure	21	6	7	31	9	52	23	**149**
Access	11	1	0	10	20	32	7	**81**
Collection	7	3	5	17	4	25	3	**66**
Safeguards	4	3	2	3	3	12	3	**30**
Consent	4	0	1	6	1	9	1	**22**
Accuracy	0	1	0	2	1	13	0	**17**
Time Limits	0	1	0	1	2	4	3	**11**
Correction/ Notation	0	0	0	5	2	3	0	**10**
Accountability	1	0	0	0	3	0	0	**4**
Retention	1	0	0	0	1	2	0	**4**
Fee	0	0	0	1	1	1	0	**3**
Openness	0	0	0	1	0	2	0	**3**
Challenging Compliance	0	0	0	0	0	0	1	**1**
TOTAL	**49**	**15**	**15**	**77**	**47**	**157**	**41**	**401**

It is notable that, of 401 complaints, only 77 (19 per cent) were "not well founded." In other words, the Commissioner could conclude that organizations had complied with *PIPEDA*'s requirements in less than one in five cases. The converse of this – the number of cases where the Commissioner could say that organizations had *not* complied with *PIPEDA*'s requirements – is more difficult to state conclusively. The number of well-founded cases is relatively small – 41, or 10 per cent – but many privacy issues are addressed by means other than full investigation, and therefore appear as "settled," "resolved" or "early resolution."

The significance of these numbers becomes clearer when we look at the types of complaints involved. The majority of complaints were of three types: use and disclosure (149, or 37 per cent), access (81, or 20 per cent), and collection (66, or 16 per cent). Of these, access complaints – where an individual has been denied access to his or her personal information by an organization – are the most easily remedied. A refusal by an organization to allow an individual access to personal information can be corrected by the organization granting access or by demonstrating that legitimate exceptions to the right of access apply. The ease with which access complaints can be remedied is reflected in the relatively high proportion (64 per cent) that were either settled in the course of investigation or that we considered resolved by the organization. Still, the large number of access complaints may be worrisome; it may suggest that some organizations still do not fully comprehend their responsibilities under the access provisions of *PIPEDA*. However, the number of successful resolutions is encouraging.

Complaints about inappropriate use, disclosure or collection are more troubling. These are complaints for which no simple remedy exists. If someone's personal information is inappropriately disclosed, it cannot be recalled. If someone's personal information has been inappropriately collected, the collection cannot be reversed. The Commissioner found that organizations complied with *PIPEDA*'s requirements (the complaints were "not well-founded") in only 26 per cent of the collection complaints and 21 per cent of the use and disclosure complaints.

For this reason, we intensified our focus in 2005 on maximizing the possible remedies under *PIPEDA*. We introduced a new procedure to allow the Commissioner to exert greater pressure on organizations to change their practices so that, if the damage to an individual cannot be undone, at the very least it will be less likely to happen to someone else in future. If an investigation indicates a likely contravention of *PIPEDA*, the Commissioner intervenes early, before making a finding about the complaint, with a recommendation to the organization as to how to remedy the matter. She then asks the organization to indicate within a set time how it will implement the recommendation. After receiving the organization's response, the Commissioner issues her finding.

The results of this approach have been encouraging, and it has led us to develop a new category of complaint finding, "well-founded and resolved." (This new finding category does not appear in the statistical tables, as it was introduced towards the end of 2005.) This is more than simply an exercise in rewording. It shows that organizations, almost without exception, have accepted the Commissioner's

recommendations and implemented them in a timely manner. For a person whose privacy has been irreversibly violated, this approach offers something beyond the satisfaction of knowing that the investigation supported their allegations; their complaint has led to a change; it has made a difference.

The table dealing with "complaints closed" also shows that our emphasis on settling complaints in the course of investigations continues. We commented last year that an increased focus on settlement of complaints was one way to address our complaints workload. This year, as in 2004, settlement during the course of the investigation was by far the most frequent disposition of our cases. Of the 401 complaints closed in 2005, 157 (39 per cent) were settled during the investigation. This included 38 per cent of the collection complaints and 35 per cent of the use and disclosure complaints. We will continue to seek settlements of complaints because settlement is a fundamental aspect of an ombudsman's role, helping organizations change their cultures and sort out their problems with clients and employees.

During the year, we closed 401 complaints. This is an improvement over the previous two years, and it broke the trend of the last three years where we had received more complaints than we closed. In 2005, we closed as many complaints as we received. (A complaint received in one calendar year is not necessarily completed in that year, which is why we can close more complaints in a year than we receive.)

This has helped to reduce our complaints backlog but, like any organization that has a public complaints function, we constantly struggle to balance our resources and keep up with the influx of complaints. Some new resources will be made available in 2006 to deal with complaints, but our focus remains on finding ways to streamline procedures and process cases more effectively and efficiently.

Complaint Investigations Treatment Times

The following tables show the average number of months taken to complete a complaint investigation, from the date the complaint is received to when a finding is made or another type of disposition occurs. The first table breaks this down by finding or disposition, the second by complaint type.

Complaint Investigations Treatment Times for the period between January 1 and December 31, 2005, by Finding or Disposition

Finding or Disposition	Average Treatment Time in Months
Not well-founded	13.79
Resolved	13.21
Well-founded	12.44
No jurisdiction	12.27
Settled	10.17
Discontinued	7.67
Early resolution	2.53
Overall average	**10.94**

Complaint Investigations Treatment Times for the period between January 1 and December 31, 2005, by Complaint Type

Complaint Type	Average Treatment Time in Months
Challenging compliance	16.0**
Collection	11.8
Accuracy	11.5
Use and disclosure	11.4
Openness	11.3*
Fee	11.0*
Access	10.9
Retention	10.8*
Consent	10.1
Accountability	10.0*
Correction/Notation	9.9
Safeguards	8.8
Time limits	6.6
Overall average	**10.9**

* The treatment time for these complaint types reflects four or fewer cases each.
** The treatment time for this complaint reflects one case only.

