Privacy Commissioner of Canada

Commissaire à la protection de la vie privée du Canada

Privacy

Annual Report to Parliament 2004

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
ISBN 0-662-68986-0

This publication is also available on our Web site at www.privcom.gc.ca, in addition to our 2004-2005 Annual Report on the *Privacy Act*.

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

October 2005

The Honourable Daniel Hays, 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, 2004.

Yours sincerely,

Jennifer Stoddart

Jennifer Stoddart
Privacy Commissioner of Canada

Privacy Commissioner of Canada

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

Commissaire à la protection de la vie privée du Canada

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

October 2005

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, 2004.

Yours sincerely,

Jennifer Stoddart

Jennifer Stoddart
Privacy Commissioner of Canada

Table of Contents

Foreword

The year 2004 saw the *Personal Information Protection and Electronic Documents Act* (*PIPEDA)* reach maturity, with the Act extending across the country to all commercial activities, except in provinces with legislation deemed substantially similar. British Columbia, Alberta and Quebec have enacted private sector privacy legislation that has been deemed substantially similar to *PIPEDA*. *PIPEDA* applies to federal works, undertakings and businesses across the country, as well as to interprovincial and international transactions.

The maturing of *PIPEDA* is cause for some celebration. Canadians now have comprehensive rights relating to personal information in the private sector in Canada, in addition to longstanding protections in the public sector through the *Privacy Act* and its provincial equivalent legislation. That is not to say that either the private sector or public sector privacy laws fully protect the privacy rights of Canadians in every sense. They do not. But much of the essential framework for protecting those rights is now in place. Our Office will continue to enforce and analyze the application of *PIPEDA* to ensure that Canadians are well-served by it, and that the Canadian private sector understands and respects its obligations under the Act. We will continue to help the business community comply with it, and develop the best practices which will minimize burden and clarify expectations.

Interjurisdictional challenges

As with any relatively new legislation, problems can emerge. Where a province has enacted legislation that is substantially similar to all or part of *PIPEDA*, confusion may arise about which law – provincial or federal – will apply to certain information-handling practices. In other cases, the laws of two jurisdictions may be involved in addressing an issue. Some elements of the handling of personal information may be subject to a provincial law – the collection of the information within a province,

for example – while another element, such as the transborder disclosure of the information, may fall under *PIPEDA*.

However, the dust is beginning to settle around these jurisdictional issues due to concerted efforts by our Office, our provincial counterparts and industry. We are working with our provincial colleagues to streamline investigations where provincial and federal jurisdictions both apply. It is not our intention to make life difficult for those who must comply with the various privacy laws in Canada, and we clearly do not want to waste the limited resources available to privacy commissioners across Canada by duplicating efforts in conducting investigations and developing policy.

A complex and changing universe

There are many powerful forces in the universe in which we assert our privacy rights – galloping advances in surveillance and data-handling technologies, global competition in business which drives companies to obtain and use more personal information about customers and personnel, and the government imperative to acquire personal information to enhance administrative efficiency and respond to the security concerns of our world. Those of us attempting to protect this fundamental right must call out strongly for a debate that can be at times unpopular and demands a wealth of expertise in ever more complex fields of research. It is a challenge to keep up.

It is important to remember that information is power, and holding the personal information of individuals conveys power to the holder. One complexity that we have been grappling with this year stems from a convergence of two phenomena which are not new by any means, but which have reached a critical point. "Outsourcing" of data processing operations and call centres results in the personal information of Canadian residents or customers of Canadian companies being transferred and processed outside Canada. The thirst of foreign governments, particularly that of the United States and its allies in the war on terror, for access to personal information for "security" purposes means that the outsourced data may be accessed for law enforcement or national security purposes, outside our jurisdiction and the protection of our laws and our Court system.

Transborder data flow has been discussed in Canada since the 1960s. The original report on *Privacy and Computers,* published in 1972 by the Departments of Communications and Justice, dealt with the matter extensively, including matters of sovereignty. The issue prompted the Organization for Economic Cooperation and Development (OECD) to meet and develop the first Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data in 1980, and it drove

the European Union to pass its Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Yet we know very little about the details of transborder flows of personal information about Canadian residents and customers.

The current interest in the *USA PATRIOT Act* has raised an issue that has been lurking beneath the surface for decades – the extent to which Canadian businesses, and governments in Canada, should share personal information with foreign governments. The discussion is far from over. In fact, it is just beginning. Our Office endorsed many of the recommendations of the B.C. Information and Privacy Commissioner, David Loukidelis, on issues of transborder flows of personal information and we will continue working to ensure Canadians' privacy protections remain in place.

This Office is tasked with protecting privacy in Canada. We cannot do the job alone, we depend on all players in society to contribute to preserving the freedoms and rights which are an intrinsic part of Canada's rich fabric and history. The complexity of the current privacy environment has led our Office to launch a Contributions Program to help develop a national privacy research capacity in Canada. The findings of this first round of research projects will be available in 2005. These research findings will complement the existing policy research function within our Office, and in a modest way help to enrich the community of privacy scholarship in Canada.

Responding to a greater need

This Office received 723 complaints under *PIPEDA* between January 1 and December 31, 2004, more than double the 302 received in the previous calendar year. We closed 379 complaints, significantly more than the 278 cases closed in 2003. While the debate about the merits of having the Commissioner continue to operate as an ombudsman versus giving the Commissioner order-making powers remains, it is clear that our Office has accomplished much that is positive using the current ombudsman approach. Some 40 per cent of the complaints closed during the year were settled, and another seven per cent resolved – an indication that suasion, a prominent feature of the ombudsman approach, is an effective tool.

We have introduced a formal procedure of systematic follow-ups to complaint investigations under *PIPEDA*. We will now be in position to monitor the progress of organizations in implementing commitments they make during complaint investigations and in response to the recommendations our Office issues to them. Equally important, our Audit and Review Branch is strengthening its capacity to audit organizations subject to *PIPEDA*.

We faced many challenges in 2004, challenges that will only increase in frequency and complexity. This is not a time for those concerned about this fundamental human right called privacy to shrink from speaking out, from debate or from controversy. We will seize the opportunity of the 2006 review of *PIPEDA* to make recommendations about how to improve and better enforce the two pieces of legislation that we oversee, Although the Act is still very new in application, the dynamic environment of information policy demands that we keep current and try to ensure that the legislation also responds effectively to current threats. We are developing a list of improvements and suggestions for change, and we are confident that in another five years, when the next review is due, there will be more changes necessary. Parliament was wise to insist on periodic review of this legislation, and we will continue to push for review of the *Privacy Act* and inclusion of such a review mechanism in it.

This year, we have published two separate reports, dividing the Privacy Act from the Personal Information Protection and Electronic Documents Act (PIPEDA). We felt this was more appropriate given that the Privacy Act requires us to report on the fiscal year (2004-2005), while under PIPEDA we are required to report on the calendar year (2004). As well, each Act provides a separate framework for investigations and audits. Both our reports detail efforts we have taken to meet the growing demands on our Office to act as the guardians of privacy for Canadians on behalf of Parliament. There is much overlapping between these reports because many of our activities are not particular to one law or another and, increasingly, the policy issues are common across the two regimes.

Our Multi-Faceted Mandate

The Office of the Privacy Commissioner oversees two laws – the *Privacy Act*, which applies to federal government institutions, and *PIPEDA,* which governs personal information management in commercial activities.

Parliament requires our Office to ensure that both the federal public sector and private sector (in most provinces) are held accountable for their personal information handling, and that the public is informed about privacy rights. The mandate is not always well understood.

As an independent ombudsman, we are:

- An *investigator* and *auditor* with full powers to investigate and initiate complaints, conduct audits and verify compliance under both Acts;

- A *public educator* and *advocate* with a responsibility both to sensitize businesses about their obligations under *PIPEDA* and to help the public better understand their data protection rights;

- A *researcher* and *expert adviser* on privacy issues to Parliament, government and businesses; and

- An *advocate for privacy principles* involved in litigating the application and interpretation of the two privacy laws. We also analyze the legal and policy implications of bills and government proposals.

Policy Perspective

In 2004, our major preoccupations in the policy area were the heightened demands for personal information in the name of national security, the transborder flow of personal information, and that hardy perennial, privacy invasive technologies. From cell phones in locker rooms to global positioning systems in cars, the need to measure the impact of these new technologies and read the privacy law into their design and application is an ongoing challenge.

Technology

During the past year, the privacy implications of using Radio Frequency Identification Devices (RFIDs) as tracking devices have become increasingly prominent. RFIDs encompass technologies that use radio waves to read a serial number stored on a microchip. The microchip or tag can be placed in military equipment, passports, clothing, currency notes, vehicles, tires, pass cards and just about anything else sold in the marketplace, including food and drink packages. RFID applications include tracking goods from the manufacturer to the retail store, tracking people in a health institution or monitoring the movements of schoolchildren.

Depending on its individual design, an RFID can transmit information over long distances or only a few centimeters. It may hold no personal information or store extensive personal information, including biometrics. An RFID can be "active" or "passive" – active where it has its own power to broadcast information to a reader, or passive in that it lies dormant until awakened by a signal from a "reader."

The combination of tags, (sometimes smaller than a grain of rice or built invisibly into the paper of a product), powerful coding and advanced computer systems has created enormous economic incentives for companies to introduce RFID technology.

A recent market forecast predicts that the global value of the total RFID tag market will expand from $1.95 billion in 2005 to $26.9 billion in 2015. Given that each RFID tag may eventually cost only pennies, the potential scale of use is greater than almost any other single technology.

Organizations must think carefully about the legal implications of deploying RFID systems. Amidst the flurry of activity involving RFIDs, very few people fully understand the myriad of privacy implications. We are now encountering many marketplace uses of RFIDs, and expect that we will soon be investigating complaints about tracking the use of RFIDs.

Similarly, although there have been some interesting stories in the press about the use and abuse of global positioning technology, most individuals are unaware of the data that is accumulated by such devices. Fortunately, *PIPEDA* contains an innovative provision requiring openness with respect to information practices.

Organizations placing global positioning devices in consumer goods or conveyances (rental cars, for example) must identify what the device does, the data it collects, how long the data is kept, and who has access to it.

We are entering a world where computing power will be present in the most ordinary day-to-day devices. If we are not careful, that power will be used to gather or broadcast personal information in ways that greatly diminish our privacy, not to mention our autonomy and human dignity. As transmitting devices are built into roadsides, licence plates, currency and books, we are hard pressed to keep up with the potential privacy invasions and abuses. Canadians need to become more aware of and participate in discussing the privacy issues that flow from these developments. We need to shape our future into something that reflects the rights and freedoms we cherish today. From Reginald Fessenden to Marshall McLuhan, Canadians have shown leadership in the development of communications technologies and in communications theory. We are confident we can now rise to the current challenge, and demonstrate how we can use these powerful devices, in the world of ubiquitous computing and communications, yet maintain respect for that most fundamental of human values, privacy.

Parliament's Window on Privacy

The Privacy Commissioner of Canada is an Agent of Parliament who reports directly to the Senate and the House of Commons. As such, the OPC acts as Parliament's window on privacy issues. Through the Commissioner, Assistant Commissioners and

other senior OPC staff, the Office brings to the attention of Parliamentarians issues that have an impact on the privacy rights of Canadians. The OPC does this by tabling Annual Reports to Parliament, by appearing before Committees of the Senate and the House of Commons to comment on the privacy implications of proposed legislation and government initiatives, and by identifying and analyzing issues that we believe should be brought to Parliament's attention.

The Office also assists Parliament in becoming better informed about privacy, acting as a resource or centre of expertise on privacy issues. This includes responding to a significant number of inquiries and letters from Senators and Members of Parliament.

➤ *Appearances before Parliamentary Committees*

Appearances before committees of the Senate and the House of Commons constitute a key element of our work as Parliament's window on privacy issues. During the period covered by this report, the Privacy Commissioner and other senior OPC staff appeared nine times before Parliamentary committees: six times on bills with privacy implications and three times on matters relating to the management and operations of the Office.

The OPC appeared on the following bills before Parliamentary committees in 2004:

- Bill C-6, the *Assisted Human Reproduction Act* (March 3, 2004)
- Bill C-7, the *Public Safety Act, 2002* (March 18, 2004)
- Bill C-2, *An Act to Amend the Radiocommunication Act* (May 6, 2004)
- Bill C-12, the *Quarantine Act* (November 18, 2004)
- Bill C-22, *An Act to establish the Department of Social Development and to amend and repeal certain related Acts* (December 9, 2004)
- Bill C-23, *An Act to establish the Department of Human Resources and Skills Development and to amend and repeal certain related Acts* (December 9, 2004)
- Bill C-11, the *Public Servants Disclosure Protection Act* (December 14, 2004)

Regarding the management and operations of the Office, OPC officials appeared before Parliamentary committees on the following matters in 2004:

- Annual Report and Main Estimates 2003-2004 (November 17, 2004)
- Supplementary Estimates (December 1, 2004)

➤ *Other Parliamentary Liaison Activities*

The OPC has undertaken a number of other initiatives over the course of the past year to improve its ability to advise Parliament on privacy matters.

In May 2004, we created a dedicated Parliamentary liaison function within the Office to improve our relationship with Parliament. This function resides in the Research and Policy Branch, reflecting the OPC's desire to focus its Parliamentary affairs activities on providing in-depth and accurate policy advice to Senators and Members of Parliament.

Improving on how we assess, monitor and forecast Parliamentary activity has been a priority for us in the past year. The OPC put in place a new and improved system for monitoring the status of bills on Parliament Hill, as well as keeping tabs on new and emerging developments of interest to privacy promotion and protection. Our goal is to build bridges to departments so that we can comment earlier in the legislative process, when our criticisms could be dealt with more effectively. It is often too late when a bill has been introduced in the House of Commons, to rethink approaches to information issues.

The Office has responded to a significant number of inquiries and letters from Senators and MPs this year, and the Commissioner and Assistant Commissioners have also met privately with Senators and MPs who wished to discuss policy matters relating to privacy, or wanted to know more about the operations of the Office.

In late 2004, the OPC in conjunction with the Office of the Information Commissioner, and in collaboration with the Research Branch of the Library of Parliament, held an information session for Parliamentarians and their staff on the roles and mandates of both Offices. This information session was well attended and raised many questions among participants. We believe such information sessions contribute to increasing awareness of privacy issues on Parliament Hill, and look forward to holding more such sessions in the future.

➤ *Priorities for the Coming Year*

The Office expects to be busy in the area of Parliamentary affairs over the next fiscal year. There are a number of bills of interest to us expected in the upcoming session, and the statutory review by Parliament of the *Personal Information Protection and Electronic Documents Act* is expected to start in 2006. The OPC plans to play a

constructive role during this review, by providing thoughtful advice to Parliamentarians mandated with studying at how the Act has worked over the course of its first years of implementation, and how it may be modified and improved.

The OPC will continue to follow with interest the Parliamentary review of the *Anti-terrorism Act*. The Privacy Commissioner appeared twice before committee on this matter in fiscal year 2005-06—once before a Senate special committee reviewing the Act (May 9, 2005), and on another occasion before a sub-committee of the Commons Standing Committee on Justice (June 1, 2005).

We recognize that to act as an effective Agent of Parliament we need to have good working relationships with federal departments and agencies. The OPC plans to put more emphasis on identifying and raising privacy concerns when government initiatives are being developed rather than waiting until they reach Parliament, as this increases the possibility that privacy concerns will be taken into account.

National Security

In May 2004, the *Public Safety Act, 2002* was enacted. The Act, first introduced in November 2001 in the wake of the September 11 terrorist attacks, allows the Minister of Transport, the Commissioner of the RCMP and the Director of the Canadian Security Intelligence Service (CSIS), without a warrant, to compel air carriers and operators of aviation reservation systems to provide information about passengers. While this may seem reasonable given the risks that terrorists pose to air transport, authorities are not using this information exclusively for anti-terrorism and transportation safety. The *Public Safety Act, 2002* also allows the information to be used to identify passengers for whom there are outstanding arrest warrants for a wide range of lesser criminal offences. In other words, the machinery of anti-terrorism is being used to meet the needs of ordinary law enforcement, lowering the legal standards that law enforcement authorities in a democratic society must normally meet.

The retention and mining of private sector data collections by government sends a troubling signal to private sector organizations trying to comply with privacy legislation. If the government can use data to manage risks from unknown individuals, why can't the private sector? Private sector companies are cutting down on data collection to comply with *PIPEDA*, but now the government is asking them to retain it so that they can access it for government purposes. *PIPEDA* sets a high bar for organizations with respect to using and disclosing personal information without consent for the purposes of investigating fraud and other illegal activities that have

an impact, while the standards that government must meet under the *Privacy Act* are much less rigorous.

In 2004, our Office raised concerns about a provision in the *Public Safety Act, 2002* that amends *PIPEDA*. The amendment allows organizations subject to *PIPEDA* to collect personal information, without consent, for the purposes of disclosing this information to government, law enforcement and national security agencies if the information relates to national security, the defence of Canada or the conduct of international affairs. Allowing private sector organizations to collect personal information without consent in these circumstances effectively co-opts them into service for law enforcement activities. This dangerously blurs the line between the private sector and the state. We comment more extensively on public safety issues in the *Privacy Act* Annual Report, but this is also an important issue under *PIPEDA* because of the potential for inappropriate manipulation of private sector data to serve state interests.

The 2001 *Anti-terrorism Act* contained a provision requiring a review after three years. The Senate has appointed a special committee to conduct its review. The House of Commons review is being conducted by the Subcommittee on Public Safety and National Security, a subcommittee of the Standing Committee on Justice, Human Rights, Public Safety and Emergency Preparedness. However, the Commons Committee is not looking at the many other pieces of legislation that were also enacted or amended in the wake of the terrorist attacks. Many of these laws contain extensive powers to intrude and should be examined as well.