These tables of through-put times are troubling. Section 13 of *PIPEDA* requires the Commissioner to prepare her report on a complaint within one year after the filing of the complaint. As the tables show, the average time elapsed from the date of complaint to the date of finding or other disposition is just under 11 months. We might take some comfort from that, but it is uncomfortably close to the outside limit, and closer examination of the tables shows that the average time elapsed for some categories has exceeded the limit. In fact, the breakdown by finding/disposition shows that complaints that require full investigation – that is, the complaints that are "well-founded," "not well-founded" or "resolved" – take on average more than a year to complete. (The delay in completing complaints where the finding is "no jurisdiction" reflects the complex factual and legal issues that must be addressed. Where jurisdiction is clearly not ours, the complaint does not get past our inquiries officers. If a complaint involving a jurisdictional issue has made it to the investigation phase, it is because the jurisdictional issue is not straightforward.) The length of time it is taking us to complete investigations can be attributed to a number of factors, including changes in procedures and resource issues. Whatever the reasons, it remains a matter of great concern to us, and we are focusing on ensuring that we process complaints within the period envisaged under the Act.

Inquiries

The OPC's Inquiries Unit responds to requests for information about the application of *PIPEDA* and the *Privacy Act*. The Office receives thousands of inquiries each year from the public and organizations seeking advice on private sector privacy issues.

In 2005, the Office received 5,685 inquiries related to *PIPEDA*. This was less than half the number for 2004, when we received 12,132. The total for 2004 was in turn lower than for 2003. As we noted last year, the decline may be attributable to greater understanding of *PIPEDA* among the organizations subject to it. In 2003 and 2004, on the other hand, many organizations were searching for guidance about *PIPEDA* as the Act approached full implementation on January 1, 2004.

The inquiries staff are now responding to fewer calls, but they are providing more information. An automated telephone system also helps to answer the public's most frequently asked questions, such as those about identity theft, telemarketing and the Social Insurance Number. In addition, our web site provides a wide range of information and is increasingly used as a key resource.

Inquiries Statistics
January 1 to December 31, 2005

PIPEDA Inquiries Received by the Inquiries Unit	
Telephone inquiries	4,597
Written inquiries (letter and fax)	1,088
Total number of inquiries received	5,685

PIPEDA Inquiries Closed by the Inquiries Unit	
Telephone inquiries	4,623
Written inquiries (letter and fax)	1,587
Total number of inquiries closed	6,210

Following Up on *PIPEDA* Case Investigations

Since 2004, the Investigations and Inquiries Branch has as a matter of course monitored the progress of organizations in implementing both the commitments they make during complaint investigations and the recommendations that the Office makes to them in letters of findings. Follow-up reinforces the Office's expectations that organizations will take measures to remedy problems identified in complaint investigations. It also provides an ongoing record of organizations' compliance with *PIPEDA*.

The following are a few examples of actions taken by organizations as a result of our recommendations:

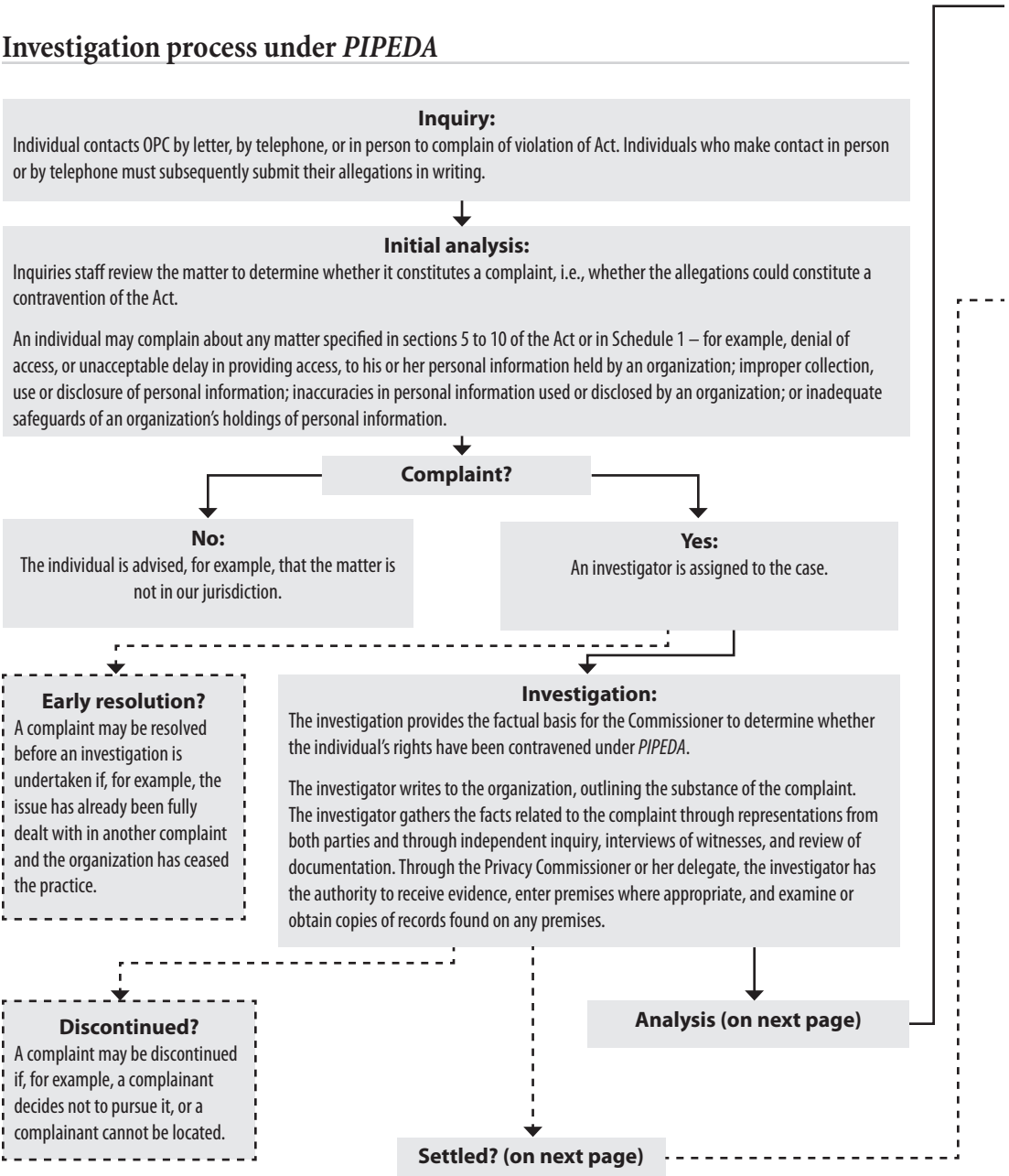
- An individual complained that his former employer was able to access his account with a rewards program and make changes to it. In her letter of finding, the Assistant Commissioner recommended to the organization now responsible for the rewards program that it implement password controls on the account holder information that can be accessed through its automated system. Our follow-up confirmed that the organization had introduced voice print technology and password protection for access to account holder information.