The *Official Secrets Act* was replaced by the *Security of Information Act* in 2001. Section 10 of the new Act allows the deputy head of a department, on the issuance of a certificate, to bind members of the private sector to secrecy for life with respect to methods of investigation or special operations. We understand that sometimes it is necessary to deal with threats to our national security and critical infrastructure, but we raise the warning flag when we see new powers without complementary oversight provisions to ensure accountability. We have raised the issue of accountability and oversight in our submission to Parliament on the review of the *Anti-terrorism Act*, but this particular provision is in the *Security of Information Act*, and we think it merits public reporting on how often it is being used.

In the war on terror, governments have made it clear that they must have the cooperation of the private sector to ensure public safety and the security of the critical infrastructure. From the perspective of this Office, we must also ask whether we can

effectively oversee the private sector and the role it might play in security matters. In the United States, the use of private sector databases and information retention for law enforcement and anti-terrorism continue to attract criticism. We do not know the extent to which such use and retention occurs in Canada, but it is an issue of growing concern to Canadians and we are trying to get answers so that we can respond to their queries and complaints.

In July 2004, Canada began enforcing new marine security requirements under the International Maritime Organization's International Ship and Port Facility Security (ISPS) Code. To further enhance port security, Transport Canada is proposing to introduce a controversial Marine Facilities Restricted Area Access Clearance Program to screen port workers who have access to restricted areas. This screening process will involve collecting significant amounts of personal and potentially sensitive information about as many as 30,000 port workers. Once again, the extent to which such security checks are dependent on private sector information databases is of interest to our Office.

The issue of data-matching is an old one that has pre-occupied privacy scholars and oversight bodies for over twenty years. Technology has advanced, and we really no longer speak of data-matching but rather data-mining. There are many invisible uses of integrated information systems that collect and analyze significant amounts of personal information related to our travel patterns, our financial transactions, and even the people with whom we associate. Many of these systems would be viewed by consumers as immensely positive, were they to know of them and fully understand them because they provide faster loan approvals, instant recognition of credit card theft, and better customer service. However, these systems also now analyze deep reservoirs of personal information in an attempt to find patterns that might suggest that an individual is a security threat, a money launderer or is engaged in financing a terrorist group.

As law enforcement and national security agencies collect more information from more sources about more individuals, the chances increase that decisions will be based on information of questionable accuracy, or that information will be taken out of context.

When personal information is misused, misinterpreted or inappropriately disclosed it can have serious adverse consequences for individuals, families, and even communities. The problem is aggravated when, because of secrecy provisions and a lack of transparency, we cannot find out where the system broke down or on what basis individuals were wrongly targeted.

Outsourcing and Transborder Flows of Personal Information

The transfer of personal information from Canada into foreign jurisdictions (transborder data flows) is another issue as old as privacy legislation itself. Scholars and government policy experts in the 1960s and 70s anticipated greater flows of data in the future as communications technology improved. Whether they could have predicted the enormity of the global flow of data that we see today is another question.

In 2004, the transborder issue became more visible in Canada when a complaint was raised in British Columbia about the outsourcing of health information processing from the B.C. government to a U.S.-linked company operating in the province. The B.C. Government Employees Union alleged that the information would be available to the U.S. government under the expansive search powers introduced in 2001 by the *USA PATRIOT Act*. Although there have been many high profile instances of outsourcing in recent years, with occasional concern about the privacy implications, this appeared to be the first where a specific piece of legislation was singled out as a threat. The B.C. Information and Privacy Commissioner, David Loukidelis, took the step of issuing a call for public comment on this issue, and we submitted a brief in response.

Our submission explained that a company holding personal information *in Canada* about Canadian residents was not required to provide the information to a foreign government or agency in response to a direct court order issued abroad. In fact, the organization in Canada would in many cases violate *PIPEDA* if it disclosed the information without the consent of the individuals to whom the information relates.

However, there would be no violation of *PIPEDA*, for example, if the organization disclosed the information under Canadian legislation such as the *Aeronautics Act* provision that allows Canadian air carriers to disclose passenger information to foreign states.

We also concluded that an organization operating in a foreign country and that holds personal information about Canadians *in that country* must comply with the laws of that country. This means that when a Canadian organization outsources the processing of personal information to a company in the United States or another country, that information may be accessible under the laws of those countries.

The foreign government could of course request the same information through a mutual legal assistance treaty (MLAT) and ask the federal Department of Justice to arrange for Canadian law enforcement agencies to obtain the information from corporations in Canada for them – a system of government-to-government cooperation that predates the *USA PATRIOT Act*.

PIPEDA deals succinctly with transborder data flows in Principle 4.1.3 of the Schedule to the Act. This principle requires that information transferred for processing must be protected at a level "comparable" to that provided by *PIPEDA*. However, when data is held or processed outside Canada there is a loss of control over what a foreign jurisdiction might do with that information and our Office has no oversight authority.

We urgently need to address these flows of personal information so that we can ensure protection of the personal information we send around the world. A series of news reports in early 2005 concerning security breaches by companies in other countries holding personal information about Canadians has further emphasized the importance of devoting attention to transborder flows of personal information.

Research into Emerging Privacy Issues

On June 1, 2004, our Office officially launched a Contributions Program to support research by not-for-profit groups, including education institutions, industry and trade associations, and consumer, voluntary and advocacy organizations, into the protection of personal information and the ways to protect it. The program represented a milestone in the development of national privacy research capacity in Canada. The program is designed to assist our Office to foster greater public awareness and understanding of privacy.

The 2003-2004 Contributions Program had two key priorities. The first was to examine how and to what extent emerging technologies affect privacy. These included video surveillance, RFIDs, location technology and biometrics. Many of these technologies have their most profound impact on privacy when they are in the hands of government, but they often also have significant privacy implications when used by the private sector.

The second priority of the research program related more directly to the implementation of *PIPEDA*, especially since new sectors of the economy became subject to the Act in January 2004. This part of the Contributions Program focused on awareness and promotion of good privacy practices as a key component of responsible commercial behaviour.

The projects that were funded for a total of $371,590 include:

FUNDED PROJECTS		
Canadian Marketing Association **Toronto, Ontario**	**Taking Privacy to the Next Level** *Assess and develop privacy best practices to assist businesses in better handling customer personal information under PIPEDA*	$50,000
École nationale d'administration publique (ENAP) **Quebec, Quebec**	**Study on the use of video surveillance cameras in Canada** *Perceptions, issues, privacy impact and best practices on the use of video surveillance*	$50,000
Queen's University **Kingston, Ontario**	**Location Technologies: Mobility, Surveillance and Privacy** *Trends and stated and implicit purposes of technology with workers, consumers, travelers and citizens*	$49,972
The B.C. Freedom of Information and Privacy Association **Vancouver, British Columbia**	***PIPEDA* & Identify Theft: Solutions for Protecting Canadians** *Gap analysis on weaknesses in personal information management practices that lead to identity theft and policy recommendations for PIPEDA implementation*	$49,775
Universities of Alberta and Victoria **Edmonton, Alberta** **Victoria, British Columbia**	**Electronic Health Records and *PIPEDA*** *Implementation of PIPEDA in the health care sector and application to electronic health records in the primary care setting*	$49,600
University of Toronto **Toronto, Ontario**	**A review of Internet privacy statements and on-line practices** *Evaluation of implementation of PIPEDA and privacy statements on the Internet by companies in the telecommunications, airline, banking and retail sectors*	$48,300
University of Victoria **Victoria, British Columbia**	**Location-Based Services: An Analysis of Privacy Implications in the Canadian Context** *Privacy implications of geographic location-based services — issues raised and major challenges and guidance to encourage compliance*	$27,390
Option Consommateurs **Montreal, Quebec**	**The challenge of consumer identification with new methods of electronic payment** *Current and new proposed methods of identification of consumers for electronic payment and risk factors*	$17,100
Simon Fraser University **Vancouver, British Columbia**	**Privacy Rights and Prepaid Communications Services: Assessing the Anonymity Question** *Justification and feasibility of regulatory measures to eliminate the sale of anonymous prepaid communications services in Canada*	$14,850
Dalhousie University **Halifax, Nova Scotia**	**An Analysis of Legal and Technological Privacy Implications of Radio Frequency Identification Technologies** *Study of RFID technology and privacy impact and legal measures to protect privacy*	$14,603

The projects are to be completed in 2005. We will post links to the research results on our Web site.

Substantially Similar Provincial Legislation

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 *PIPEDA*.

Beginning on January 1, 2004, *PIPEDA* extended to all commercial activities. However, section 26(2)(b) allows the Governor in Council to issue an order exempting certain activities from the ambit of *PIPEDA*. This order can be issued if the province has passed legislation that is deemed substantially similar to *PIPEDA*. The order can exempt 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 subject to that legislation that occurs within the province.

The intent of this provision is to allow provinces and territories to regulate the personal information management practices of organizations within their borders while ensuring seamless and meaningful privacy protection throughout Canada.

If the Governor in Council issues an Order declaring a provincial act to be substantially similar, the collection, use or disclosure of personal information by organizations subject to the provincial act will not be covered by *PIPEDA*. Interprovincial and international transactions will be subject to *PIPEDA,* and *PIPEDA* will continue to apply within a province to the activities of federal works, undertakings and businesses that are under federal jurisdiction, such as banks, airlines, and broadcasting and telecommunications companies.

Process for assessing provincial and territorial legislation

On August 3, 2002, Industry Canada published a notice in the *Canada Gazette* Part 1 setting out how it will determine whether provincial/territorial legislation is deemed substantially similar to *PIPEDA*.

A province, territory or organization triggers the process by advising the Minister of Industry of legislation that they believe is substantially similar to *PIPEDA*. The Minister may also act on his or her own initiative and recommend to the Governor in Council that provincial or territorial legislation be found substantially similar. The notice states that the Minister will seek the Privacy Commissioner's views and include those views in the submission to the Governor in Council. The public and interested parties will also have a chance to comment.

According to the *Canada Gazette* notice, the Minister will expect substantially similar provincial or territorial legislation to:

- Incorporate the ten principles found 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 legislation enacted to date

Quebec's *An Act Respecting the Protection of Personal Information in the Private Sector* came into effect, with a few exceptions, on January 1, 1994. The legislation sets out detailed provisions that enlarge upon and give effect to the information privacy rights contained in Articles 35 to 41 of the *Civil Code of Quebec*. In November 2003, the Governor in Council issued an Order in Council (P.C. 2003-1842, 19 November 2003) exempting organizations in that province, to which the provincial legislation applies. *PIPEDA* continues to apply to federal works, undertakings or businesses and to interprovincial and international transactions.

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

Using the criteria set out in the *Canada Gazette* notice – the presence of the ten principles found in Schedule 1 of *PIPEDA*, independent oversight and redress and a provision restricting collection, use and disclosure to legitimate purposes (a reasonable person test) – we concluded that the British Columbia and Alberta laws are substantially similar to *PIPEDA*.

For Alberta and British Columbia, the Governor in Council issued two Orders in Council (P.C. 2004-1163, 12 October 2004 and P.C. 2004-1164, 12 October 2004) exempting organizations, to which the provincial legislation applies. *PIPEDA* continues to apply to federal works, undertakings or businesses and to interprovincial and international transactions..

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. Our Office has informed Industry Canada that we believe *PHIPA* as it relates to health information custodians to be substantially similar to *PIPEDA*. Industry Canada has requested comments on a proposed order declaring the Ontario law substantially similar to *PIPEDA*, but an Order in Council had not been issued when we prepared this Annual Report.

Jurisdictional Issues

For most of 2004 – beginning January 1 and ending October 12 – the Alberta and B.C. private sector privacy laws were in force, but had not yet been declared substantially similar to federal law. During this period, both the provincial private sector laws and *PIPEDA* applied. There was concurrent jurisdiction.

In Ontario, *PIPEDA* applied to personal information in the private sector (except for provincially-regulated employees) beginning on January 1, 2004. Ontario's *Personal Health Information Protection Act, 2004* (*PHIPA*) came into force on November 1, 2004. Since November 1, both *PIPEDA* and the Ontario legislation have applied to personal health information in the private sector. As was the case with the Alberta and B.C. private sector legislation until Ontario's *PHIPA* is deemed substantially similar, both *PIPEDA* and *PHIPA* will apply to personal health information in the private sector.

Even a "substantially similar" order may not be broad enough to eliminate concurrent jurisdiction completely. With Ontario, for example, the "substantially similar" order

will not apply to some entities regulated by Ontario's *PHIPA*. The proposed order may apply in respect of the rules governing health information custodians; Ontario's *PHIPA* would therefore be the sole law applying to health information custodians' collection, use, or disclosure of personal information in Ontario.

But the substantially similar order would not apply to third parties who receive personal information from health information custodians. *PHIPA* imposes rules on non-health information custodians only about the use and disclosure of personal health information. *PHIPA* does not regulate other privacy obligations, such as collection, access and safeguards. Therefore, *PIPEDA* would continue to apply to these activities.

One simple way to avoid the work of Commissioners overlapping in areas of concurrent jurisdiction is to reach informal agreements about who handles what. Our Office will work closely with Ontario, as it has with B.C. and Alberta, to ensure that both Acts are enforced in the most seamless way possible.

Even where a "substantially similar" order exists, not all intraprovincial commercial activity will necessarily be covered by the order, and jurisdictional boundaries are not always clear. Complex jurisdictional issues may still arise and require close collaboration between jurisdictions to deal with them.

For instance, Alberta's *Health Information Act* (*HIA*) applies to health service providers who are paid under the Alberta Health Care Insurance Plan to provide health services. On this definition, *HIA* does not cover health practitioners, who provide health services privately. While Alberta's *Personal Information Protection Act* (*PIPA*) does apply to private sector organizations, it does not apply to health information, as defined by *HIA,* which is collected, used or disclosed for health care purposes. Under this regime, the collection, use or disclosure of personal health information by practitioners working in private practice to provide health services seems to have fallen between the cracks; it is not currently covered by either Alberta Act. Hence, such activity is subject to the federal *PIPEDA*.

As a postscript, a bill was introduced in the Legislative Assembly of Alberta in March 2005 to amend Alberta's *PIPA* in favour of bringing the activities of private practitioners who collect, use or disclose personal health information in the course of providing health services clearly within the scope of *PIPA*. This amendment has since come into force and resolved this jurisdictional problem.

Flows of personal information across provincial boundaries

Another aspect of the jurisdictional issue arises with flows of information across provincial boundaries. An Alberta company may disclose personal information to another company in Saskatchewan in the course of a commercial activity. An individual could complain about this interprovincial transaction to our Office. Alternatively, an individual who wants to complain about the disclosure of personal information by the Alberta company could direct the complaint to the Alberta Information and Privacy Commissioner under Alberta's *PIPA*. However, if the individual is complaining about the collection in Saskatchewan of their personal information, he or she may direct the complaint to the Privacy Commissioner of Canada, as Saskatchewan does not have substantially similar legislation in place governing its private sector organizations' activities. Whether the complaint is initiated in Alberta, with our Office, or both, our respective offices will work together to coordinate our work where possible.

Sometimes the jurisdictional issue is entangled. In one case handled by our Office, the complainant worked for an organization in one of the western provinces that has substantially similar legislation. The organization provides disability insurance. The individual applied to the insurance company, located in Quebec, for access to her files. Those files are kept in Toronto. The insurance company responded as if *PIPEDA* regulated the question. Is *PIPEDA* the appropriate legislation or does it fall to one of the provinces?

In another case, an individual worked for a company in one of the western provinces with substantially similar legislation. Through the company, the individual had an employee assistance program (EAP) in Ontario, and complained about a disclosure by the EAP. Because Ontario does not yet have substantially similar legislation, *PIPEDA* would apply in Ontario. But is this an Ontario issue – because the EAP is located in Ontario – or is it within the jurisdiction of the western province under that province's private sector legislation?

Streamlining our approach to jurisdictional issues

Federal and provincial Commissioners are working together to resolve jurisdictional challenges. This process has been collegial, not confrontational. Some individuals may raise jurisdictional matters in the courts but these issues can largely be resolved through discussion. Our goal in every case is to establish as simple and clear a mechanism as possible for individuals and organizations.

One way we have sought to streamline our approach to jurisdictional and related investigative issues is to establish a regional private sector privacy forum with Alberta

and British Columbia. This forum operates under the authority of the federal and provincial Commissioners and seeks to coordinate and harmonize federal and provincial oversight of the private sector in Canada. Senior investigations and legal staff from each of the Commissioners' offices take part in monthly teleconferences and twice-yearly meetings. The forum serves many functions, but among the most important is to develop procedures for determining jurisdiction, transferring complaints and conducting parallel investigations.

Federal and provincial Commissioners have also been working to develop protocols for handling investigations where there may be overlapping jurisdiction. In March 2004, the Privacy Commissioner of Canada sent a letter of understanding to the Information and Privacy Commissioners of Alberta, British Columbia, and a similar letter to the Ontario Information and Privacy Commissioner in January 2005, to confirm discussions about the handling of complaints relating to organizations in those provinces. In part, these letters of understanding set out how our Office would handle complaints both before and after a finding of "substantially similar" occurs in respect of the provincial laws.

These letters of understanding are available on the Privacy Commissioner of Canada's Web site (www.privcom.gc.ca). There is further information about jurisdictional issues, including a fact sheet, on our Web site, as well as on the Web sites of other provincial Information and Privacy Commissioners.

Our Office has had a long-standing relationship with the *Commission d'accès à l'information* (CAI) in Quebec. Quebec was the first Canadian jurisdiction to adopt private sector privacy legislation in 1994. In order to take advantage of the rich body of jurisprudence accumulated in Quebec since 1994, we have commissioned a document to review and summarize Quebec's experience to date.

In order to ensure that this may be as helpful as possible to all jurisdictions, we established an External Editorial Board to assist in the project. The members are:

Madeleine Aubé, General Counsel, Commission d'accès à l'information du Québec
Jeffrey Kaufman, Fasken Martineau, Toronto
Mary O'Donoghue, Senior Counsel, Ontario Information and Privacy Commissioner's Office
Murray Rankin, Arvay Finlay, Victoria
Frank Work, Q.C., Information and Privacy Commissioner of Alberta

This document was published in August 2005 and is available on our Web site.

The Alberta and federal Commissioners have already cooperated in investigating issues that have both federal and provincial elements – see for example, the case summary relating to a joint federal/provincial investigation of misdirected medical information mentioned below in the section on Incidents under *PIPEDA*. In another case, Edmonton police conducting an investigation found information used in determining security clearances for Alberta government employees. The information included credit reports. The aspects of the investigation relating to correction of erroneous credit reports fell to the Alberta Information and Privacy Commissioner, while our Office handled the systemic issue of retention of credit reports.

While the constitutional pitfalls may be numerous, we hope a practical approach to the application of the way personal information protection legislation in Canada will yield, overall, effective privacy protection in Canada.

Evolution of the *Personal Information Protection and Electronic Documents Act*

Statutory Changes

PIPEDA Amendments

The *Public Safety Act, 2002*[1] included two amendments to *PIPEDA*. Their effect is to permit organizations to collect and use personal information without consent for the purposes of disclosing this information when required by law or to government institutions if the information relates to national security, the defence of Canada or the conduct of international affairs.

The Commissioner appeared before the Senate Standing Committee on Transport and Communications on March 18, 2004, to voice her concerns about these amendments.[2] In her statement to the Committee, the Commissioner pointed out that the amendments will allow organizations to act as agents of the state by collecting information without consent for the sole purpose of disclosing it to government and law enforcement agencies. She asked that the changes to *PIPEDA* be dropped, and expressed concern that the wording of these changes was so broad that they could apply to any organization subject to *PIPEDA*, with no limit on the amount of information to be collected or the sources of the information.

The *Public Safety Act, 2002*, without the changes recommended by the Commissioner, came into force on May 11, 2004.

[1] See http://www.parl.gc.ca/PDF/37/3/parlbus/chambus/house/bills/government/C-7_4.pdf

[2] See http://www.privcom.gc.ca/speech/2004/sp-d_040318_e.asp

Amendments to Other Acts

The *Federal Court Rules, 1998* were enacted before *PIPEDA*. Because of this, rule 304(1)(c), which deals with service of a "notice of application", had no reference to *PIPEDA*. Accordingly, in February 2003 our Office's Legal Branch requested an amendment to rule 304(1)(c) to include notifying the Privacy Commissioner whenever an application is filed under *PIPEDA*, as well as when one is filed under the *Privacy Act*.

The *Rules Amending the Federal Court Rules, 1998* came into force on November 29, 2004 and were published in the *Canada Gazette, Part II* of December 15, 2004 as SOR/2004-283. Section 16 of this document amended rule 304(1)(c) to include *PIPEDA* so that the text of that section now reads:

> […] 304(1)(c) where the application is made under the *Access to Information Act*, Part 1 of the *Personal Information Protection and Electronic Documents Act*, the *Privacy Act* or the *Official Languages Act*, the Commissioner named for the purposes of that Act; and […]

2006 Review of *PIPEDA* by Parliament

The Office has been preparing for the upcoming review of *PIPEDA* by Parliament, scheduled to take place in 2006. The year 2006 may appear a long way off from the vantage point of this 2004 Annual Report, but our experience over the past four years in overseeing the application of the law has convinced us that this a good time to begin preparing, and that our Office is also the right place to begin. This Office will be active in developing policy positions to make the operation of the law simpler and more effective for organizations and individuals alike, and to ensure that the fair information practices at the heart of *PIPEDA* are translated into practice.

Like any significant new law, *PIPEDA* has its problems. It is hard to get the first version of any law completely "right", particularly when it is breaking new ground and providing new rights and obligations. We don't have all the solutions for these problems, but we have identified several issues and, in some cases, suggested possible ways to address them.

- **Scope**

  - Does *PIPEDA* deal effectively with employee information? Many of our complaints arise in the context of the employer/employee relationship. The current *PIPEDA* doesn't always fit that relationship. Both the B.C. and Alberta private sector legislation deal with employee information under a separate set of rules.

  - There are clear overlaps between *PIPEDA* and the *Canada Labour Code* and between the mandate of the Office of the Privacy Commissioner and that of labour arbitrators.

  - There remains uncertainty about the distinction, if there is one, between "commercial" activity, as defined in the Act, and "professional" services.

  - Elsewhere in this report, we describe a case that involved sending unsolicited commercial e-mail to a business e-mail address. The legislated definition of "personal information" excludes certain business information such as address and phone number. Should business e-mail addresses also be excluded?

- **Consent**

  - Consent is at the heart of *PIPEDA*. It is also one of the most problematic issues under the Act. For example, must an organization obtain the consent of all its customers when it proposes to disclose their information in the context of a business merger or acquisition? That seems to be what the law requires, but it is not always practicable for several sound business reasons. The B.C. and Alberta private sector laws both deal with this issue head-on and establish rules to protect customer information in these circumstances. Should *PIPEDA* do the same?

- **Oversight**

  - *PIPEDA* gives the Commissioner the powers of an ombudsman – in other words, no power to issue an order or levy a penalty against an organization violating *PIPEDA*. While we think that the ombudsman model works well overall (in fact, even in jurisdictions that have order-making powers on privacy matters, the vast majority of cases are settled without an

order) we are aware that oversight bodies in other jurisdictions have enforcement powers. Parliament may want to consider the advantages and disadvantages of both models in its 2006 review of *PIPEDA*.

These are simply a few of the issues that may need to be addressed in the five year review of the Act.

Complaints

In 2004, *PIPEDA* reached its full extension, to cover all commercial activities in provinces without substantially similar legislation. Over the year, we saw a significant spike in complaints filed under *PIPEDA*: we received 723 complaints between January 1 and December 31, more than double the 302 received in the previous calendar year. The expansion of the Act's coverage appears to be a considerable factor in the increase. Financial institutions were once again the most frequent object of complaints, as one might expect given the vast quantities of personal information that pass through their hands. They were followed by the telecommunications sector, also a front-runner in years past. But complaints in four areas new to us – insurance, sales, accommodation, and professionals – accounted between them for over 25 per cent of the complaints. It remains to be seen whether we will see further increases, as the Act becomes better known to Canadians.

PIPEDA COMPLAINTS RECEIVED BETWEEN JANUARY 1 AND DECEMBER 31, 2004

Sectoral Breakdown

Sector	Count	Percentage
Financial Institutions	212	29.3%
Telecommunications	125	17.3%
Insurance	82	11.3%
Sales	82	11.3%
Transportation	67	9.3%
Health	36	5%
Accommodation	18	2.5%
Professionals	15	2.1%
Services	10	1.4%
Other	76	10.5%
Total	**723**	**100%**

The complaints related to the following concerns:

Breakdown by Complaint Type

Complaint type	Count	Percentage
Use and Disclosure	286	39.6%
Collection	172	23.8%
Access	112	15.5%
Safeguards	40	5.5%
Consent	37	5.1%
Accuracy	22	3%
Correction/Notation	11	1.5%
Fee	12	1.7%
Other	4	0.6%
Retention	6	0.8%
Accountability	9	1.2%
Time Limits	9	1.2%
Challenging Compliance	1	0.2%
Openness	2	0.3%
Total	**723**	**100%**

During the year, we closed 379 complaints. This is an improvement over the previous year, where we closed 278. Nonetheless, in both years we received more complaints than we closed. This presents the Office with the risk of a developing backlog.

We are taking initiatives to address this, including reallocating resources and reviewing the way in which we conduct our investigations. One of the most promising approaches may be a new emphasis, since January 2004, on a category of complaint disposition, "Settled during the course of the investigation." These are cases in which, during the investigation, we have helped bring about a solution satisfactory to all parties.

COMPLAINT INVESTIGATIONS TREATMENT TIMES – *PIPEDA*

This table represents the average number of months it has taken to complete a complaint investigation by disposition, from the date the complaint is received to when a finding is made.

By Disposition

For the period between January 1 and December 31, 2004.

Disposition	Average Treatment Time in Months
Early resolution	2.9
Discontinued	5.6
Settled	7.2
No jurisdiction	7.8
Overall average	8.3
Resolved	10.5
Not well-founded	11.0
Well-founded	11.0
Overall Average	8.3

By Complaint Type

For the period between January 1 and December 31, 2004.

Complaint Type	Average Treatment Time in Months
Fee	3.4
Accuracy	6.4
Consent	6.9
Time Limits	8.1
Use and Disclosure	8.2
Access	8.3
Safeguards	8.4
Correction/Notation	8.5
Collection	8.9
Retention	9.5
Accountability	12.0*
Challenging compliance	12.0*
Overall average	8.3

* The average treatment times for these two complaint types in fact represent one case for each.

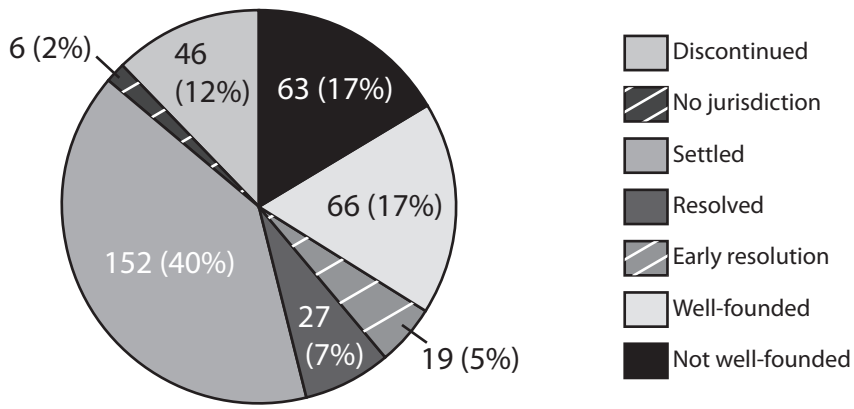
Settling complaints in investigation is not new, but our emphasis on it is. In 2003, settled cases represented two per cent of our completed cases. In contrast, of the 379 cases concluded in 2004, 152 – just over 40 per cent – fell in the "settled" category. This was by far the most frequent disposition of our cases.

This new emphasis on settlement is an important element in dealing with the volume of complaints that we face. Over the course of the year, settlement of a complaint took, on average, less time than any other complaint resolution except discontinuance (where, for instance, the complainant may no longer want to pursue the matter or cannot be located) or early resolution, where the issue is dealt with before any investigation takes place.

If we take the figures for the "settled" and "early resolution" categories, we can see that 45 per cent of our complaints are concluded without the investment of resources entailed in a complete investigation. This is welcome news to an organization facing an increasing workload.

That we were able to settle so many of our cases suggests that organizations and individual complainants welcome the opportunity to resolve complaints expeditiously and pragmatically. This fits well with our ombudsman role; we are in this business, after all, to help people resolve problems. At the same time, of course, we have a responsibility to ensure that the public policy intentions of *PIPEDA* are respected. Our Office, as much as the complainant and the organization, has an interest in any settlement; our view, however, is that enthusiasm for settlement does not mean settling complaints at any cost. Our investigators work closely with the parties in the settlement process to ensure that systemic issues raised in a complaint are addressed.

COMPLAINTS CLOSED BETWEEN JANUARY 1 AND DECEMBER 31, 2004: TYPE OF CONCLUSION

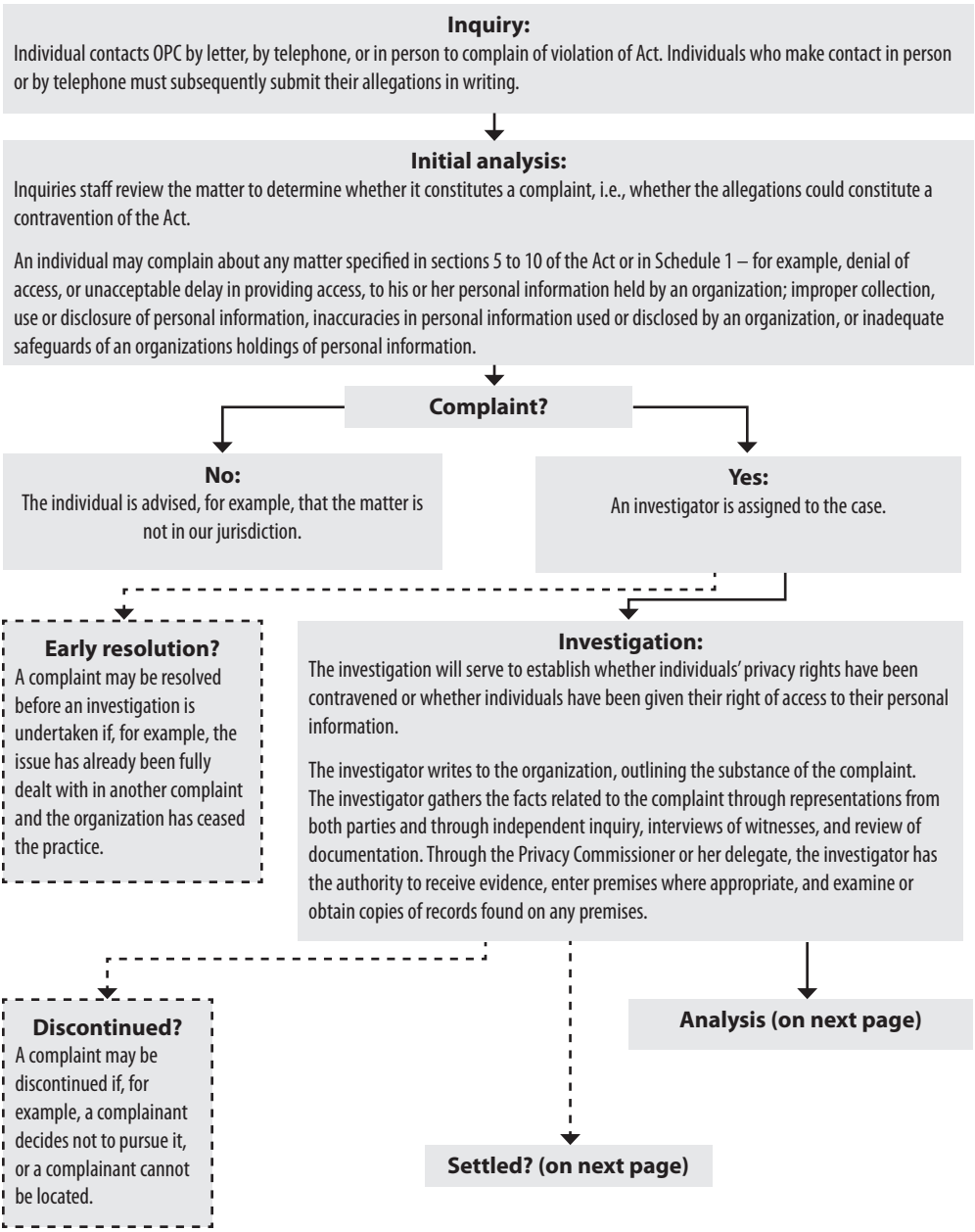


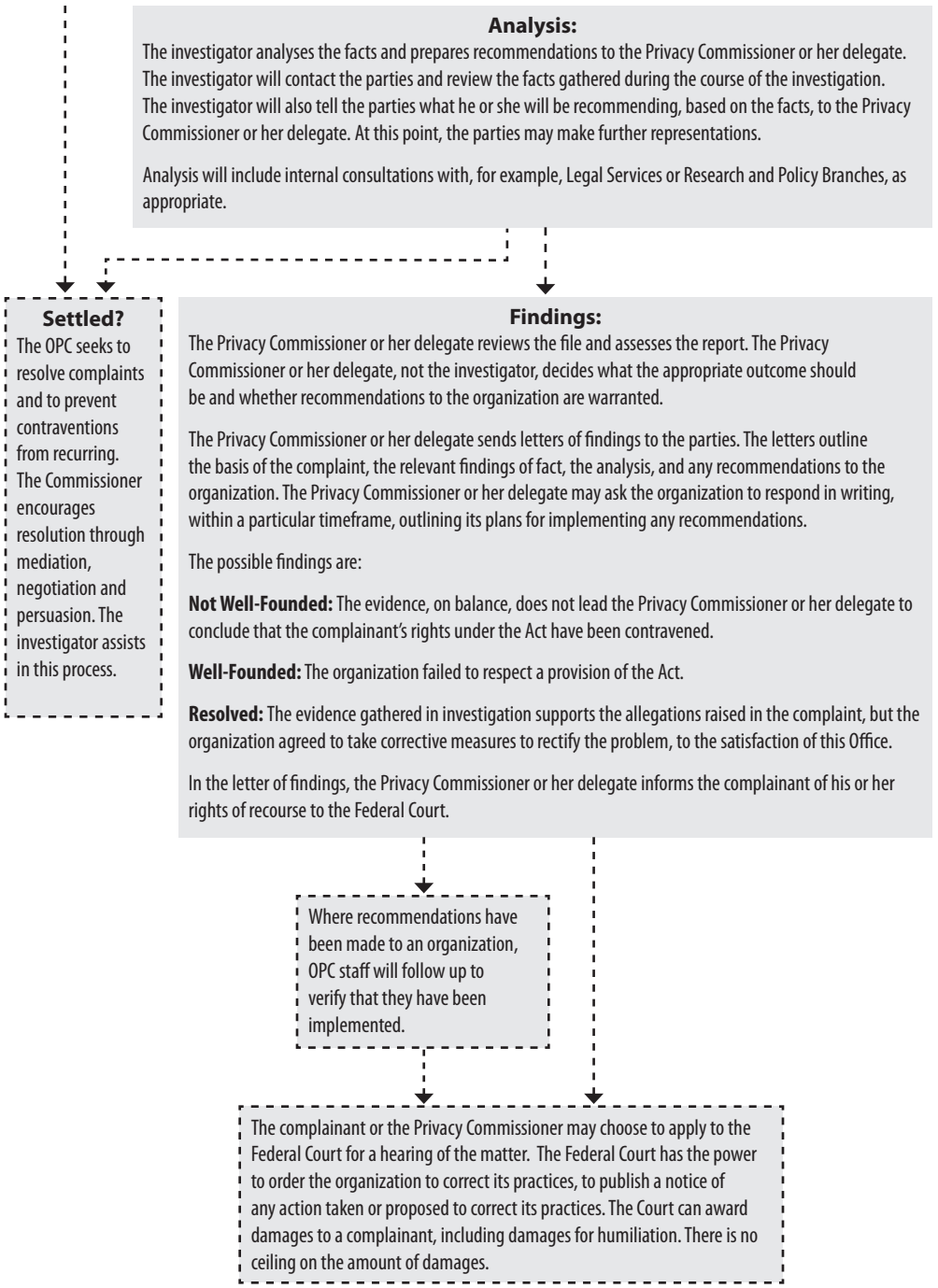
Definitions of Complaint Types under *PIPEDA*

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 his or her personal information, either because some documents or information are missing or 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 failed to identify an individual responsible for overseeing its compliance with the Act.
- **Accuracy.** An organization has failed to ensure that the personal information that 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.