- An individual was disputing an auto insurance claim against her and sought various documents, including the claimant's statement. The insurance company refused to release the statement without the claimant's consent. The Assistant Commissioner recommended that the company sever the personal information of the third party claimant and provide the complainant with access to her personal information. She also recommended that the adjusters who work on the insurer's behalf notify third party claimants that their statements to the insurer will be shared with the insured person upon request, and that, for the purposes of providing access, only the personal information of the third party claimant that is not directly related to the statement to the insurer be severed from the statement. Our follow-up confirmed that the company did give the complainant a copy of the statement, with the relevant personal information of the claimant severed, and that the company had implemented our recommendations about its practices.
- An individual complained when his bank refused to allow him to opt-out of receiving marketing materials that were included in his credit card account statements. These materials, or "statement stuffers," were advertisements for various products and services, such as magazines or travel insurance, and were being offered by the bank in conjunction with other organizations. In response to the Assistant Commissioner's recommendations, the bank has implemented a procedure for customers to opt-out of receiving secondary marketing inserts.
- A former employee of an aviation company complained that his employer inappropriately destroyed his employment file. The Assistant Commissioner concluded that the complainant's file had been destroyed in accordance with the *Canadian Aviation Regulations*, and that the complaint was not well-founded. Nonetheless, she recommended that the company specify its maximum retention period for these files, and keep a record of when and by whom files are destroyed. Our follow-up confirmed that the aviation company amended its internal directives to specify the minimum and maximum period for retention of a pilot's file, and also instituted a log to indicate when and by whom files are destroyed.
- An individual complained that her Internet service provider failed to protect her personal information adequately, did not provide her with a satisfactory explanation when she tried to resolve her concerns, and did not give her access to the personal information she had requested. The investigation did not support the allegations about failure to protect her personal

information, and the access complaint was resolved during investigation. On the accountability issue, the Assistant Commissioner recommended that the company implement a procedure for outstanding privacy concerns to be brought to the attention of the company's privacy officer. The organization already had such a procedure, but acknowledged that its staff required greater awareness of and sensitivity to privacy. It undertook to provide the necessary training.

- An individual complained about a bank using his personal information for marketing purposes. The Assistant Commissioner concluded that the complaint was not well-founded, because the complainant had not requested that his name be suppressed from marketing lists. In reviewing the bank's privacy policy, however, she noted that it required customers to obtain and complete a form to have their names suppressed from the bank's marketing lists. She commented that this did not meet the reasonable expectations of most individuals – namely, that an immediate, easy and inexpensive means of withdrawing consent to the optional collection, use and disclosure of their personal information be provided. She therefore recommended that the bank review its opt-out procedures. In response, the bank amended its policy and procedures on direct marketing preferences. Clients wanting to opt-out of the use of their personal information for secondary marketing purposes can now simply contact any branch of the bank or the bank's call centre.

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.

Audit and Review

The goal of the Audit and Review Branch is to conduct independent and objective audits and reviews of personal information management systems for the purpose of promoting compliance with applicable legislation, policies and standards and improving privacy practices and accountability.

Section 18(1) of *PIPEDA* allows the Commissioner, after giving reasonable notice and at any reasonable time, to audit the personal information management practices of an organization if the Commissioner has reasonable grounds to believe that the organization is contravening a provision of *PIPEDA*.

Given the magnitude of privacy issues and risks now facing Canadians, audit must become more central to the activities of the Office, and more proactive. We are carefully developing criteria for determining the reasonable grounds for conducting an audit. We plan to make these criteria publicly available in July 2006.

As well, as part of the upcoming review of *PIPEDA*, we are considering seeking amendments that would give the Privacy Commissioner the discretion to visit private sector entities and review their privacy management framework and practices to ensure that significant privacy risks are being identified and managed, even when a privacy breach has not become public. We believe that this discretion should also be used in particular when a significant privacy breach comes to light and the Commissioner decides that independent assurance is required that the organization concerned has taken appropriate corrective action. Such action would include critical diagnosis of internal systems and practices to remedy root causes and avoid future problems.

At the same time, we wish to support measures to encourage and help organizations to "self-regulate" and take responsibility for their own privacy governance and management. This is why, for example, we are developing a privacy self-assessment tool.

Radio Frequency Identification Device (RFID) Use in Canada

This year, the Audit and Review Branch conducted a study of a technology that is causing considerable concern from a privacy perspective – radio frequency identification devices, or RFIDs.

RFIDs form a subset of a group of technologies, often referred to as automatic identification, that are used to help machines identify objects. An RFID "tag" can be placed in just about anything that is sold to, or used by, people. This includes bank cards, credit cards, money, passports, luggage, badges and wrist bands, clothing, vehicles and vehicle parts, appliances, phones, drugs, and food packaging. RFIDs can be implanted in livestock, and at least one company is advertising them for implanting in humans. Perhaps of greatest significance, RFIDs are capable of uniquely identifying a product.

The small size of the tags and their ability to uniquely identify an object may pose various threats to individual privacy, including the following:

- *Surreptitious collection of information*. RFID "tags" are small and can be embedded into/onto objects and documents without the knowledge of the individual who obtains those items. Tags can be read from a distance, by readers that can be incorporated invisibly into nearly any environment. Without clear notification, it may not be readily apparent that RFID technology is in use, making it virtually impossible for a person to know when or if he or she is being "scanned."
- *Tracking an individual's movements*. If RFID tags are embedded in clothing or vehicles, for example, and if there is a sufficiently dense network of readers in place, it becomes possible to track those tags in time and space. Applications to do just this, using a combination of RFID and Global Positioning System (GPS) technology, are being proposed by RFID vendors. If the tags can then be associated with an individual, then by that association the individual's movements can be tracked. For example, a tag embedded in an article of clothing could serve as a *de facto* identifier for the person

wearing it. Even if information about the tagged item remains generic, identifying items people wear or carry could associate them with particular events – for example, political rallies or protests.

- *Profiling of individuals*. When using bar codes, one bottle of water has the same barcode as all other bottles of water of that particular brand. RFID technology potentially enables every object on earth to have its own unique ID (i.e., each bottle of water would have a unique identifier). There is, perhaps, the risk that the use of unique ID numbers could lead to the creation of a global item registration system in which physical objects are identified and linked to its purchaser or owner at the point of sale or transfer. If these unique identifiers are associated with an individual (by linking through a credit card number, for example), a profile of that individual's purchasing habits can easily be created.
- *Secondary use* (particularly in the sense of limiting or controlling such use). For example, the revelation of personal information such as medical prescription or personal health histories could have an impact on insurance or employment.

RFIDs in Canada

Early in 2005 we wrote to 14 corporations in Canada asking them to help us understand the emerging use of RFIDs in Canada.

Twelve responded to the survey we sent them. The survey was not intended as a statistically representative sample of Canadian businesses as a whole. Instead, the focus was on larger corporations whose business activities were most likely to use RFID technology. The organizations included those in manufacturing, retailing, transportation, and distribution, as well as those directly involved in manufacturing RFIDs. A standard survey letter was sent to each organization asking for information about current or planned RFID use.

Of the 12 organizations that responded, two were involved in the production of RFIDs. Of the remaining ten, two were considering RFIDs, four had or would be testing RFID use, and four were using RFIDs already.

Of the four already using them, three used them to track goods, and two indicated that they linked this with personal information. One organization was using RFIDs to track employees, but stated that it was not collecting personal information.

Six of the ten organizations responded in some way to the privacy issues mentioned in the survey letter. Of the six, one indicated that it would conduct a privacy impact assessment (PIA) in reviewing the possible use of RFIDs, one would not, two others might consider a PIA or privacy compliance test in their consideration of RFIDs, and two reported that they believed a PIA was not required, since their RFID application did not identify individuals and/or link with personal information.

We learned that one central player in the RFID industry sets standards to enable and support RFID use. It also requires subscribers to respect certain privacy principles. For example, consumers must be notified of the presence of an RFID tag in an item and be given the choice to end the tag's function ("kill" the tag) after purchasing the item. As well, the tags are not to contain personal information. We are encouraged by this attention to privacy, and we call for similarly responsible practices by all those in Canada who may use RFIDs.

The only key government application for RFID of which we are now aware is its planned use in Canadian passports. We are monitoring this. As well, a group in Industry Canada is supporting and facilitating the development of commercial RFID technology.

Need for RFID Awareness and Guidance

Even at this early stage, RFID has expanded beyond simply tracking materials. RFIDs are already being linked to personal information, and are sometimes used to track people.

Comprehensive privacy risk management for RFIDs does not yet seem to be firmly in place. Perhaps this is because RFIDs use is only beginning, with companies merely considering their business case for RFIDs, while RFID manufacturers are still focused on technical matters such as common standards to ensure security, compatibility and interoperability.

Greater public and political awareness of the potentially intrusive nature of RFID technology is essential now. The OPC will develop guidelines to help ensure that, even as RFIDs become more common, they do not erode informational privacy rights.