Investigation Process under *PIPEDA*





Note: a broken line (- - - -) indicates a *possible* outcome.

Definitions of Findings under *PIPEDA*

The Office has developed a series of definitions of "findings" to explain the outcome of its investigations under *PIPEDA*:

Not well-founded: This means that the investigation uncovered no or insufficient evidence to conclude that an organization violated the complainant's rights under *PIPEDA*.

Well-founded: This means that an organization failed to respect a provision of *PIPEDA*.

Resolved: This means that the investigation substantiates the allegations, but that the organization has taken or has committed to take corrective action to remedy the situation, to the satisfaction of our Office.

Settled during the course of the investigation: This means that the Office has helped negotiate a solution that satisfies all involved parties during the course of the investigation. No finding is issued.

Discontinued: This means that the investigation ended before a full investigation of all the allegations. A case may be discontinued for any number of reasons — for instance, the complainant may no longer want to pursue the matter or cannot be located to provide information critical to making a finding.

No jurisdiction: This means that the investigation leads to a conclusion that *PIPEDA* does not apply to the organization or to the activity that is the subject of the complaint.

Early resolution: This is a new type of disposition. It applies to situations where the issue is dealt with before a formal investigation occurs. For example, if an individual files a complaint about a type of issue that the Office has already investigated and found to comply with *PIPEDA*, we would explain this to the individual. "Early resolution" would also apply when an organization, on learning of allegations against it, addresses them immediately to the satisfaction of the complainant and this Office.

FINDINGS BY COMPLAINT TYPE

Complaints closed between January 1 and December 31, 2004

	Discontinued	Early Resolution	No Jurisdiction	Not Well-founded	Resolved	Settled	Well-founded	TOTAL
Access	10	3	2	8	5	20	14	**62 (16%)**
Accountability	0	0	0	0	0	1	0	**1 (0%)**
Accuracy	2	1	0	1	0	1	0	**5 (1%)**
Challenging Compliance	0	0	0	0	0	0	1	**1 (0%)**
Collection	10	2	1	25	15	30	13	**96 (25%)**
Consent	2	1	0	0	0	3	1	**7 (2%)**
Correction/ Notation	0	0	0	0	0	1	1	**2 (1%)**
Fee	0	2	1	0	0	2	0	**5 (1%)**
Retention	0	0	0	0	1	1	0	**2 (1%)**
Safeguards	0	0	1	2	0	13	2	**18 (5%)**
Time Limits	0	0	0	2	1	3	1	**7 (2%)**
Use and Disclosure	22	10	1	25	5	77	33	**173 (46%)**
TOTAL (# and %)	**46 (12%)**	**19 (5%)**	**6 (2%)**	**63 (17%)**	**27 (7%)**	**152 (40%)**	**66 (17%)**	**379**

Inquiries

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

In 2004, the Office received 12,132 *PIPEDA* inquiries, down from 2003, when we received 13,422. The decline may be attributable to greater understanding of *PIPEDA* among the organizations that are subject to it; in 2003, many organizations were searching for guidance as they anticipated the full implementation of *PIPEDA* on January 1, 2004.

In the course of the year, staff shortages in the Inquiries Unit coupled with the ongoing heavy volume of work have presented challenges. As a result, it was necessary

to reassess the way we respond to public inquiries. We no longer accept or respond to inquiries or complaints by e-mail. We introduced an automated telephone system to answer the public's most frequently asked questions such as those about identity theft, telemarketing and, of course, the social insurance number. And we continue adding information to our Web site to answer the most frequently asked questions. We also temporarily assigned some investigators to help the unit. Lastly, we now invite individuals to telephone during office hours since we can often determine a caller's needs faster and better in person than in a series of e-mails and letters.

INQUIRIES STATISTICS

January 1 to December 31, 2004

The following table represents the total number of *PIPEDA* inquiries responded by the Inquiries Unit.

Telephone inquiries	8,861
Written inquiries (letter, email or fax)	3,271
Total number of inquiries received	12,132

Inquiries Response Times

On average, written inquiries (one quarter of the workload of the Unit) were responded to within three months. Nearly 3/4 of our inquires were received by telephone. The majority of these were responded to immediately; the remainder, which may have required research, were responded to within one to two weeks.

Providing written responses to inquiries is very time consuming and labour intensive. Over the year, the Inquiries Unit accrued a backlog of inquiries which exacerbated the average monthly response times. As we implement new measures, we will monitor the situation to determine whether these changes have resulted in efficiency gains.

Select Cases under PIPEDA

The following cases illustrate the breadth and variety of the cases investigated by our Office. We also posted 29 summaries of findings for 2004 on our Web site.

Medical information divulged through indiscreet choice of words

Even with the best of intentions, and even in such seemingly harmless activities as arranging for a taxi, health professionals must watch what they say to company managers about employees' health situations.

The facts

After completing a substance abuse program, a complainant signed a "last chance" contract as a condition of continued employment with a national transportation company. This contract required him to submit to regular monitoring, as well as random drug and alcohol testing, by the company's health service provider. The complainant was very concerned about confidentiality and for the most part had managed to keep his situation from fellow employees and supervisors.

One day while he was at home on active furlough, he received a call from a nurse, who told him he had to be at the clinic within four hours to give a urine sample. When he told the nurse he had no way of getting there, she said she would call the company and arrange for a taxi. The complainant soon got a call from his supervisor, who told him a taxi would take him "to the lab". The supervisor then asked him whether he was "under contract" – meaning a last-chance contract.

From the supervisor's words, the complainant assumed that the nurse had revealed too much information about him. Angered by what he believed to be a breach of his confidentiality, he later confronted both the nurse and the supervisor in abusive language that the company deemed to be grounds for disciplinary action. An investigation ensued, and the complainant was eventually dismissed for conduct unbecoming an employee (he has since been reinstated).

The supervisor told our Office that he had assumed the complainant's involvement in the substance abuse monitoring program from the nurse's use of the words "test" and "clinic" in his telephone conversation with her. The nurse, on the other hand, told us that she had used the word "appointment", not "test". She claimed to have given the supervisor only the minimum information necessary to make it clear that a taxi was needed and that there was a reasonable basis for the company to pay for it.

At one point, the company's regional superintendent had asked the nurse to document her version of the events relating to the complainant's alleged misconduct. She did so in an e-mail, which was sent to the regional superintendent and later forwarded to two other senior managers. In the e-mail, the nurse stated that the complainant had been required to undergo a "medical test … to assure his continuing fitness for duty" and that he had had to take the test within four hours after her phone call to him. Believing that this information implied his participation in the program, the complainant objected that it had been conveyed to the parties in question.

The complainant's allegation to our Office was that the nurse had inappropriately divulged his personal information to his supervisor in a telephone conversation and to other senior managers in an e-mail message.

Our findings

With respect to the telephone conversation, though it seemed appropriate that the nurse would have had to provide the supervisor with a reason to justify the taxi request, our investigation could not establish what exactly she had said to the supervisor. Whatever wording she used, it either caused the supervisor to conclude, or confirmed his suspicion, that the complainant was in the substance abuse monitoring program.

Similarly with respect to the e-mail, we did not dispute the need to inform senior managers of the complainant's alleged misconduct, but the problem was the information's content. Since the nurse's purpose had been to document the complainant's behaviour, stating that he had been required to go for a medical test within four hours was superfluous. The words "medical appointment" would have been sufficient to explain the need for a taxi.

The company was therefore found to have inappropriately used the complainant's personal information in contravention of Principle 4.3 of the Act. The complaint was well-founded.

Professor objects to getting spammed at the office

Is a person's business e-mail address fair game for marketers?

The facts

At his university office, a complainant received an unsolicited commercial e-mail promoting season's tickets for a professional team's games. The sales agent in question admitted to having obtained the e-mail address from the university's Web site, and he

agreed not to send the complainant further e-mails without his consent. Two weeks later, however, the complainant received a second e-mail solicitation from the same organization, but a different sales agent.

The complainant's allegation to our Office was that the organization had collected and used his personal information without his consent.

The organization did not dispute that it had sent the complainant a solicitation at his office e-mail address on two occasions. The two sales representatives in question were each responsible for a different solicitation "program" – one the "university program", and the other the "lawyer program". The agent responsible for the lawyer program had generated his contact list from the Web site of a law firm with which the complainant was associated. There was no cross-referencing system in place to flag the complainant's previous request that his name be deleted from the organization's marketing lists.

In response to the complaint, the organization removed the complainant's name from all its marketing lists and instituted cross-selling controls to ensure similar treatment of any future objection. The organization has also engaged a new ticketing and sales firm that is more knowledgeable about the requirements of *PIPEDA*.

The view of the university in question is that the e-mail addresses of its staff are business information. The university generally requires its faculty members to agree to have their business e-mail addresses published, in accordance with its business model and its expectation that employees be easily accessible. However, the university also expects a business or organization to obtain permission before contacting faculty for purposes unrelated to promoting the university's interests.

Section 2 of the Act specifically excludes the name, title, or business address or phone number of an employee of an organization from the definition of personal information, but makes no mention of an employee's business e-mail address. Sections 7(1)(d) and 7(2)(c.1) stipulate that an organization may collect and use personal information without the individual's knowledge and consent if the information is publicly available and specified in the regulations.

The regulations applying to these sections state that publicly available information includes an individual's name, title, address, and telephone number appearing in a professional or business directory, listing, or notice that is available to the public, where the collection, use, and disclosure of the personal information relate directly to the purpose for which the information appears.

Our findings

We determined first that, since section 2 does not specify a business e-mail address as being among the excluded types of information, it must therefore be deemed personal information for purposes of the Act.

The question then to be considered was whether the sports organization could rely on the exceptions to consent set out in sections 7(1)(d) and 7(2)(c.1).

The university had listed faculty e-mail addresses on its Web site with the expectation that businesses, organizations, and individuals might contact faculty members to further the university's interests. The sale of season's tickets to a sporting event, however, was not related to that purpose. The same reasoning applied to the Web site of the firm with which the complainant was associated. Moreover, even after the complainant's initial objection, the organization had collected his e-mail address from that other source and used it again for marketing purposes against his explicit instructions.

In sum, we determined that, since the purposes for which the organization had collected and used the complainant's personal information was entirely unrelated to the reason for which the information had been published, the organization could not rely on the exceptions to consent. The organization had thus collected and used the complainant's personal information without his consent, in contravention of Principle 4.3 of the Act. The complaint was well-founded.

Video surveillance as a last resort

Our Office considers video surveillance an extremely privacy-invasive form of technology. The medium's very nature entails the collection of a great deal of personal information, much of which may relate to innocent third parties, may be extraneous, or may lead to judgments about the subject that have nothing to do with the original purpose for collecting the information.

Only as a last resort should companies use video surveillance for investigative purposes – especially in investigating employees away from the workplace.

The facts

Over the course of his employment with a company, a complainant had reported a number of work-related injuries and had eventually requested workplace accommodation for physical limitations. For almost two years, the company attempted to satisfy his accommodation requests, but to no avail. The complainant

grew increasingly dissatisfied with the company's efforts, unwilling to perform his work duties, and resistant to the company's repeated requests for up-to-date medical information.

In view of the complainant's behaviour and lack of cooperation in providing accurate information about his ability to perform certain job-related tasks, the company became increasingly suspicious about the extent of his physical limitations. It eventually requested that he undergo an independent medical assessment, which he initially refused but in the end accepted. The independent assessors concluded that, although the complainant did have physical limitations, there also appeared to be many "non-physical barriers" to his returning to work. The assessors also noted that further functional testing would be unlikely to provide an accurate assessment of the complainant's true functional abilities.

Two months later, while the complainant was on leave, the company hired a private investigator to conduct surveillance on him with a view to determining whether he was being truthful about his physical limitations. After two weeks, the investigator provided the company with a report and eight hours of videotape showing the complainant performing tasks of which he had claimed to be incapable. On this evidence that he had misrepresented the state of his health, the company dismissed him.

The complainant's allegation to our Office was that his employer had collected his personal information by way of video surveillance without his knowledge and consent and had used that information to terminate his employment.

To justify its actions in this case, the company relied on sections 7(1)(b) and 7(2)(d) of the Act. These provisions permit an organization to collect and use personal information without the individual's knowledge and consent if seeking knowledge and consent would compromise the availability or the accuracy of the information and if the collection and use are reasonable for purposes of investigating a breach of an agreement or a contravention of a law.

The company maintained that its decision to conduct video surveillance was the result of consultation among a small team of legal, medical, and industrial-relations professionals, who had determined that such a measure was necessary as a last resort in the circumstances. The company had provided information about the complainant's physical limitations and had instructed the investigator to monitor the complainant's activities over a significant-enough period to provide a complete picture of his capability and establish sound, factual, and irrefutable evidence of his fraudulent behaviour. The

company acknowledged, however, that it had no formal policy or procedures in place to guide managers in such situations.

Our findings

There was no question that the company had collected the complainant's personal information through video surveillance without his knowledge and consent. The issue was whether section 7(1)(b) could apply. However, this exception could not be read in isolation. Among the factors to consider were whether the organization had substantial evidence to support the suspicion that the relationship of trust had been broken, could show that it had exhausted all other means of obtaining the information that it required in less privacy-invasive ways, and had limited the collection to the purposes as far as possible.

On the evidence, our Office was satisfied that the company's purpose of determining whether the complainant was violating his employment contract by misrepresenting the state of his health was based on substantial evidence. Furthermore, the company had made numerous less privacy-invasive attempts to gather the information it had required, but these had mostly met with resistance from the complainant and in the end had not dispelled the organization's concerns. It had also, in taking the step of hiring the private investigator, outlined what information it was seeking and focused the collection of personal information as far as possible.

In sum, the company had had reasonable cause to believe that the complainant was violating his employment contract, and had clearly had difficulty in obtaining accurate information from him with his knowledge and consent. We accepted the company's reliance on sections 7(1)(b) and 7(2)(d) to collect and use the complainant's personal information without his knowledge and consent. The complaint was not well-founded.

Notwithstanding the findings, we recommended that the company formalize the measures it had taken by developing privacy-conscious policy and practices regarding the use of video surveillance. Such policy should consider the following:

- Video surveillance is a last resort and should only be contemplated if all other avenues of collecting personal information have been exhausted.
- The decision to undertake video surveillance should occur at a very senior level of the organization.

- The private investigator should be instructed to collect personal information in accordance with the Act, and should be especially mindful of Principle 4.4 (Limiting Collection).

The company implemented this recommendation.

Cameras in the workplace: The importance of stating purposes

Employees naturally tend to resent the presence of video cameras on the job. However, by being forthcoming about purposes, the employer can often alleviate employees' fears about loss of privacy.

The facts

Implementing a recommendation from a security review, a broadcasting company installed three surveillance cameras at its workplace – one outside and two inside the building. The outside camera captured the parking lot and building entrance, and the inside cameras aimed at the interior entrance and a central corridor.

Several employees of the company lodged complaints with our Office, alleging that the company was using the cameras to collect their personal information, particularly about their behaviour and work performance.

The employer maintained that a memorandum had been posted to inform employees of the camera installation and its true purpose, which was to ensure the safety and well-being of employees by tracking non-employee traffic in and out of the building. The employees, however, were not aware of the memorandum.

During our investigation, the company agreed to inform employees of the purposes for which information collected by the cameras would be used. It also agreed to develop a policy document on the use of surveillance cameras, including the objectives, installation sites, employees authorized to operate the system, time of surveillance and recording, and applicable equity principles.

The company subsequently fulfilled these commitments.

Our findings

The company had not made reasonable efforts to inform its employees and had thereby violated Principle 4.3.2 of the Act.