Follow-up Audit of the Canadian Imperial Bank of Commerce

Between 2001 and 2004, the Canadian Imperial Bank of Commerce (CIBC) misdirected a number of facsimiles containing customers' personal information. Our Office investigated and identified concerns about privacy protection safeguards within the CIBC. In March 2005, we reported the results of this investigation to the CIBC. In light of other investigations into similar cases, we also publicly urged all banking organizations subject to *PIPEDA* to assess their policies and privacy management practices and address any shortcomings.

CIBC then reported on a number of measures to identify problems and to enhance its personal information safeguards. It also conducted an internal audit.

In a March 2005 letter to CIBC, we explained that representatives of our Audit and Review Branch would visit CIBC to verify the corrective actions that CIBC has taken and to discuss any other risks to personal information. In December 2005, we wrote CIBC that we would start this process in March 2006. We invited CIBC to send information in advance of our site visit to explain corrective actions taken by CIBC. We said that we would consider the results of the work done by the bank's internal audit department in August 2005, as well as actions taken by bank management in response.

A few weeks later, CIBC suggested meeting before our audit to confirm its scope and to understand the audit process. As requested, it agreed to give the Office a chance to examine the materials assembled in preparation for the review. We appreciate this level of cooperation. Results of our follow-up audit will appear in next year's annual report.

Privacy Self-assessment

In our last annual report we noted that we were developing a privacy self-assessment tool for organizations to adapt and use as they wish. A draft is now being finalized with the help of internal and external expertise. The self-assessment tool is intended to promote good privacy practices and help ensure compliance with *PIPEDA*. It may also be of general interest to any entity wishing to advance privacy principles. We hope to publish the self-assessment tool in July 2006.

In the Courts

PIPEDA Applications

Under sections 14 and 15 of *PIPEDA*, a complainant or the Commissioner herself may in certain circumstances apply to the Federal Court of Canada for a hearing in respect of any matter which is referred to in the Commissioner's report and which falls within those specific clauses and sections of *PIPEDA* listed in section 14.

Since we reported on the status of ongoing court cases in our 2004 *PIPEDA* Annual Report, further developments have occurred and new applications have been filed. A selection follows of *PIPEDA* developments and new applications from 2005.

In keeping with our mandate, we have chosen not to reproduce the official style of cause in order to respect the privacy of the individual complainants. We are listing the court docket number and the name of the organization only.

Developments in Ongoing Applications

Telus Communications Inc.
Federal Court Files T-1862-04, T-1863-04, T-1864-04 and T-1865-04
Federal Court of Appeal File No. A-639-05

(See 2004 *PIPEDA* Annual Report at pages 85-86.)

A hearing was held in Vancouver in September 2005. On November 29, 2005, Mr. Justice Gibson released his decision. He found that: (1) the Telecommunications Workers Union was not a proper party to the proceedings (i.e. it was not "an individual" entitled to apply to the Court); (2) the collection of the voice print

information at issue would be seen by a reasonable person to be appropriate in the circumstances pursuant to section 5(3) of the Act; and (3) Telus met its consent obligations under the Act.

The applicants filed an appeal on December 22, 2005.

Alta Flights (Charters) Inc.
Federal Court File No. T-1066-04
Federal Court of Appeal File No. A-184-05

(See our 2004 *PIPEDA* Annual Report at pages 84-85.)

The application was heard on March 15, 2005, and the decision released on March 29. The Court concluded, as had the Assistant Privacy Commissioner, that since there was no evidence that Alta Flights had recorded any conversations, the company did not actually manage to collect and/or use any personal information. In the absence of any explicit or implicit statutory language, common law principles of attempted breach cannot be read into *PIPEDA*. The Court therefore found that an attempted collection does not violate the Act.

The applicant filed an appeal of the decision in April 2005. A requisition for hearing of the appeal was filed on August 4, 2005 and the hearing date was set for March 21, 2006.

New Applications of Interest

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

The complainant was the long-time general manager of the Brampton Flying Club (BFC) until dismissed from his position. He took legal action regarding his dismissal and also made an access request for a copy of all his personal information held by the club.

In December 2003, he complained to the Privacy Commissioner that BFC had (1) failed to provide him with his personal information within 30 days of his written request; (2) subsequently tried to charge him an unreasonable amount of $1,500 to conduct a five-day forensic audit which BFC claimed would be necessary to answer his request; and (3) still had not supplied him with all his information.

The Assistant Commissioner determined that the statutory time limit in section 8(3) had been exceeded, that the $1,500 charge was beyond the scope of "minimal or no cost" set out in Principle 4.9.4, and that some of the complainant's personal information was improperly withheld by the organization.

The individual filed an application to the Federal Court under section 14 of *PIPEDA* on February 3, 2005. The Privacy Commissioner was added as a party to this application on May 18, 2005.

The Privacy Commissioner took the position that fact that the complainant may have been seeking access to documents that might assist him in parallel court proceedings between the parties was irrelevant. A complainant's motive should not be used to limit his or her right of access to personal information under *PIPEDA*. In these unique circumstances, the Privacy Commissioner filed a confidential affidavit with the Court to identify the documents to which the complainant was seeking access and which had been withheld by the organization.

The matter was adjourned for 60 days on January 3, 2006, to allow for settlement discussions.

Jeffrey P. Wyndowe
Federal Court File No. T-711-05

The complainant alleged that Dr. Wyndowe, an independent medical examiner who examined the complainant on behalf of his insurance company, refused to provide him with access to his personal information. The complainant asked for a copy of the questions the doctor asked him, as well as a record of his answers. Dr. Wyndowe refused, indicating that in his view they did not form part of the complainant's medical record and were therefore not his personal information.