However, it was also established that the use of such a surveillance system constituted an appropriate means of protecting employees. Since the cameras were not to be used to collect employees' personal information and were not installed in places where there was a reasonable possibility of privacy invasion, it did not seem appropriate that the employer be required to obtain employees' consent for their use. If the cameras inadvertently collected employees' personal information, the employer would not be able to use such information without the employees' consent except in the circumstances set out in the sections 7(2)(a) and (b) of the Act (these provisions apply to legal investigations and emergencies, respectively).

Because of the company's commitments to inform employees and develop a policy document, the complaints were deemed resolved.

Cameras in the workplace: The importance of keeping to reasonable purposes

In this case, our Office supported the use of video cameras to enhance the safety of the workplace, but warned that the unrestrained use of such cameras to monitor employee productivity or to manage the employer/employee relationship would have a chilling effect on employee morale. Employers using cameras for legitimate operational purposes must make every effort to keep to those purposes, and must exercise great care and deliberation in resorting to video surveillance for any exceptional purposes allowable under the Act.

The facts

A railway company uses cameras to monitor train movements and to inform crew members of train locations. The company installed the cameras after a risk analysis, and both the company and the employee union agree that the cameras are needed for operational purposes.

One day the manager responsible for the cameras spotted two on-duty employees getting into a car. He went into his office and used the cameras' zoom capacity to determine that the employees were driving off site. The company subsequently imposed a disciplinary penalty against them for leaving work without permission. One of the two employees grieved the discipline, and the matter was referred to arbitration. Both employees complained to our Office that the company had used video cameras, ordinarily used for operational purposes, to determine that they were leaving company property during regular working hours.

The company argued initially that the Commissioner should exercise her discretion not to issue a report of findings, since the matter was also being dealt with through arbitration. Referring to a recent decision of the Federal Court to the effect that labour tribunals have exclusive jurisdiction over disputes arising out of collective agreements, the company later contended that the Commissioner's Office did not have jurisdiction with respect to such complaints.

The company also argued that the Act allows organizations to collect, use, and disclose information for purposes that a reasonable person would consider appropriate in the circumstances. It denied actually having *collected* the complainants' personal information, since the camera did not record. It described the camera as a "visual aid" that had allowed the manager to follow up on a concern he had already identified without the use of a camera. It maintained that the complainants had had no reasonable expectation of privacy, given that the rail yard was constantly busy with pedestrian traffic. It contended that, given the complainants' suspicious behaviour on the day in question, a reasonable person would have considered it appropriate to use the cameras as a visual aid to determine the direction of their vehicle.

Finally, the company referred to section 7(1)(b) and argued that, should the Commissioner conclude that the camera had indeed collected the complainants' personal information, their consent to the collection and use of the information had not been required since the company was investigating a breach of an employment condition at the time.

Our findings

The Office observed first that the Federal Court decision to which the company had referred was under appeal. We therefore concluded that we had jurisdiction to investigate the complaints.

The Office also declined to exercise its discretion not to deal with the complaints. We referred to the lead role of the Office in determining whether organizations are adhering to the *Act* and in educating both organizations and the public about the Act. We noted that the complaints raised issues that could set a precedent.

We concluded as follows:

- The *Act* does not restrict the definition of personal information to information that is recorded only, but rather clearly defines personal information as including any information about an identifiable individual. The cameras in question do

collect the personal information of employees, and were used to collect the complainants' personal information – that is, the fact that they were leaving the yard during work hours.

- There is no question that the customary use of the cameras to enhance the safety of the workplace is appropriate in the circumstances, as contemplated by section 5(3) of the Act. The cameras were installed after a risk analysis, and both union and management support their use.

- Regarding the appropriateness of using the cameras in the circumstances surrounding the complaints, the company did not present any evidence that unauthorized absences from the workplace were a persistent problem with the complainants or with other employees. The company did not present any evidence of other, less intrusive efforts it had taken to manage unauthorized absences. A reasonable person would not consider it appropriate to use the cameras to manage a workplace performance issue. In the circumstances, the use was contrary to section 5(3) of the Act.

- Where an employer suspects that the relationship of trust has been broken, it can initiate the collection of information to investigate that breach without the consent of the individual. However, the only evidence the company presented to suggest a possible breach in the relationship of trust was that the employees in question had been seen entering a private vehicle. The company admitted that the employees might have been leaving the site with the permission of their immediate supervisor and that the manager who used the camera had only determined *after the fact* that the employees left the work site without permission. Cameras being highly privacy-intrusive, a decision to use them, even in the circumstances set out in section 7(1)(b), must be taken with great care and deliberation. Where there is a less intrusive method of achieving the same result, that method should be the first choice.

We concluded that the complaints were well-founded.

Bank customers required to declare citizenship

This complaint, specifically about a bank's collection and use of personal information, also raised a general concern about whether a bank was putting the requirements of foreign legislation ahead of the privacy interests of its Canadian customers.

The facts

Several account holders complained when their bank sent them a form letter asking them to declare whether or not they were U.S. citizens.

In 2001, the bank had become an indirect subsidiary of a U.S.-based holding company. For purposes of U.S. income tax law, the bank was therefore a "controlled foreign corporation" and was required to comply with applicable U.S. Internal Revenue Service (IRS) regulations on information reporting and tax withholding. Notably, it had to report interest income earned on personal deposit accounts by persons either known to be U.S. citizens or presumed to be U.S. citizens because they had not declared themselves non-U.S. citizens.

The bank mailed an explanatory letter and an account declaration form to all of its personal deposit account holders. The letter indicated that, if an account holder did not declare that he or she was not a U.S. citizen, his or her name and address, as well as the amount of interest income earned, would be disclosed to the IRS. The letter also outlined the purpose for collecting such information and how it would be used.

The complainants alleged that the bank was requiring them to consent to the collection and use of more personal information than was needed to provide account services.

Our findings

As far as the substance of the complaint was concerned – that is, the collection and use of personal information – our Office was of the view that the bank was *not* putting foreign legislation ahead of Canadian customers' privacy interests.

As a controlled foreign corporation, the bank was required to comply with applicable IRS regulations. Notably, it had to report the interest income earned by U.S citizens, but did not have to report that earned by non-U.S. citizens. To ensure provision of accurate information to the IRS and to protect the personal information of non-U.S citizens, the bank had sent the account declaration form to its account holders, asking them to declare whether they were U.S. citizens or non-U.S. citizens. This was a

reasonable request, for purposes that a reasonable person would consider appropriate in the circumstances, as contemplated by section 5(3) of the Act.

Furthermore, since the bank had identified its purposes and limited the collection of personal information to those purposes, it was also in compliance with Principles 4.2 and 4.4 of the Act.

On this account, the complaint was not well-founded.

Quebec company's information-sharing notice not clear enough

If an organization intends to share customers' names and addresses with third parties for marketing purposes, it must let the customers know, but not just in any old way. Principle 4.3.2 of the Act puts an onus on organizations to make a "reasonable effort" at both bringing purposes to the attention of customers and presenting them in a way the customers can understand.

The company in this case did make an effort, but the question for our Office was, "How reasonable?" The case also has an interesting jurisdictional aspect relating to a transitional provision in *PIPEDA*.

The facts

Some months after purchasing beauty products by telephone from a company in Quebec, a complainant had requested in writing that the company remove her name from its mailing list. Several weeks later, in October 2002, her name was still on a list that the company had recently sent to an Ontario consultant hired to trade and rent its customer lists to other organizations.

The complainant's allegation to our Office was that the company had sold her name and address to third parties in Ontario without her consent. She also raised concerns about the company's procedure for allowing customers to opt-out of third-party marketing.

The company explained that the continued appearance of the complainant's name on the mailing list was the result of normal administrative delay in processing the opt-out request. The company also pointed out that its practice of sharing lists of customers' names and addresses with other businesses, as well as its procedure for having one's name removed from the lists, was set out in a document made available to customers in mail-outs and catalogues.

Our investigation confirmed the existence of this document. However, the dominant title on the document was "Money Back Guarantee", and the notifications in question appeared under the headings "Help Us Conserve Natural Resources" and "Beauty Care is Personal".

The company removed the complainant's name from its mailing lists. As a result of our Office's intervention, the company changed its promotional materials to make them more understandable. Customers can now simply check a box on the purchase order to prevent the sharing of their information. The company also set up a privacy committee, which has adopted a policy on the protection of customers' personal information and is developing a similar policy for all employees.

The complainant expressed satisfaction with the company's removal of her name from its mailing lists and with the changes it made to its promotional materials.

Our findings

Under section 30 of *PIPEDA*, a transitional provision that remained in force for the first three years, the *Act* applied until 2004 to personal information that an organization disclosed outside the province for consideration. Even though the company in question resides in Quebec, our Office agreed to investigate the complaint under the *Act* because the complainant alleged that the company had disclosed her information outside that province for consideration in 2002 – that is, while section 30 was still in effect.

At the time of the complaint, the company's promotional materials contained a notice stating that customers' names and addresses were shared with third parties and laying out a procedure for customers to remove themselves from the lists. However, the notice and the removal procedure lacked clarity. The information was hidden away under headings that were not representative of the contents. The notice did not constitute a reasonable effort by the company to ensure that individuals were clearly informed about the secondary disclosure purposes for which the personal information was collected. Therefore, the company was in contravention of Principle 4.3.2 of the Act, and the complainant's consent was not meaningful.

However, since the complainant was satisfied with the outcome of the investigation, our Office concluded that the complaint was resolved.

Satellite television company alleged to have monitored customers' viewing habits

When told to keep his satellite system continuously plugged in, the customer assumed the worst of the company. But was its intention really to invade his privacy?

The facts

A complainant believed that his satellite television provider was keeping track of what programs he watched. He was convinced that, in requiring customers to keep their telephone lines continuously plugged into receiver boxes, the company's sole purpose was to monitor their viewing habits.

His allegation to our Office was that the company was indiscriminately collecting and using his personal information that it gathered through his telephone connection.

The company confirmed that it does require its satellite customers to keep their telephone lines continuously plugged into the receiver boxes it supplies, but for purposes of billing for pay-per-view and preventing piracy, not monitoring viewing habits. The company explained, and our Office confirmed, that it was not possible with its current technology to monitor any programming other than pay-per-view, since the satellite transmission is one-way only and the receiver boxes are not capable of recording other programs. The only information the company collects is about the packages a customer has purchased and transactions that customers initiate electronically through the pay-per-view ordering system, and it collects such information only for billing purposes.

As for preventing piracy, our Office examined the technical aspects and was satisfied that continuous connection with a live telephone line is effective for this purpose. Despite the company's explanation, the complainant continued to believe it was collecting more information than necessary to prevent piracy, but he could not provide any evidence to support his belief.

Our findings

The company's purposes of billing for pay-per-view and preventing piracy were ones that a reasonable person would find appropriate in the circumstances.

There was no evidence that the company was collecting information on subscribers' viewing habits from the telephone connection. Information on program packages and other billing information was collected at the time of purchase, not through a telephone line.

Although the company did collect pay-per-view information through the connection, it did so to meet one of its stated purposes – billing the customer. The continuous connection was also effective in fulfilling the company's other purpose – preventing piracy.

In sum, the company was collecting and using customers' personal information to fulfil reasonable purposes and was not collecting or using excessive information for those purposes or any others. The company had complied with Principles 4.4 and 4.5 and section 5(3) of the Act. The complaint was not well-founded.

Bank discloses client's mortgage history to her ex-husband's lawyer

"He-said, she-said" cases can be devilishly difficult to adjudicate. In this one, fortunately, a paper trail largely supported what "she said".

If there's a lesson for bank staff in this situation, it's that, when dealing with lawyers, you had better make sure at the outset whose side they're on.

The facts

While attending a court hearing regarding her support arrears action, the complainant had received copies of three documents entered into evidence by her ex-husband's side: the deed for her home, a land registry office listing of mortgages registered against her home, and a mortgage transaction history.

The complainant believed that the manager of financial services at her bank had given these documents, as well as other information about her financial affairs, to her ex-husband's lawyer on a certain date. She also held that the manager had admitted as much to her and had asked her not to tell the court about his inappropriate disclosures.

Her allegation to our Office was that the bank had disclosed her personal financial information to her ex-husband's lawyer.

With respect to the deed and the mortgage listing, our investigation determined that the bank manager would not have had access to these documents on the date in question. Moreover, such documents are publicly available at the land registry office, and evidence indicated that the lawyer had already obtained these two documents from that office when he visited the bank manager.

However, with respect to the mortgage transaction history, documentary evidence established that the lawyer had prepared and sent a summons to the bank manager,

had then written to the manager to make an appointment for the date in question in order to review the documentation demanded on the summons, and had, on the day before the date in question, acknowledged receipt of a reply from the manager. Furthermore, the copy of the complainant's mortgage transaction history that the lawyer submitted to the court had been printed from the bank manager's computer and was dated the same day as his reply to the lawyer.

The manager did not admit to printing the document, providing it to the lawyer, or asking the complainant not to reveal his disclosures. Nevertheless, he did admit that, at first contact, he had mistakenly assumed that the lawyer was acting on the complainant's behalf.

Conceding that the complainant's mortgage transaction history had been disclosed to the complainant, the bank issued her an apology.

Our findings

The deed of land and the mortgages registered against the complainant's home were determined to be publicly available information obtainable through the land registry office. Such information could be disclosed without knowledge and consent, pursuant to section 7(3)(h.1) of the Act. In any case, it appeared that the lawyer had already gathered this information before approaching the bank.

The mortgage transaction history, however, was determined to have been printed from the bank manager's computer on the same date he had written to the lawyer. Our Office believed, and the bank agreed, that the document had been disclosed without the complainant's consent. The complaint was well-founded.

Select Settled Cases under *PIPEDA*

In January 2004, the Office of the Privacy Commissioner introduced a new category of complaint disposition, "Settled during the course of the investigation". A settled case is one in which, during the actual complaint investigation, the Office has helped negotiate a solution satisfactory to all parties, including the Office itself. Of the 379 cases concluded in 2004, 152 (or 40 per cent) fell under the "settled" category.

The following are summaries of several representative settled cases.

Laptop lapse by computer store

When a computer store did not fix a complainant's laptop within a certain time limit, it provided her a new one. Some time later, she was surprised to get a call from a complete stranger, telling her he had just bought a laptop containing her personal information.

As it turned out, the store had repaired the complainant's original computer, and an employee had put it up for resale without examining its contents. The store was able to retrieve the laptop and return it to the complainant. The company also significantly improved its safeguarding policy and practices. Notably, employees now have to not only ensure, but also document, that personal information is completely erased from the hard drives of all computers returned to any of the company's stores across Canada. The company also agreed to implement similar safeguarding procedures for other electronic devices that it sells.

Phone and e-mail procedures: One security concern leads to another

Whenever customers pay their bills through the telecommunications company's interactive voice response system, the system reads back the credit card number and expiry date that the customer entered via the telephone keypad. A complainant was concerned that anyone intercepting a cell phone call could obtain these numbers. But when he e-mailed to express this concern, the company's e-mail reply repeated the account number and personal identification number that he had entered to gain access to the secure account information system. The complainant was now concerned that this sensitive personal information, too, could be available to anyone else who might gain access to the e-mail.

The company reviewed its practices and agreed that it was not necessary to automatically reproduce in e-mail responses the personal data required for accessing the secure site. It has now ceased to include message threads in its e-mail responses to customers. As for the original concern, however, the company pointed out to the complainant that several payment options were available to customers and that, even if credit card numbers were no longer to be read back, customers who chose to pay bills by cell phone would still risk interception of the numbers as they were keyed in.

Insurance company fails to heed client's warning

On two distinct occasions, a complainant had warned his insurance company that unauthorized persons might try to obtain information about life insurance policies he held on his nephews. Despite these warnings, and despite the company's authentication and flagging procedures in place at the time, information was later disclosed to an unauthorized party against the complainant's express wish.

The complainant and the company reached a settlement. As a result of the complaint, the company has greatly improved its authentication and flagging policy and procedures and has incorporated the new policy in its training for customer service representatives.

Transportation company eliminates excessive database information

An employee of a national transportation company complained about lack of security of personal information in an automated crew management system. Specifically, he was concerned that unauthorized personnel, especially union representatives, could gain access to such employee information as date of birth, social insurance number (SIN), health information, wage rates, and vacation eligibility.

In fact, it was not possible for union representatives to gain access to some of the information of concern to the complainant. Moreover, at the time of the complaint, the company had already identified date of birth and the SIN as privacy concerns and was in the process of adjusting its crew management system accordingly. In the end, the company agreed also to remove employees' health information from the system.

Personal information circulates on hundred-dollar bill

When a complainant offered a $100 bill for a gasoline purchase, the service station attendant asked for identification. According to the complainant, the attendant then wrote his name and driver's licence number on the bill itself, explaining the practice as "company policy" due to the high incidence of counterfeit bills. On reflection after the incident, the complainant worried that his personal information would thus be available to anyone handling the bill for as long as it remained in circulation.

The company does make a policy of having station staff temporarily record identification for customers tendering $100 bills, but stipulates that the recording be done on separate tracking sheets, not on the bills themselves. Although the attendant

knew the correct procedures and did not admit to having written on the bill, the company took responsibility in the matter, apologized to the complainant, and reached a settlement with him. The company also reminded all its service station employees of the proper procedures for handling personal information.

Pharmacy makes consent procedure more customer-friendly

A complainant objected that his pharmacy was requiring him to sign a consent form before giving him his medication. It seemed to him that the form authorized overly broad disclosure practices, and he was concerned that his personal information might be disclosed for marketing purposes. He also worried that he would not be able to obtain the medications he needed if he refused to sign.

In fact, the pharmacy chain does not disclose customers' personal information to other organizations for marketing purposes. Nevertheless, in response to this and several other complaints about its consent form, the company decided to change the language of the form, making it simpler and easier for customers to understand. The company also implemented a new policy and practice whereby clients who are uncomfortable signing a consent form can provide oral consent to the company's privacy practices, as explained to them by the pharmacist.