The Assistant Commissioner found that the notes taken by Dr. Wyndowe in support of his report were the complainant's personal information as defined in section 2 of *PIPEDA*. Dr. Wyndowe then argued that the independent medical examination took place in the context of a litigious situation, and that access could therefore be denied because the information was protected by solicitor-client privilege. The Assistant Commissioner did not accept this interpretation of section 9(3)(a) of *PIPEDA*, since Dr. Wyndowe had not been retained by the insurance company as an expert in the context of ongoing litigation; rather, he was retained as an expert to help the company determine its obligations under a group insurance policy.

Nor was the Assistant Commissioner convinced that section 9(3)(d) – which permits an organization to deny access to information generated in the course of a formal dispute resolution process – could be used in this case, since processing the insurance claim did not constitute a formal dispute resolution process.

The Assistant Commissioner recommended that Dr. Wyndowe provide the complainant with access to his personal information.

The complainant filed an application to the Federal Court under section 14 of *PIPEDA* on April 25, 2005. The Privacy Commissioner was added as a party on July 7, 2005. A requisition for hearing was filed on October 3, 2005, although no date has yet been set.

Scotiabank
Federal Court File No. T-2126-05

An individual complained that one or more employees of Scotiabank obtained her personal information without her consent, and that this information was then communicated to a third party.

During the investigation, it was confirmed that one of the bank's employees had improperly accessed the applicant's account profile without her consent, and had provided this information to the director of the branch, but not to any outside party. The bank had already taken disciplinary measures against this employee following its own internal investigation.

The Assistant Commissioner concluded that the bank employee had indeed violated the provisions of *PIPEDA* and that the complaint was well-founded.

The complainant filed an application to the Federal Court under section 14 of *PIPEDA* on December 1, 2005. The matter is proceeding before Federal Court.

Privacy Commissioner of Canada v. RBC Action Direct Inc.
Federal Court File No. 05-T-17

An individual complained that RBC Action Direct refused to release to him all his personal information in response to an access request made under *PIPEDA*. The information included a transcript of the complainant giving instructions by telephone to an RBC Action Direct representative regarding an account which he

claimed to be a joint account between him and a third party. The organization contended that the information was the personal information only of the third party account holder, not that of the complainant, and withheld the transcript.

The Assistant Privacy Commissioner concluded that information may be personal to more than one party. In this case, there was personal information of the third-party account holder but the transcript capturing the complainant's telephone conversation with the organization's representative also constituted the personal information of the complainant. Accordingly, the complaint was well-founded and the Assistant Commissioner recommended that the organization release the transcript to the complainant. Though RBC Action Direct provided the complainant with a copy of the transcript, it severed virtually all the information in it, maintaining – despite the Commissioner's finding – that it was the account holder's personal information only.

As more than 45 days had lapsed since the issuance of the Commissioner's report, the Commissioner requested an extension of time to file a section 15(a) application in Federal Court against RBC Action Direct Inc. Leave to file the application was granted on December 16, 2005.

Applications No Longer Proceeding

Canadian National Railways
Federal Court File No. T-948-04

An individual complained that a nurse affiliated with CN shared his personal information when she revealed to his supervisor sufficient information for the supervisor to deduce that the complainant was in the company's substance abuse program, and that she disclosed further personal information about him in an email to the supervisor, superintendent and two other CN supervisors.

The Assistant Privacy Commissioner concluded that the nurse had indeed revealed too much personal information in both instances, and that the information was not necessary in the circumstances. CN therefore inappropriately used his personal information and violated Principle 4.3.

The complainant filed an application in the Federal Court under section 14 of *PIPEDA* on May 14, 2004. The Privacy Commissioner was added as a party in

October 2004 in order to make arguments concerning: (1) the scope of the Privacy Commissioner's jurisdiction and that of the Federal Court over *PIPEDA* complaints that arise in the context of a collective agreement; and (2) the proper interpretation of section 5(3) and Principle 4.3 of *PIPEDA*.

The Application was discontinued on June 8, 2005.

3web Corporation
Federal Court File No. T-1603-04

(See our 2004 *PIPEDA* Annual Report at pages 88-89.)

The company discontinued the proceeding in June 2005.

Calm Air International Ltd.
Federal Court File No. T-2061-04

(See our 2004 *PIPEDA* Annual Report at page 87.)

The Privacy Commissioner was added as a party on October 24, 2005. On November 18, 2005, the parties reached a settlement at mediation. The application was dismissed on January 20, 2006.

Citibank Canada
Federal Court File No. T-2135-04

(See our 2004 *PIPEDA* Annual Report at page 86.)

An application under section 14 of *PIPEDA* was filed in the Federal Court on December 1, 2004. A settlement was reached at mediation. The application was dismissed on June 15, 2005.

King Cole Ducks Limited
Federal Court File No. T-445-05

A Canadian Food Inspection Agency employee, working at a federally registered meat processing plant, complained that the organization was collecting personal information without consent through video cameras aimed at his workstation. The company stated that the cameras could help it address food safety concerns.

However, there was no evidence that the cameras could capture sufficiently detailed images to do this effectively. The Assistant Privacy Commissioner concluded that the organization was indeed collecting the complainant's personal information without his consent, contrary to Principle 4.3, for purposes which, upon closer examination, would not likely be considered appropriate in the circumstances pursuant to section 5(3) of *PIPEDA*.

The complainant filed an application to the Federal Court under section 14 of *PIPEDA* on March 9, 2005, requesting, among other things, an order that the organization remove the surveillance camera aimed at his workstation. This application was discontinued on November 4, 2005.

Judicial Review

There were two applications, in accordance with section 18.1 of the *Federal Court Act*, for judicial review of the Privacy Commissioner's decisions and/or actions on the limited grounds of jurisdictional-type errors.

Blood Tribe Department of Health v. Privacy Commissioner of Canada et al.
Federal Court File No. T-2222-03
Federal Court of Appeal File No. A-147-05

(See our 2004 *PIPEDA* Annual Report at pages 87-88.)

The Federal Court dismissed this judicial review application on its merits in March 2005. At that time, Mr. Justice Mosley stated that when the Privacy Commissioner is seized with a complaint over the retention and use of personal information, she has the responsibility to determine the facts and the duty to prepare a report of her findings. She cannot perform that role effectively if she is denied access to the information necessary to ascertain the facts merely because a claim of privilege is made. The Court was satisfied that the Commissioner had correctly exercised her authority to order the respondent to give her the documents in question, so that the Commissioner might herself assess the claim of solicitor-client privilege. Given the Commissioner's statutory obligation of confidentiality, such an order does not otherwise limit or deny any solicitor-client privilege that the applicant might enjoy in the documents at issue.

The applicant filed an appeal of this decision in April 2005. A requisition for hearing was filed in September 2005, but no date for a hearing has yet been set.

Accusearch Inc., COB Abika.com
Federal Court File No. T-2228-05

A complaint was filed against a data search and profiling organization in the United States. The Privacy Commissioner determined that, to investigate the U.S. organization, she must have the requisite legislative authority to exercise her powers outside Canada. The Commissioner concluded that *PIPEDA* cannot be construed as having extraterritorial effect. Based on available information, there were insufficient real and substantial connecting factors between the organization and Canada to deem the organization within the current scope of *PIPEDA*. In the circumstances, the applicant was informed that the Privacy Commissioner could not proceed with the complaint, as she lacked jurisdiction to compel the organization to produce evidence necessary for her to carry out an investigation and issue findings.

The applicant filed an application under section 18.1 of the *Federal Court Act* on December 19, 2005, seeking an order quashing or setting aside the Privacy Commissioner's decision that she lacks jurisdiction to investigate the complaint.

Public Education and Communications

Section 24 of *PIPEDA* gives the Privacy Commissioner a specific mandate for public education and communications, as well as for research into privacy issues.

The Act requires the Commissioner to:

(a) 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;
(b) undertake and publish research that is related to the protection of personal information, including any such research that is requested by the Minister of Industry;
(c) encourage organizations to develop detailed policies and practices, including organizational codes of practice, to comply with sections 5 to 10; and
(d) promote, by any means that the Commissioner considers appropriate, the purposes of Part 1.

In 2005, the OPC took several steps to gain a better understanding of Canadians' views on privacy issues, to raise awareness and understanding of privacy in general and, specifically, to help organizations understand their responsibilities, and individuals their rights, under *PIPEDA*. This has involved, for example, undertaking public opinion research, media relations activities, speeches and participation in special events and conferences, the printing and dissemination of publications, and posting information on our web site.

Public Opinion Research

This year, the OPC commissioned EKOS Research Associates to conduct a public opinion study about Canadians' views on a variety of important privacy issues.

Canadians support strong and responsive public and private sector privacy laws. Approximately 70 per cent of those surveyed expressed a strong sense that their privacy and protection of their personal information were being eroded. They identified privacy as among the most important issues facing the country. That said, however, a gap remained between the perceived importance of privacy and privacy laws, and public awareness about these matters. Only one in five of those surveyed expressed "clear" awareness of privacy laws, so much education remains to be done.

There was an extremely high level of concern about cross-border sharing of personal information, and a strong demand for consent as a condition for such sharing. Approximately 90 per cent of those surveyed wished not only to be informed of such sharing, but also insisted that governments and the private sector first obtain their permission. The Government has since developed guidelines to ensure that personal information is protected when government contracts involve outsourcing – one step in the right direction.

A substantial majority of those surveyed said there was no real privacy because technology has made it too easy for governments to keep track of people. Although about three in ten were willing to allow companies to track how they shop in return for a discount on products or services, the vast majority of those surveyed wanted to be notified about the privacy implications of the products and services they buy.

Speeches and Special Events

Conferences, meetings and other special events offer a unique opportunity for the OPC to reach out to its audiences and make significant contributions to the protection of personal information in Canada and abroad.

Our Office hosts a regular in-house lecture series (roughly one a month). The series features experts on a variety of privacy issues and brings together people from government, academia and other invited guests, as well as our staff.

In addition, representatives from our Office made more than fifty presentations in 2005, several focusing on *PIPEDA*. For example, in the Northwest Territories we

provided guidance on *PIPEDA*'s application to the tourism industry, and at an event in Toronto we explained *PIPEDA* to the bookkeeping industry. At a technology industry conference in Banff, we explained the importance of privacy standards.

The Privacy Commissioner and other senior officials also participated in a select number of international meetings and conferences. It is important that we participate in these meetings to establish Canada's position on privacy issues abroad and to help represent Canada's interest in strong privacy standards internationally, so that the personal information of Canadians processed in other countries is not compromised by lower privacy standards there. This has involved our Office participating in international data protection conferences, and meetings of the Asia-Pacific Economic Cooperation (APEC) and the Organisation for Economic Co-operation and Development (OECD). Our web site features some of the recent resolutions adopted by the data protection and privacy commissioners at their 2005 international conference in Montreux, Switzerland. This annual conference is an important event for the evolution of common approaches and the debate on global challenges to privacy, and we are honoured to be hosting the meeting in Montreal in 2007.