Another pharmacy clarifies consent policy

A customer alleged that, even after he had withdrawn his consent to collection, use and disclosure practices, his pharmacy had disclosed personal information to his doctor. He also complained that the pharmacy refused to fill his prescriptions because of his consent withdrawal.

The pharmacy's only record of the complainant's withdrawal of consent was dated some time after the alleged disclosure. After recording the withdrawal, the pharmacy had indeed refused to fill the complainant's prescriptions, but had explained to him at the time that it was company practice not to fill prescriptions for persons who had revoked consent to the collection, use, or disclosure of personal information within the patient's circle of care. The company's privacy literature, however, explained such practice only in general ways, indicating that withdrawal of consent could adversely affect "service". The company agreed to amend its privacy policy to specify that prescriptions could not be filled unless consent was provided.

Insurance company welcomes complainant's suggestions about consent form

An applicant for life insurance complained that the insurance company was requiring her to consent to overly broad collection, use, and disclosure practices.

Our Office facilitated a teleconference with the complainant and the company. The company explained to her its actual practices, which were consistent with the Act. Though the complainant was satisfied with this explanation, the company acknowledged that she had raised a number of important issues about the precision and clarity of its consent language – issues it was taking into account in a current review. The company agreed to send the complainant a copy of its revised form and invited her to make further comments, to be considered in subsequent reviews.

An unappreciated birthday announcement

An employee of a foreign airline's Canadian office complained when a secretary e-mailed his date of birth to fellow employees, despite his previously expressed objection to the local tradition of announcing birthdays. He also alleged that the airline had disclosed his home address and telephone number on lists provided to employees having no need to know such information, and that these lists were not properly safeguarded.

At the suggestion of our Office, airline officials met with the complainant to address the issues he had raised. In the end, the airline resolved the issues to the complainant's satisfaction – notably, by ceasing the practice of announcing birthdays and by taking measures to safeguard and limit access to documents holding employees' personal information. The airline also held privacy briefing sessions with management and administrative staff and posted a privacy notice on an internal bulletin board accessible to all employees.

Department store neglects to identify itself as source of mail-out

Two individuals complained after receiving a mail solicitation ostensibly from a credit monitoring company. Though appearing to have been sent from the company itself, the solicitation indicated an association with a major department store chain with which both complainants held accounts. They both assumed that the chain had given their personal information to the credit monitoring company without their consent. In one case, the complainant had expressly withdrawn consent for the chain to use his personal information for any purpose other than directly conducting business with him.

In fact, the chain had not given personal information to the company. Rather, it had itself had the mail-out notice prepared and sent out, but under the other company's name. The chain's published policy is to rely on opt-out consent for disclosures of customer information to affiliated companies of its own "brand", but it does not disclose to non-affiliated third parties such as the credit monitoring company. In the case of the complainant who had previously withdrawn consent, the chain explained the mail-out as the result of a normal administrative delay in processing his opt-out request.

The chain agreed, however, that it had done a poor job in the marketing campaign and should have clearly indicated that it was acting on the other company's behalf. It also apologized to the complainants, agreed to revise its account application policy to allow new customers to opt-out at the time of enrolment, and undertook a review of its suppression mechanisms to ensure consistency of the opt-out process across all its companies.

Non-consensual disclosures to a union

Several employees complained that a transportation company had forwarded a list of participants in its voluntary separation program to the employees' union without their knowledge and consent. The list included the employees' SINs.

Admitting its mistake, the company changed the application form for severance packages to exclude the requirement for the SIN and to include a statement asking applicants to consent to the release of their personal information to the union.

Two cases of envelope mix-ups

In one case, a complainant had received a student loan notice from her bank – about someone else's loan, not hers. She worried that this other person might be in possession of the same personal information about her as she had received about him – specifically, name, address, SIN, loan number, and loan amount. The mix-up had been the result of simple human error in filling envelopes. No other persons in the complainant's mailing group had received a wrong notice, and the person whose information she had received had not received hers, since he had moved and not left a forwarding address. The bank reached a settlement with the complainant and advised its student centre staff to exercise greater diligence in mailing material to customers.

In the other case, a complainant had received another person's airline ticket in the mail, and that other person had received that of the complainant. The tickets contained personal information in the form of travel itinerary, home address, and telephone number. This mix-up was also the result of human error, in that an airline employee had inadvertently reversed the tickets and envelopes for two phone ticket purchases. The airline apologized to the complainant and reached a settlement with him. It has also reminded its employee to exercise due diligence and care in sending material out to customers.

SINs on display: An overly revealing envelope window

A pension fund administrator complained that transfer documents he regularly received from a certain bank displayed clients' SINs in the window of the envelopes. Readily acknowledging the problem, the bank instituted a new process whereby both the SIN and the account number were moved from the address portion of the document to an area not visible through the envelope window.

Collection agency corrects inaccurate information

A complainant had been having difficulty securing credit because of inaccurate information held by a collection agency. He had paid off a debt several years earlier, but the agency had not reported the payment to the credit bureaus. After several unsuccessful attempts through his lawyer to have the information corrected, the complainant approached our Office.

The collection agency had no record of the lawyer's letters. However, after receiving a notice from our Office and yet another letter from the lawyer, the agency looked into the complainant's file, confirmed the debt payoff, and notified the credit bureaus, which amended the complainant's credit files accordingly.

Car dealership refuses credit on erroneous information

A complainant knew her credit rating was good. When a car dealership turned down the credit application she had cosigned with her son, she wrote the company to ask for the information on which the credit decision had been based. Two months later, she wrote again. Still having received no response after three months, she filed her complaint.

As it turned out, the decision had been based not on her own credit rating, but on her son's. The company had not responded to her access requests because it was unsure

how to do so without disclosing the son's personal information. At our suggestion, the complainant wrote the company another letter, signed by both her and her son and stating that they consented to the disclosure of information about themselves to each other. The company finally responded, indicating that the credit application had been declined because of a bankruptcy entry on the son's credit report. The complainant wrote the company again to advise that the report was in error – the son had not in fact declared bankruptcy, but rather had made a proposal with his creditors and had satisfied its terms more than a year earlier. The company replied that it would use a current credit report for any future application. The complainant was satisfied just to finally have a response from the company.

Meanwhile, the son had managed to lease a car from another dealership under the same brand. In the complainant's words, someone at that dealership "clearly *did* know how to read the credit information."

Companies Getting Their Act Together

A lending institution

A woman complained that a lending institution had disclosed information about her delinquent account to her uncle without her consent.

The complaint had merit, and the institution adjusted the complainant's outstanding account and agreed to send her a letter of apology. During the investigation, our Office noted that the organization had no privacy policies or practices in place. At our urging, it struck a privacy committee, instituted privacy training for employees, and reminded staff to limit the amount of information disclosed in recovering debts.

A trucking company

A former employee alleged that a small, family-owned interprovincial trucking company had disclosed personal information to a creditor without his consent.

There was no evidence to support the allegation, and it came to light that the complainant himself had provided some of the information to the creditor. Nevertheless, our investigation had the effect of educating the company about its obligations under the Act. The company subsequently implemented a written privacy policy, appointed a privacy officer, reviewed its practices regarding employee personal information, and took steps to train employees in proper information handling.

Incidents under *PIPEDA*

Over and above individual complaints, incident investigations are conducted into matters of improper collection, use or disclosure of personal information that come to the attention of our Office from various sources, including the media, and directly from organizations themselves. They often highlight a systemic issue, or an unrecognized privacy breach that needs to be fixed as soon as possible. Usually, victims are not identified and a formal written complaint has not been filed with the Office.

Last year, the Office completed six incident investigations. Three cases of interest are described below.

Disclosure of credit reports to fraudster

In March 2004, a credit reporting agency issued a statement that, as a result of a security breach, the credit reports of some 1400 consumers had been disclosed to criminals posing as legitimate credit grantors. The media picked up the story.

The agency's security staff discovered the breach and notified the RCMP, which launched an investigation. It appeared that a single individual committed the breach, and had not been caught as of May 2004.

The agency confirmed that 1398 consumers were affected – 1145 in British Columbia, 163 in Ontario, and 90 in Alberta.

The information disclosed in each credit report was the consumer's name, address, previous address (if available), date of birth, and payment history, as well as creditor names and account numbers, public record items, and collection activity. The agency confirmed that the disclosed information did not include social insurance numbers or bank account particulars.

By way of corrective action, the agency:

- Notified all affected individuals by registered mail;
- Encouraged them to call the agency and review the contents of their credit files;
- Placed an alert message reading "Lost or stolen identification" on their credit files so that creditors would be prompted to ask for additional proof of identity;
- On being contacted by an affected individual, requested that the other major credit reporting agency place a similar message on its credit file for that individual; and

- Offered the affected individuals a free one-year subscription to a credit monitoring service (most accepted this offer).

To address the security problem, the agency put certain fixes in place on its systems. These fixes appear to be effective, in that the same perpetrator attempted to access credit files in the same way a second time, but was blocked.

Since the incident, there have been a small number of fraud attempts involving the disclosed information, but in each case the alerts prevented the fraud.

Joint federal/provincial investigation of misdirected medical information

In July 2004, a newspaper article reported that a married couple had been receiving faxes from various sources containing other parties' personal health information. The couple alleged that they had so notified some of the sources in question, but had continued to receive more of the same.

The Office of the Information and Privacy Commissioner for Alberta originally investigated this incident. That Office determined that, though provincial privacy legislation applied to some of the information transmitted in the faxes, it also appeared to fall under federal jurisdiction under *PIPEDA*. The Office of the Privacy Commissioner of Canada therefore undertook its own investigation in concert with the Alberta office.

The couple in question manages an apartment building. The fax line they use in managing the property has a telephone number similar to that of a health care provider, but with two of the digits reversed. The couple received ten faxes misdialed to their number.

Our Office concerned itself with seven of the ten errant faxes (the other three fell under provincial jurisdiction). Two of the seven were found not to contain personal information. For the remaining five, the sources were determined to be three separate and distinct companies.

The first is a company that owns and operates medical laboratories. The fax it misdirected to the couple's number contained the personal information of an individual who had undergone medical testing by the company. The information included the person's name, age, height, smoking habits, and patient number, as well as a diagnosis and specific medical test results.

In its own internal investigation, this company was unable to determine which of its employees had keyed in the erroneous telephone number, but it did manage to narrow the possibilities down to five. All five employees were aware of the confidential nature of the medical records and the need to ensure against disclosure, and all five had signed a confidentiality oath at the time they were hired, but had not been required to renew the oath since then.

For regularly used fax numbers, this company has now equipped its computers with an electronic automated fax function which checks numbers entered into the system for accuracy before use. For numbers used one time or infrequently (i.e., not programmed into the automated system), the company has provided its employees with a set of instructions to ensure accuracy of transmission. At the Office's request, the company also undertook to revise its policies and procedures to ensure full compliance with the provincial *Health Information Act* and *PIPEDA*.

The second source of the errant faxes is a waste disposal company whose employees are required to have annual medical examinations. This company misdirected three faxes, one of which predated the full implementation of *PIPEDA*. The other two were completed health information forms about two employees who had just had the annual examination. However, it was not the company that had misdirected the faxes, but rather the employees themselves, each misdialing the number in the same way. For privacy reasons, it is the company's practice to have its employees send in their own health forms.

This company has now put the correct fax number on speed dial so that its employees may continue to send in their own health forms with much less risk of inadvertent disclosure. The company also has a privacy officer and acceptable privacy policies in place.

The third company involved is a medical consulting firm whose doctors review and assess new medical consultants' reports on patients. The single misdirected fax in this instance contained such a report that one of the company's doctors had reviewed. The doctor in question had not sent the fax himself, and the company was unable to determine who had. The faxed report contained the patient's name, age, and occupation, as well as a detailed medical history relating to an injury she had sustained in a motor vehicle accident. It also contained information about her children.

When the couple had called to notify this company of the errant fax, a company employee had instructed them to destroy it. In hindsight, the company realized that

this instruction was inappropriate, in that the employee had had no way of confirming that the document was destroyed or whether it was destroyed by a suitable method. The company has arranged to have errant faxes picked up by courier in future. It has also taken procedural measures to have all facsimile numbers verified before transmission and to have any future incidents reported to management.

At our Office's request, this company has informed the patient in question of the disclosure of her personal information, has appointed a privacy officer and has sent the Office copies of its revised fax transmission procedures and privacy policy.

The Office made the following recommendations to the first and third of the companies:

(1) That the companies implement and follow the Office's recommendations on the transmission of faxes, as set out in the fact sheet entitled "Faxing Personal Information";

(2) That the companies implement measures to ensure that faxes are recovered if reported as misdirected;

(3) That the companies notify individuals when their personal information has been inadvertently disclosed as a result of a misdirected fax; and

(4) That the companies have their employees sign confidentiality/privacy agreements, update such agreements yearly, and review company privacy policies.

Credit card receipts blowing in the wind

In August 2004, a newspaper reported that two women had observed credit card receipts blowing about in their neighbourhood and had traced the source to a local gas station, where old receipts had been placed in a dumpster.

The station owner admitted to having disposed of various receipts from 2002 in the dumpster, but claimed he had been unaware of the privacy implications of this action. He said that the receipts had been contained in boxes, placed in the middle of the dumpster, and covered by other garbage. He suspected that neighbourhood children had climbed into the dumpster and opened the boxes out of curiosity, thereby exposing the receipts to the elements.

He stated that, on being informed of the problem by a reporter on the day in question, he had taken immediate action to gather up the loose receipts, clear the dumpster of

those remaining, and have all the receipts shredded. Though he maintained that he and his employees had been able to find few loose receipts to gather, our investigation established that the two original women witnesses had previously gathered three bags and one boxful of the loose receipts in vicinity of the gas station.

The witnesses turned in the receipts they had gathered to our investigator. A sampling of 1,897 of these documents indicated that most were debit card receipts with no identifiable personal information, and many others were credit card receipts showing a past expiry date. However, a further 151 credit card receipts showed valid (unexpired) account numbers, 16 showed valid account numbers as well as handwritten licence plate numbers, three showed valid account numbers as well as handwritten driver's licence numbers, and one showed both a driver's licence number and a plate number.

The owner gave assurances that he was now aware of his responsibilities under the *Act* and had initiated policies to keep all receipts only for the required six months and then have them destroyed securely by means of shredding.

The owner leases the station from an energy company. In an interview, the company's district manager initially took the position that the company's privacy policy did not apply to its leased establishments. He later conceded, however, that leaseholders were generally expected to adhere to the company's policies and procedures and that the company did customarily provide training and information sessions for leaseholders. But neither he nor the station owner could recall any such information session about privacy policy. The district manager indicated that the company would provide privacy information sessions for leaseholders in the near future, and that he himself would review privacy policies in his monthly meetings with the leaseholders in his district.

Our Office made two recommendations:

(1) That the company ensure that privacy policies are in place at all of its leased locations and examine the option of putting requirement to that effect into its lease agreements; and

(2) That the privacy policies for the company's gas stations contain procedures for the proper retention, safeguarding, and disposal of all personal information collected.

Following Up on *PIPEDA* Case Investigations

In 2004, we introduced a formal procedure of systematic follow-ups to complaint investigations under *PIPEDA*. As a matter of course, the Investigations and Inquiries Branch monitors the progress of organizations in implementing both commitments they make during complaint investigations and recommendations that the Office issues to them in letters of findings. We ask organizations to report on their intentions and their progress in meeting these commitments and recommendations. We also ask them to provide documentary evidence of implementation.

The purpose of follow-up is two-fold. First, it reinforces and clarifies the Office's expectations that organizations take remedial measures in response to specific problems identified in complaint investigations. Second, it provides a reliable ongoing record of organizations' compliance with *PIPEDA*.

In late 2004 and early 2005, in a special exercise to establish a solid basis for such a record, our Investigation and Inquiries Branch applied the new follow-up procedure to past cases in which organizations' responses to recommendations or commitments remained unverified. Specifically, Branch investigators completed follow-ups on over 50 significant unverified cases concluded between January 1, 2001 and November 1, 2004, and involving the federally regulated organizations that had been subject to *PIPEDA* from the beginning (banks, telecommunications companies, national transportation companies, etc.).[3] The subject cases were those in which the Office had identified privacy problems and expected the organizations to take specified remedial action in response either to commitments they had made at our suggestion during investigations or to recommendations we had later made to them in letters of findings.[4]

Through day-to-day dealings, the Office had already formed a good sense of how well respondent organizations had been co-operating in investigations and following through on commitments and recommendations. However, when we analyzed the results of these follow-ups in conjunction with case results already known, we were able to see a fuller, clearer and statistically representative picture of the cumulative effect of our complaint investigations on compliance with *PIPEDA*.[5]

---

[3] The analysis did not include cases involving provincially regulated companies, since such organizations had been subject to the *Act* for less than a year (January 1, 2004).

[4] In the interest of time and efficiency, the many routine cases of (largely resolved) complaints under the access provisions of the *Act* were also excluded from consideration in both the follow-ups and the analysis.

[5] The analysis accounts for approximately 75 per cent of applicable cases concluded during the period in question.

Most notably, we determined that, of the verified cases in which our Office expected a remedial response, federally-regulated organizations had fully implemented our recommendations arising out of the investigation of a complaint about nine times out of ten. We also determined that 67 per cent of these satisfactory responses involved some degree of systemic improvement in the organizations themselves. In other words, in approximately two of every three cases, the organization's remedial response had gone beyond the mere settling of a complainant's immediate concern and had led the organization to establish positive substantive change in its information management systems relating to privacy policy, procedures and practices.