Publications

Each year, the OPC produces and disseminates thousands of copies of publications to individuals and organizations seeking information on privacy matters. Increasingly, Canadians are viewing these documents on our web site. These documents include annual reports, guides for businesses and individuals about *PIPEDA*, as well as fact sheets and copies of both *PIPEDA* and the *Privacy Act*.

In 2005, we also published a new educational document – *Learning from a Decade of Experience: Quebec's Private Sector Privacy Act* – which aims to review and summarize Quebec's experience with its private sector law, which has been in force since 1994.

Quebec has had more than a decade of experience interpreting and applying its Act in numerous sectors and multiple situations. This has resulted in a rich body of jurisprudence that provides important insights for other jurisdictions dealing with private sector privacy compliance. We have heard that this publication has been extremely useful in helping to interpret *PIPEDA* and similar laws.

Web Site

The OPC web site has seen a steady and significant increase in visits over the last several years. As with other organizations, our web site has become a key vehicle for sharing information with broad audiences. We are pleased to report that in 2005 we had almost a million visitors to our site – a milestone for our Office. We regularly post new material. This includes speeches, fact sheets, news releases, useful links and case summaries under *PIPEDA*. These materials give a real sense of the application of the law in a variety of circumstances.

Although public education and communications are an important part of our mandate, limited financial and human resources have constrained our ability to go much beyond simply responding to issues, rather than anticipating them and preparing public education strategies in advance. However, expected increased funding will permit more extensive public awareness initiatives and enable us to carry out a comprehensive proactive communications and outreach strategy.

Corporate Services

During 2005, the main priority of the Corporate Services Branch was completing the business case for stable, long-term funding. The second priority was strengthening our human resources management capacity.

Planning and Reporting

An essential component of the institutional renewal of our Office is a strategic planning, reporting and control process. The year 2005 was our second using this new process. The strategic plan established at the beginning of the year became our road map for the year. We reviewed and made adjustments to plans and budgets throughout the year. To assist in our reporting, we continued work on our Performance Measurement Framework, and our monthly performance report system has now been in place for 18 months. This serves as a critical management tool for measuring whether our results meet our Office's targets.

Human Resources

We continue trying to improve workplace quality and Office operations. Significant changes and improvements have been made to human resources management policies and practices.

We have implemented several human resource policies in consultation with central agencies and unions and in line with the new *Public Service Employment Act* requirements. These policies will guide us as we build on the successes of the past year and continue on our path towards renewing the Office. An Instrument of Delegation of Human Resource Management was developed and will guide managers in addressing human resource issues. A new Strategic Human Resource Plan and Staffing Strategy, as well as an Employment Equity Action Plan, will

help the OPC fulfill its mandate and ensure the recruitment of a highly qualified, diverse and representative workforce. As part of OPC's commitment to increase transparency in the staffing processes, a staff newsletter was developed; it is distributed monthly to all members of staff.

We made significant strides in organizational learning, including the development of a learning strategy with the Canada School of Public Service (CSPS), training and information sessions in values-based staffing, language training sessions, performance management, employee appraisals, and harassment awareness in the workplace. We have provided briefing sessions at our quarterly all-staff meetings and to all managers on various aspects of the new *Public Service Modernization Act* and *Public Service Employment Act*. The learning strategy and curriculum with the CSPS enables staff members to continue to develop the expertise and competencies required in their work, which in turn positions staff to assume new responsibilities and accountabilities. The learning strategy has been modified to reflect training requirements related to the new *Public Service Employment Act*.

We continue to work with the Public Service Commission and the Public Service Human Resources Management Agency of Canada on responses to recommendations in their audit reports. These include measures to allow OPC to regain its full staffing delegation authority.

Finance and Administration

The OPC received a clean opinion on Audited 2004-2005 Financial Statements by the Office of the Auditor General of Canada. Along with the clean opinion for 2003-2004, this is a very firm indication that the Office has advanced along the path of institutional renewal. The organization has built on this success by establishing planning and review cycles, and by streamlining and improving the financial management policies and practices.

Information Management/Information (IM/IT) Technology

The IM/IT Division has accomplished much over the past year. We have renewed our server infrastructure and increased data storage to allow for the scanning of documents. Substantial progress has been made on our information management project. Upgrades to our records management and correspondence tracking systems have been completed. Financial systems – the Salary Management System (SMS) and FreeBalance – have been upgraded, and the FreeBalance server has been upgraded as well. Five new tracking systems have been developed for the Audit and Review

Branch to allow the tracking of audit files. We have completed the Action Plan for Management of Information Technology Standards Compliance and we are working steadily towards the December 2006 compliance deadline.

Our Resource Needs

As described earlier in this report, the Office has completed a business process review of all OPC functions. Following that review we requested a greater than 50 per cent increase in resources. We are planning for an overall budget of approximately $18 million and 140 full-time equivalents (FTEs), and for a shift in the distribution of new resources to enable the Office to become more proactive.

Financial Information

Past annual reports of this Office have provided financial tables relating to our expenditures. The overall financial framework in which the OPC operates is based on the government fiscal year, not on the calendar year. We are required to report on *PIPEDA* for the calendar year, whereas for the *Privacy Act*, we report on the fiscal year. For this reason, and to avoid any confusion, we have not included our Office's financial tables in this report. In any case, we set out these tables in our Reports on Plans and Priorities, as well as our Departmental Performance Reports. For additional financial information, we encourage you to visit our web site at **www.privcom.gc.ca**.