The following are just a few examples of systemic improvements implemented by respondent organizations in the first four years of *PIPEDA* arising from our recommendations:

- A bank instituted an alternative process to accommodate deposit account applicants who refused to consent to a credit check.
- Another bank, on our recommendation, collaborated with credit reporting agencies to develop understandable, consumer-friendly formats for credit information.
- Several organizations acknowledged that the use of social insurance numbers (SINs) is a privacy-sensitive issue and changed their policies and practices accordingly. One bank, for example, stopped requiring customers to use a SIN in activating credit cards. Another bank amended its loan application form to indicate that provision of the SIN is optional, and stressed to its employees that the SIN is not required for processing loan applications.
- Through extensive consultation with our Office, a bank whose privacy literature we originally considered to be the least compliant among all the banks greatly improved its consent language and practices, particularly as they related to use and disclosure of personal information for secondary marketing purposes. We now regard this bank's privacy literature as among the best.
- Another bank followed our recommendation to improve the security of computers at its kiosk branches.
- Another bank discontinued its practice of issuing unsolicited credit cards and creating credit card accounts without consent.
- A lending institution struck a privacy committee, instituted privacy training, and instructed staff on limiting the amounts of information they disclose in recovering debts.

- A telecommunications company stopped using customers' telephone records to obtain information about other individuals.
- In a case about the posting of employees' sales records, another telecommunications company told its sales managers about appropriate uses and disclosures of such information, updated its employee training program accordingly, and revised its recruitment and selection process to inform employees of the company's intended uses of their personal information.
- A broadcaster developed and distributed a policy on its use of security cameras and access controls.
- An airline vastly improved its privacy policy and practices related to its rewards program.
- A transportation-related management corporation fully implemented our recommendations concerning its sick leave policy. Most notably, the corporation no longer requires its employees to include specific diagnoses on their medical certificates.
- In close consultation with our Office, a market research company implemented our recommendations regarding its consumer surveys, particularly relating to identification of purposes, and consent to third-party disclosures. The result is a much more transparent and privacy-compliant survey form and process.
- A rewards program not only improved its communications materials as we recommended, but also made other privacy-related improvements beyond our recommendations.

Though not yet complete, the record already abounds with evidence that federally regulated organizations have largely taken their responsibilities under *PIPEDA* very seriously. They have generally cooperated with our Office in complaint investigations and have tended to remedy, in substantive and permanent ways, the problems that we identify. Similarly, the record clearly shows that complaint investigations in themselves greatly increased overall compliance with the *Act* by respondent organizations. Almost half of satisfactory responses by organizations have occurred, not pursuant to recommendations in a letter of findings, but rather during or as a direct result of the complaint investigation itself. In other words, our Office's investigators have been the main instruments of problem solving in almost half the cases of a satisfactory response by an organization.

Our rate of success shows not only the effectiveness of our investigative function, but also the continuing efficacy of the Commissioner's ombudsman role. Although the record appears sound, we are taking measures to improve it. We believe that our new formal procedure of systematic follow-up is one measure in particular that will enable us to bring about an even higher rate of compliance with *PIPEDA*.

Audit and Review

Strengthening the Audit Function

Section 18(1) of *PIPEDA* allows the Commissioner to audit the personal information management practices of an organization if the Commissioner has reasonable grounds to believe that the organization is contravening the fair information practices set out in the *Act* and Schedule. To date, we have conducted no audits under *PIPEDA*. However, now that *PIPEDA* is fully in force and organizations have had time to adapt to it, our Office has recently begun actions to use the audit power where warranted.

In March 2005, the Branch name changed from "Privacy Practices and Reviews" to "Audit and Review". This signals an important transformation. Our Office intends to make greater use of audits, and they will become an important tool in carrying out our mandate under both the *Privacy Act* and *PIPEDA*.

The Audit and Review Branch's goal 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.

The year 2004 marks the beginning of efforts to rebuild and strengthen audit and review functions. Audits have not yet been used to their potential as among the key tools for addressing the many privacy risks. The systemic risks are wide ranging, including inadequate data security, identity theft, inappropriate gathering, retention and use of personal information, and failure to act when privacy breaches occur.

It will take time to build the capacity to undertake sufficient and appropriate audits. The Branch now has only four auditors to undertake both public and private sector audits. The scope of the "audit universe" is over 150 federal departments and agencies subject to the *Privacy Act*, and thousands of commercial organizations in Canada subject to *PIPEDA*.

Steps our Office will take to strengthen the audit function include:

- Completing an external review of audit methods and practices;
- Setting a Branch goal and articulating team values;
- Undertaking a process to develop a longer term audit strategy and plan in view of privacy risks and issues;
- Building a business case to submit to Treasury Board of Canada to obtain further funding for audit and review;
- Raising awareness with Parliamentary committees about the value of privacy audits;
- Initiating a project to determine and test a process for establishing "reasonable grounds" to select subjects for audits under *PIPEDA*. The criteria and process will be published on our Web site during the next fiscal year, and we will welcome comments;
- Initiating a project to develop a self-assessment tool to help organizations ensure compliance with *PIPEDA*, and to promote good personal information management practices. We want organizations to understand that good privacy makes for good business and that they need a sound privacy management framework. This would include internal auditing of systems and practices for meeting privacy obligations. The self-assessment tool (audit program) will also be published on our Web site; and
- Undertaking a survey of private industry about the use of radio frequency identification devices (RFIDs).

Keeping Watch on Radio Frequency Identification

We continue to monitor advances in RFID technology. In our view, companies should establish policies and standards before they implement RFID technology, not after the fact. Any use of RFIDs must comply with *PIPEDA*. Furthermore, we want to know the role of RFID applications in data aggregation and mining activities, since these depend on obtaining ever-increasing amounts of detail about individuals and what they buy or rent.

We plan to send letters to selected corporations in Canada that might be introducing RFIDs, to better understand the emerging uses of RFID. Our primary interest is in learning how RFID might be used to link personal information with products and services. We want to know if the technology will be used to identify or track individuals. We also want to know if companies will do privacy impact assessments or threat/risk assessments when developing and implementing RFID applications, and how employees and customers would learn about the presence and use of RFIDs.

The survey results will appear in next year's Annual Report. We will not disclose proprietary business information. We will continue monitoring developments in RFID technology to see where guidance on privacy issues is necessary.

In the Courts

PIPEDA Applications

Under section 14 of *PIPEDA*, an individual complainant has a right, following the Commissioner's investigation and report, to apply to the Federal Court for a hearing in respect of any matter referred to in the Commissioner's report. These matters must be among those identified in section 14. Section 14 also allows the Commissioner to apply directly to the Federal Court in respect of a Commissioner-initiated complaint.

Section 15 also allows the Commissioner to apply directly to the court for a hearing in respect of any matter covered by section 14 (with the consent of the complainant); appear before the Court on behalf of any complainant who has applied for a hearing under section 14; or, with the permission of the Court, appear as a party to any section 14 hearing not initiated by the Commissioner.

Between January 1, 2001 and December 31, 2004, 35 applications were filed in Federal Court in relation to *PIPEDA*. Fifteen of those were filed in 2004. This means that the number of applications in 2004 alone almost equaled all other applications filed since *PIPEDA* came into force until the start of 2004 – a huge annual increase. Following is a list of all of the PIPEDA applications filed in the Federal Court in 2004:

- Karen and Daniel Edwards v. Canadian Imperial Bank of Commerce (Federal Court No. T-35-04), Discontinued November 2, 2004
- Keith Vanderbeke v. Royal Bank of Canada (Federal Court No. T-222-04)
- Ron Gass v. NAV Canada (Federal Court No. T-821-04), Dismissed July 2004 (by consent)

- Pierre Jean Trudeau v. Banque TD Canada Trust (Federal Court No. T-851-04), Dismissed February 23, 2005 (for delay)
- Bradley Nazaruk and United Transportation Union, Local 691 v. Canadian National Railways (Federal Court No. T-948-04), Discontinued July 8, 2005
- Janice Morgan v. Alta Flights (Charters) Inc. (Federal Court No. T-1066-04)
- Ian David Kosher v. Canadian Imperial Bank of Commerce (Federal Court No. T-1143-04)
- 3web Corporation v. Llano Gorman (Federal Court No. T-1603-04), Discontinued June 2005
- Paul Wansink and Telecommunications Workers Union v. Telus Communications Inc. (Federal Court No. T-1862-04), Consolidated with Federal Court No. T-1865-04, December 31, 2004
- Henry Fenske and Telecommunications Workers Union v. Telus Communications Inc. (Federal Court No. T-1863-04), Consolidated with Federal Court No. T-1865-04, December 31, 2004
- Paul Bernat and Telecommunications Workers Union v. Telus (Federal Court No. T-1864-04), Consolidated with Federal Court No. T-1865-04 31, December 2004
- Randy Turner and Telecommunications Workers Union v. Telus (Federal Court No. T-1865-04)
- John Testa and Brenda Marie Testa v. Citibank (Federal Court No. T-2135-04), Dismissed June 15, 2005 (settlement reached at pre-trial conference)
- Richard Breithaupt and Peggy Fournier v. Hali MacFarland and Calm Air International ltd. (Federal Court No. T-2061-04)

Important Decisions

Following are important decisions made in 2004 on the application of *PIPEDA*:

Mathew Englander v. Telus Communications Inc. and Privacy Commissioner of Canada
Federal Court File No. T-1717-01 and Federal Court of Appeal File No. A-388-03

Mr. Englander argued that Telus uses and discloses customers' names, addresses and telephone numbers in its white pages directories and otherwise, without customers' knowledge and consent. He also claimed that Telus inappropriately charges customers for choosing to have their telephone number "non-published". He felt that these actions by Telus contravene sections 5(1) and (3) of *PIPEDA*, as well as several clauses of Schedule 1.

On the question of consent, the former Commissioner found that the company did obtain valid consent through implication and complied with the regulations regarding publicly available information. He focused on the company's questioning of customers about how their information should appear in the white-pages directory and determined that the question itself implied the eventual appearance of the information in publicly available directories. Since information subsequently published in other formats merely reflects what is published in the white pages directory, it too is considered publicly available information for purposes of the regulations under the Act, and may be collected, used or disclosed without consent.

As to charging fees for the non-publication of customers' information, the Commissioner referred to CRTC Telecom Order 98-109, which states that telecommunications companies may charge no more than $2.00 per month to provide non-published telephone service. He determined that the company did have the authority to charge its monthly fee of $2.00 for non-publication, and that doing so was not unreasonable.

Mr. Englander filed the very first Federal Court application under section 14 of *PIPEDA* after the former Commissioner released his findings. The former Commissioner was not a party to these proceedings. Ultimately, the Federal Court concluded that Mr. Englander had failed to convince the court that his application was well-founded, and dismissed the application with costs to the Respondent.

Mr. Englander filed an appeal in the Federal Court of Appeal. The current Privacy Commissioner was granted leave to intervene in the appeal.

The Court heard the appeal on October 7, 2004. The decision, released on November 17, 2004, allowed the appeal in part on the basis that Telus did not have proper informed consent from first-time customers to use their personal information in directories; consent is not informed when the person allegedly giving it is not aware at the time of the possibility of opting-out. Information given to customers subsequently may factor into an evaluation of compliance with the "openness" principle, but comes too late for consent. The Court emphasized that consent in this situation was particularly critical because it was the gateway to information becoming publicly available.

The Court's February 9, 2005, decision declared that in light of Telus' undertaking to change its practices to conform with *PIPEDA*, there was no need to compel Telus to make those changes. The judgment states that "the Court is satisfied that it is sufficient in the case at bar to declare that Telus has infringed section 5 of the *Personal*

Information Protection and Electronic Documents Act and that there is no need for the issuance of a mandatory injunction."

Erwin Eastmond v. Canadian Pacific Railway and Privacy Commissioner of Canada
Federal Court File No. T-309-03

Mr. Eastmond complained that his employer was collecting the personal information of employees without their consent. Specifically, he was concerned that digital video recording cameras installed at the company yard could collect personal information of employees.

The former Privacy Commissioner applied section 5(3) of *PIPEDA* and explained that when using this section one must consider both the appropriateness of the organization's purposes for collection and the circumstances surrounding those purposes. To that end, he used a four-point test for assessing reasonableness: (1) Is the measure demonstrably necessary to meet a specific need; (2) Is it likely to be effective in meeting that need; (3) Is the loss of privacy proportional to the benefit gained; and (4) Is there a less privacy-invasive way of achieving the same end? The former Commissioner found that a reasonable person would not consider these circumstances to warrant such an intrusive measure as digital video surveillance. He concluded that the company's use of this type of surveillance for their stated purposes was not appropriate and that the company had contravened section 5(3) of *PIPEDA*.

In February 2003, Mr. Eastmond filed an application, as permitted by section 14 of *PIPEDA*. He sought an order confirming the finding of the former Commissioner as well as various related orders. He also requested a certified copy of the former Commissioner's record of investigation.

The former Commissioner objected to this request for materials, and the Court agreed in June 2003 that the *Federal Court Rules* do not allow an Applicant, in a section 14 application under *PIPEDA*, to request material in the possession of the Privacy Commissioner.

The Interim Privacy Commissioner was also added as a party pursuant to section 15(c) of *PIPEDA*, but took no position as to the appropriate outcome on the facts, instead arguing on points of law that the Court should accord some deference to the expertise of the Commissioner and should adopt the four-point test to determine the appropriateness of the collection of the information by CP Rail. A supplementary factum was filed in December 2003 addressing the jurisdiction over the issues of

both the Commissioner and the Court, notwithstanding that these issues arose in a collective bargaining situation. The supplementary factum suggested that concurrent jurisdiction existed in this situation.

The application was heard in April 2004. On June 11, 2004, the court released its decision. The Court found that the Privacy Commissioner did have jurisdiction, that the essence of this dispute did not arise from the collective agreement, and that it was not Parliament's intention to exclude unionized workers from the scope of *PIPEDA*.

The Court also concluded that although this was a proceeding *de novo,* the Commissioner was entitled to a degree of deference in light of the Commissioner's expertise.

Finally, the Court adopted the four-point test for section 5(3), with the caveat that the specific factors considered in this case might not be appropriate in all cases. Using that test, the Court concluded that a reasonable person would consider the organization's purposes for collecting the images through the medium of a digital video camera to be appropriate in the circumstances. CP Rail therefore had not contravened *PIPEDA*.

Cases in the Courts

The following cases are of particular interest in the ongoing interpretation of PIPEDA:

Keith Vanderbeke v. Royal Bank of Canada

Federal Court File No. T-222-04

Mr. Vanderbeke had previously made a complaint about Royal Bank of Canada's (RBC) treatment of his personal information. This related complaint alleged systemic improprieties in RBC's record keeping procedures, specifically that the bank was not "properly" retaining mortgage renewal acknowledgement letters for its clients. The bank explained that they do not keep a copy of the acknowledgement letters sent to customers as the letters contain information that is available in other documents. Reviewing the complaint, the Assistant Privacy Commissioner considered that *PIPEDA* provides individuals with a right of access to personal information itself, but not necessarily the specific documents containing that information. Accordingly, she considered the complaint not well-founded.

Mr. Vanderbeke filed an application, as permitted by section 14 of *PIPEDA*, on January 29, 2004. RBC made a motion for an order to strike the application, but was not successful.

An order dated July 5, 2004, stipulated that Mr. Vanderbeke pay security monies into Court before filing his affidavit. This caused delay in the proceedings until February 23, 2005. To date, the Commissioner has not become involved in this application, but is monitoring developments closely.

Janice Morgan v. Alta Flights (Charters) Inc. and Privacy Commissioner of Canada
Federal Court File No. T-1066-04 and Federal Court of Appeal File No. A-184-05

Ms. Morgan, a former employee of Alta Flights, complained that her employer tried to collect and use her personal information without her knowledge and consent. Specifically, she alleged that a manager had taped a digital recorder to the underside of a table in a smoking room accessible to employees in an attempt to collect their personal information. The company acknowledged that the manager had attempted to collect employee personal information without the knowledge or consent of those employees.

The investigation determined that since there was no evidence of a recording, there was no evidence that the complainant's personal information had been collected or used. The Assistant Privacy Commissioner concluded that the company was not in contravention of *PIPEDA* and, accordingly, the complaint was not well-founded. However, she cautioned that the company should not interpret her finding as an approval of what the manager had attempted to do.

Ms. Morgan filed an application in Federal Court, as permitted by section 14 of *PIPEDA*, on May 26, 2004. The original application incorrectly named the Privacy Commissioner as a respondent. On September 14, 2004, the Court granted the Privacy Commissioner's motion to be struck as a respondent and added as a party to the application, as permitted by section 15(c) of *PIPEDA*.

At trial, the Privacy Commissioner made representations concerning five matters: (1) jurisdiction of *PIPEDA* over the subject matter notwithstanding a *Canada Labour Code* unjust dismissal complaint in respect of the same issue; (2) the appropriate standard of review and deference to be accorded the Privacy Commissioner's findings; (3) the appropriate interpretation of section 7(1)(b); (4) whether an attempted collection constituted a collection; and (v) whether there is a common law jurisdiction to grant remedies not authorized by *PIPEDA*.

The court heard the application on March 15, 2005. Like the Assistant Privacy Commissioner, the Court concluded that since there was no evidence that any conversations were recorded, the company did not actually manage to collect and/or

use any personal information. There was no violation of *PIPEDA* since an attempt to breach the *Act* does not exist as a violation of *PIPEDA*.

On the issue of whether to give deference to the Privacy Commissioner's decision, the Court concluded that it may rely on the decision of the Privacy Commissioner or certain parts of it in arriving at its determination, but it is not bound to do so. When exercising its discretion *de novo*, the Court will give less deference to the decision of the Privacy Commissioner than it would otherwise. However, some regard is warranted about the factors taken into consideration by the Privacy Commissioner in balancing the privacy interests of the complainant and the employer's legitimate interest in protecting its employees and property.

Ms. Morgan filed an appeal of the decision in April 2005.

Paul Wansink and Telecommunications Workers Union v. Telus and Privacy Commissioner of Canada
Federal Court File No. T-1862-04
Henry Fenske and Telecommunications Workers Union v. Telus and Privacy Commissioner of Canada
Federal Court File No. T-1863-04
Paul Bernat and Telecommunications Workers Union v. Telus and Privacy Commissioner of Canada
Federal Court File No. T-1864-04
Randy Turner and Telecommunications Workers Union v. Telus and Privacy Commissioner of Canada
Federal Court File No. T-2222-03

The Applicants complained to the Privacy Commissioner that their employer, Telus Communications Inc., had contravened *PIPEDA* by forcing them to consent to the collection of personal biometric information and to provide the information to enable a computer to automatically authenticate identity using their voice prints.

The Assistant Privacy Commissioner assessed the requirement of the voice print and found it not overly invasive. She found it an appropriate balance between the employees' right to privacy and the employer's needs. The purpose was reasonable and appropriate, Telus had properly informed its employees of the purposes, and it had appropriate safeguards in place in relation to the information.

After the release of the Assistant Commissioner's findings, each of the four complainants filed a separate application in Federal Court under section 14 of *PIPEDA*. An order dated December 31, 2004 consolidated all of the applications under Federal Court File No. T-1865-04.

The Privacy Commissioner then sought under section 15(c) of *PIPEDA* to become a party to these applications in order to make representations to assist the court in developing a test for negotiating the balance between commercial needs and individual privacy rights. Telus consented to the motion but made representations to the Court suggesting a limited role for the Privacy Commissioner. The Commissioner successfully challenged this, and on February 22, 2005, obtained full party status.

The Commissioner made representations on several matters, including: (1) that the Telecommunications Union was not a proper applicant in the proceeding; (2) that the Court should have due regard for the factors to be considered in balancing the interests of the parties; (3) that the legal framework and factors used by the Commissioner in balancing the interests of the parties should be applied by the Court; (4) that *PIPEDA* does not require that the employer seek union consent rather than seeking consent directly from individual employees; (5) that exceptions to consent requirements do not apply in this situation; (6) when may consent be implied; and (7) a recognition of the ability to withdraw consent.

A hearing has been scheduled for September 20, 2005.

John Testa and Brenda Marie Testa v. Citibank
Federal Court File No. T-2135-04

Mr. Testa claimed that Citibank disclosed a significant amount of his personal information to his employees without his consent. He further alleged that these disclosures were extremely damaging to his reputation and contributed to his decision to resign as the head of the company.

In her finding, the Assistant Commissioner acknowledged that *PIPEDA* allows an organization to disclose an individual's personal information without consent for the purposes of collecting a debt. However, this exception did not confer *carte blanche* for an organization to disclose however much information it wished. She felt that in this instance it was clear that excessive amounts of information had been divulged. Accordingly, she found the bank to be in contravention of Principle 4.3 of Schedule 1 of *PIPEDA* and the complaint to be well-founded.

An application was filed in Federal Court on December 1, 2004. The Commissioner was expected to seek leave to appear as a party as permitted by section 15(c) of *PIPEDA*. However, a settlement was reached at a pre-trial dispute resolution conference and, accordingly, the application was dismissed on June 15, 2005.

Richard Breithaupt and Peggy Fournier v. Hali MacFarlane and Calm Air International Ltd.
Federal Court File No. T-2061-04

Mr. Breithaupt complained that a Calm Air employee (Ms. MacFarlane) disclosed his and his wife's itinerary information to the RCMP without their knowledge and consent. It was undisputed that the Calm Air employee had obtained access to the information without their knowledge and consent. However, both the Calm Air employee and the RCMP officer denied that the employee disclosed this information to the officer.

Documentary evidence led the Assistant Commissioner to conclude that there was indeed a disclosure. She found that the employee had used personal information for purposes other than those for which it was collected, and then disclosed it in contravention of Principles 4.3 and 4.5 of Schedule 1 of *PIPEDA*. Accordingly, the complaint was well-founded.

The complainant filed an application under section 14 of *PIPEDA* in Federal Court on November 18, 2004. The Commissioner is not a party to this application, though she is monitoring its progress.

Judicial Review

The following cases are important in defining the extent of the Commissioner's enforcement powers under *PIPEDA*:

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

A complaint was filed with our Office alleging (among other things) that the Blood Tribe Department of Health had denied an individual access to her personal information and did not provide reasons for the denial.

In our view, the Commissioner must have access to all documents to ensure that exemptions claimed have been properly applied and to guard against abuse. However, during this investigation the Blood Tribe Department of Health refused to provide the Commissioner with access to solicitor-client privileged documents. As a result, our Office issued its first order for the production of records, using the enforcement powers as set out in sections 12(1)(a) and (c) of *PIPEDA*.

In response, an application for judicial review of the Privacy Commissioner's decision to issue an order for production was made by the Blood Tribe Department of Health, as permitted by section 18.1 of the *Federal Court Act*. The Court dismissed the application in March 2005. 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 effectively perform that role 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 issue the production order. The order did not limit or deny any solicitor-client privilege that the applicant may enjoy in the questioned documents.

The Applicant filed an appeal of this decision in April 2005.

3web Corporation v. Llano Gorman and Privacy Commissioner of Canada
Federal Court File No. T-1603-04

Mr. Gorman complained that 3web Corporation, an internet service provider who had been his employer, had installed web-cameras to monitor employees in the workplace. The cameras were located in the sales and marketing division and the technical support staff area. The Assistant Commissioner concluded that the complaint was well-founded. In doing so, she stated that: (a) it was unlikely that a reasonable person would consider employee productivity to be an appropriate reason to use video and audio surveillance; and (b) by using web cameras in the manner described in this complaint, the company was not fundamentally recognizing the right of privacy of its employees; the balance integral to section 3 of *PIPEDA* was tipped too far away from the privacy rights of individuals. The use of cameras for these purposes would undermine *PIPEDA*.

PIPEDA provides that a complainant or the Privacy Commissioner may apply to the Federal Court for a hearing of any matter referred to in the Commissioner's report. In that the Commissioner's report makes recommendations only, there is no such provision for a respondent organization. In this case, the organization initiated a judicial review application. It named Mr. Gorman as a respondent, although it also sought an order stating that the Assistant Privacy Commissioner's report was "illegal and invalid."

In October 2004, the Privacy Commissioner filed a motion requesting that (a) she be added as an intervener and (b) the application be struck. This motion was heard

in February 2005, at which time the Commissioner was added as an intervener to the proceeding. The Court dismissed the Commissioner's motion to strike the application as a whole, concluding that the issue was best suited for determination at trial.

The company discontinued the proceeding in June 2005.

Public Education and Communications

The Office of the Privacy Commissioner of Canada is mandated specifically under *PIPEDA* to develop and conduct information programs to foster public and organizational understanding and recognition of the rules that govern the collection, use and disclosure of personal information. And although there is no legislative mandate for public education specified under the *Privacy Act*, there is certainly a mandate to ensure departments and agencies are held accountable for their personal information handling practices. There is often a necessity to inform the public, as well as departments and agencies, about the requirements of the Act and related policies, and the impact on the privacy rights of Canadians of current and proposed government activities.

In 2004, the Office undertook a strategic communications planning effort with the expertise of external consultants, and the result was a comprehensive communications and outreach strategy for the coming years. This strategy will enable the Office to have a more comprehensive, proactive approach to communications planning and delivery; a more truly public education-focused approach to communications surrounding *PIPEDA*; and build a greater level of awareness of the Office and of key privacy issues under both laws.

In addition to developing this strategy the Office undertook the following communications activities in 2004:

Speeches and Special Events

Speaking engagement opportunities have helped our Office raise awareness of privacy issues among diverse audiences and settings, including professional and industry associations, non-profit and advocacy groups and universities. In 2004, the Commissioner, Assistant Commissioners and other senior officials delivered

19 speeches, speaking out about issues with privacy implications, such as security initiatives and health care delivery.

In March 2004, the Office began hosting an in-house Lecture Series (approximately one per month). These information sessions featured experts on a variety of privacy issues and brought together members of the privacy community and staff. In 2004, the Office hosted ten of these information sessions.

Media Relations

Privacy issues continued to be of interest to the media in 2004, with significant coverage in Canada on issues such as the full implementation of *PIPEDA*, about which the Office received media calls and participated in interviews. In addition, through other proactive media relations efforts, such as the dissemination of news releases, the Office had the opportunity to raise awareness of, for example, the launch of its Contributions Program; the Commissioner's views on important legislation, such as the *Public Safety Act* and the do-not-call list legislation; and the Office's views regarding transborder flows of personal information.

Web Site

We post new and useful information on our Web site on an ongoing basis. Fact sheets, news releases, speeches, case summaries of findings under *PIPEDA*, are posted to keep the site interesting to individuals and organizations. In 2004-2005, the Office redesigned its Web site in order to make it compliant with the Common Look and Feel standards established by Treasury Board. This resulted in an enhancement to the design as well as to the navigation tools on the site, in order to help visitors make better use of the site. The Office also made the site more dynamic with the posting of a downloadable Web-video for businesses on complying with *PIPEDA*. Since 2001, we are pleased to report that visits to the site have more than quadrupled, reaching 922,106 in 2004.

Publications

The Office has produced information materials, including guides for individuals and organizations on *PIPEDA*, as well as a variety of new fact sheets on issues including consent, use of the social insurance number in the private sector, transborder flow of personal information, and how our Office conducts investigations into potential privacy breaches.

In 2004-2005, in addition to preparing new fact sheets, we developed an e-kit for businesses to help them comply with the new law. We also revised the content of our guides, to ensure they were up-to-date given the final stage of implementation of *PIPEDA* on January 1, 2004. We received requests for these materials on a daily basis. Not only were these materials sent to individuals upon request, they were also distributed at conferences and special events, and accessed in electronic format by visitors to our Web site. In 2004, close to 22,000 of our publications (guides, fact sheets, annual reports, copies of both federal privacy laws) were sent out, in addition to the more than 742,000 publications which were downloaded from our Web site.

Internal Communications

Internal communications activities were also a focus of the Office and played a key role in 2004, increasing transparency between management and staff, especially during its ongoing institutional renewal, but also through day-to-day activities. Internal communications activities in 2004 involved providing staff with information on, for example, human resources issues, upcoming speaking engagements, Parliamentary appearances, senior management and labour management committee meetings, and special events such as all-staff meetings and information sessions. The Office has been developing an Intranet, an internal communications portal to host all internal communications and maximize staff access to information, which will be launched in 2005.

In the upcoming year, the Office will continue to undertake the activities outlined above. We also hope to be in a position to initiate many of the more proactive public education activities outlined in the communications and outreach strategy.

Corporate Services

On the Path to Institutional Renewal

The Commissioner's most immediate priority has been to lead the Office's institutional renewal by strengthening OPC management processes, particularly human resources and financial management – planning, budgeting, reporting and control mechanisms.

The overall financial framework in which our Office operates is based on the government fiscal year (2004-2005).

Planning and Reporting

A foundation component of the Office's institutional renewal is a strategic planning, reporting and control process. During 2004-05 we completed our first year under this revised process. The strategic plan established at the beginning of the year was our road map for the year. As part of the new process were reporting and review opportunities. We made adjustments to plans and budgets throughout the year. To assist in our reporting and reviews we developed a Performance Measurement Framework and a monthly performance report. We also launched a Business Process Review of the entire organization which will enable the Office to better estimate resource requirements and to draft a business case for permanent funding.

Human Resources

We continue to work toward the development and implementation of changes to improve how the office is run and the quality of the workplace. Significant changes and improvements have been made to the Human Resource management policies and practices.

We developed a number of Human Resource policies in consultation with central agencies and unions. These policies will guide us as we build on the successes of the past year and we continue on our path of institutional renewal. An Instrument of Delegation of Human Resource Management was developed and will serve as a tool to inform and guide managers, and enable them to manage their human resources. A new Strategic Human Resource Plan and Staffing Strategy, as well as an Employment Equity Action Plan, will help the OPC achieve its mandate and ensure the recruitment of a highly qualified workforce that is diversified and representative of Canadian society. As part of OPC's commitment to increase transparency in the staffing processes, a staff newsletter was developed; it is distributed on a monthly basis to all staff.

Over the course of the past fiscal year we made significant strides in the area of 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 and employee appraisals and harassment in the workplace. The development and implementation of a Learning Strategy and Curriculum with the CSPS will enable staff to continue to develop the expertise and competencies required to fulfil their functions, as well as to position staff to take on new responsibilities and accountabilities.

We continued to work collaboratively with Central Agencies such as the Public Service Commission and the Public Service Human Resources Management Agency of Canada on follow-up measures to the recommendations of the Public Service Commission and the 2003 report of the Auditor General of Canada. This included measures that will allow OPC the opportunity to regain its full staffing delegation authority.

Finance and Administration

The OPC received a clean opinion on Audited 2003-2004 Financial Statements by the Office of the Auditor General of Canada. This is a significant milestone and a very positive indicator that the organization has indeed advanced on the path of institutional renewal. The organization has built on that success by establishing planning and review cycles, by streamlining and improving the financial management policies and practices.

Information Management / Information Technology

Signification advancements have also been made in how we manage our information assets. We completed an audit of our information management systems and we

completed a vulnerability assessment of our information technology. We also completed an information technology strategy. This will help us to not only meet our obligations with respect to the management of government information and security policies, but more importantly it will guide us as we move forward in improving on the management of our information assets. During the year we completed a significant upgrade to our case tracking and reporting system, Integrated Investigations Application (IIA). Finally we also established the framework for an internal Intranet site. This site will allow for effective communicating and sharing on information for employees.

Down the road

Strategic planning is an important annual exercise for the OPC. Our last session in January 2005 provided managers and employees an opportunity to re-examine the OPC's priorities for 2005-2006, and the actions they would take to achieve these priorities.

Corporate Services priorities for 2005-2006 are to:

- Develop and implement a Management Accountability Framework (MAF);
- Implement and maintain a human resource strategy that enables the Office to recruit, retain and develop staff and foster a continuous learning environment;
- Satisfy central agencies' requirements to regain delegated authorities, and enable the Office to take on new delegation to implement the Public Service Modernization Act;
- Develop and implement integrated information management;
- Complete Business Case for Resources for the OPC;
- Review Corporate Services Branch and Human Resources Branch policies and procedures; and
- Continue providing effective integrated financial services to the OPC.

Our Resource Needs

At the beginning of fiscal year 2004-2005, the Office's budget was $11.2 million, the same as the previous year. Included was $6.7 million for the Office's *PIPEDA* activities. Ongoing funding of OPC activities continues to be extremely important.

With privacy rights continually under threat, the Office's operations need to be funded adequately so that it is prepared to address the multitude of emerging privacy issues in the public and private sector.

The Office does not have adequate resources to fully exercise its powers and responsibilities under both Acts. Without adequate permanent funding, the Office cannot:

- Reinforce our audit and review functions to effectively address compliance under both privacy laws or strengthen our capacity to monitor, research and respond to emerging issues of technology and privacy;
- Conduct outreach and public education to influence change so policies and programs are viewed through a privacy lens;
- Continue investigating in a timely manner and resolving the growing number of complaints under both Acts; and
- Continue providing specialized legal and strategic advice and litigation support under both federal privacy laws, as well as strengthening established approaches and procedures to deal with cross-jurisdictional complaints.

To this end, the Office's priority beginning in the last quarter of fiscal year 2004-05 was to completely review all business processes. The review included establishing workload indicators and reviewing the legislative requirements, as well as external and internal factors that have an impact on our operations. This will enable the Office to develop a Business Case and make a formal submission to the Treasury Board Secretariat and to Parliament later in 2005 to stabilize our resource base and seek permanent funding for the Office.

We hope that with adequate permanent funding, the Office can further assure Parliament that it is effectively ensuring respect for Canadians' privacy rights in the public and private sectors.

Financial Information

April 1, 2004 to March 31, 2005

	Expenditure Totals ($)	% of Totals
Privacy Act	3,745,058	32
PIPEDA	6,849,650	58.5
Corporate Services	1,107,296	9.5
Total	11,702,004	100

Note: Although OPC salary budget allows for approximately 100 FTEs (full-time equivalents), there were only 86 FTEs staffed at the Office at the end of March 2005.

Detailed Expenditures[1]	*Privacy Act*	*PIPEDA*	Corporate Services	Total
Salaries	3,330,147	3,039,732	419,120	6,788,999
Employee Benefits Program	190,327	844,575	154,640	1,189,542
Transportation & Communication	41,238	266,129	81,282	388,649
Information	1,907	147,911	5,239	155,057
Professional Services	171,783	1,397,579	210,403	1,779,765
Rentals	2,730	107,874	23,759	134,363
Repairs & Maintenance	4,698	155,805	85,353	245,856
Materials & Supplies	9,304	50,764	21,633	81,701
Acquisition of Machinery & Equipment	384	451,788	98,026	550,198
Other Subsidies & Payments	- 7,460	20,084	7,841	20,465
Transfer Payments	0	367,409	0	367,409
Total	**3,745,058**	**6,849,650**	**1,107,296**	**11,702,004**

[1] Total expenditure figures are consistent with the Public Accounts of Canada.

Financial Statements

The Management Responsibility letter and the audited financial statements as at March 31, 2005 will be available on our Web site at www.privcom.gc.ca in October 2005.