Privacy Commissioner of Canada

Commissaire à la protection de la vie privée du Canada

Privacy

Annual Report to Parliament 2003-2004

Canada

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. IP50-2004
ISBN 0-662-68421-4

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

Privacy Commissioner of Canada

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

Commissaire à la protection de la vie privée du Canada

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

November 2004

The Speaker

The Honourable Daniel Hays, Senator
The Senate of Canada
Ottawa

Dear. Mr. Speaker:

I have the honour to submit to Parliament the Annual Report for the Office of the Privacy Commissioner of Canada, for the period from April 1, 2003 to March 31, 2004 for the *Privacy Act* and from January 2 to December 31, 2003, for the *Personal Information Protection and Electronic Documents Act*.

Yours sincerely,

Original signed by

Jennifer Stoddart
Privacy Commissioner of Canada

Privacy Commissioner of Canada

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

Commissaire à la protection de la vie privée du Canada

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

November 2004

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 for the Office of the Privacy Commissioner of Canada, for the period April 1, 2003 to March 31, 2004 for the *Privacy Act* and from January 1 to December 31, 2003 for the *Personal Information Protection and Electronic Documents Act*.

Yours sincerely,

Original signed by

Jennifer Stoddart
Privacy Commissioner of Canada

TABLE OF CONTENTS

FOREWORD

This has been an exceptional year for the Office of the Privacy Commissioner of Canada. When I was appointed on December 1, 2003, I took over stewardship of an office that had undergone a great upheaval. In the course of six months, a Commissioner and several senior officials resigned amid scandal and intense publicity, an interim Commissioner was appointed, numerous internal and external reviews, audits and investigations were undertaken – and some are still ongoing – two Assistant Privacy Commissioners were appointed and a significant corporate restructuring was undertaken. I took over the helm of a ship that, while set on a positive course by Interim Privacy Commissioner Robert Marleau, was still navigating through a sea of administrative, financial and organizational crises.

Great progress has been made in the institutional renewal and strengthened management and financial framework of the OPC. This progress has been essential to rebuilding this Office and our efforts to emerge as a more effective organization, which upholds the principles of the Public Service while, at the same time, delivering on its mandate to protect and defend the fundamental privacy rights of Canadians.

I would like to salute the tremendous work of Interim Commissioner Robert Marleau in helping to move this Office through a difficult and complex period. M. Marleau's support and encouragement of staff, his work with audit and investigation teams and his emphasis on responsibility and teamwork have provided a strong foundation for a return to normalcy. He has our appreciation and gratitude.

In building on that foundation, corrective measures have been taken and continue to be taken to restore the overall wellness of the working environment, to further strengthen management practices and financial controls, to bring greater transparency and fairness to the human resources function, to encourage innovation, and to engage employees and union representatives in re-building and sustaining a process of organizational learning.

Other measures successfully undertaken include a cost recovery plan and a comprehensive planning process to realign our strategies and goals. An initial Report to Parliament on Action Arising from the Auditor General's Report on the Office of the Privacy Commissioner of Canada, jointly tabled by our Office and the President of Treasury

Board of Canada on October 31, 2003, detailed actions taken or to be taken on recovery actions by our Office. The report was followed by a final report tabled in April 2004.

We have also established an External Advisory Committee comprised of distinguished national privacy experts to provide input and guidance to the Office on strategic directions and priorities and established a Union Management Consultation Committee and a Health and Safety Committee to restore the overall wellness in the workplace. In addition, we are working actively with the Treasury Board Secretariat to improve our Human Resources functions. A significant focus of our renewal has been to re-build and regain the confidence of the Parliament of Canada. To this end, we have created a new role for a Parliamentary Liaison Officer, to help us fulfill our ongoing responsibilities as Parliament's window on privacy issues.

In the midst of this challenging and chaotic year, our Office was preparing for full implementation of the *Personal Information Protection and Electronic Documents Act* — also known as *PIPEDA*. On January 1, 2004, *PIPEDA*, which has come into force in stages, extended to the collection, use or disclosure of personal information in the course of any commercial activity within a province – except where privacy legislation deemed "substantially similar" by the federal government is in force.

PIPEDA is a flexible, pragmatic law that addresses the multi-jurisdictional issues raised in our constitutional context. The *Act* may be replaced by legislation that has been found to be "substantially similar" to the federal law. At the time of publication of this report, only Quebec's legislation has been found to be substantially similar, although we expect positive findings for the privacy legislation passed in Alberta and British Columbia. Our Office is working and will continue to work cooperatively with our provincial counterparts in a harmonized approach to dealing with privacy complaints in the private sector.

PIPEDA thus affects organizations from large corporations to small convenience stores, multi-national financial and insurance industries to corner florists and the neighbourhood dry cleaners. There has been an initial period of confusion and anxiety over these new rules about personal information in the private sector.

However, over the year and particularly in the months leading up to the January 1, 2004 target date, our focus was to help organizations implement and comply with *PIPEDA* and to engage in outreach, cooperation, public education, and the creation of innovative new partnerships with the private sector. We have consulted extensively with private sector business associations, in particular with the banking and financial sector and with the direct marketing industry. Assistant Privacy Commissioner Heather Black,

former General Counsel with our Office and with Industry Canada, where she worked on development of the *Personal Information Protection and Electronic Documents Act*, has criss-crossed the country this year on a busy schedule of speaking engagements to a wide variety of groups to raise awareness about *PIPEDA*.

We also responded to thousands of inquiries and requests for information on *PIPEDA* from businesses and organizations all across Canada; we engaged in consultations with business groups and associations; we sent out thousands of copies of reports, business guides, fact sheets and other public education materials; we have reorganized and overhauled our Web site to be compliant with the Government Common Look and Feel standards, and have made several new resources, guides and compliance tools available electronically to Canadian businesses and individuals.

It has been an exceptional year for *Privacy Act* complaints as well. Our Office received a record number of new complaints — a 250 per cent increase over the previous year. You will find more details explaining these statistics further on in this Report. As well, our investigators closed a record number of complaint investigations – an achievement to be highly commended in light of the extra challenges faced by our staff this year.

While it has been a difficult and challenging time for our Office, our work to monitor technological trends and initiatives to help protect Canadians' privacy and the integrity of personal information continued, with new threats to privacy emerging nationally and internationally. At the start of the year, the idea of a National Identity Card was proposed, opposed by many Canadians, and has been put on hold — for the time being at least. The vast majority of Canadians who made presentations to the Committee — including representatives from this Office – were staunchly opposed to the introduction of a national identity card. We remain opposed.

Personal information about Canadians continued to be gathered, stored, sorted and shared in alarming amounts on the basis of the idea – however unproven – that more information about individuals equals greater security against terrorists and other threats. We are concerned about the increasing integration of our border security with that of the United States, and the impetus this gives to the collection of large databases of personal information about travellers, potential travellers, and people in the transportation industry who must cross borders regularly to do their jobs. Our Office is looking very closely at the personal information handling practices of the newly created Canadian Border Services Agency.

The issue of trans-border data flow also commanded our specific attention this year. In an increasingly digital world, Canadians' personal information can be sent anywhere in the world

at the click of a mouse. We are concerned about the impact this may have on Canadians' rights to privacy. Our Office is working on a project that will help outline the pathways for personal information flow across borders, and what rights and protections may apply to that information. We recognize the need for increased security in today's environment, and would never stand in the way of legitimate measures to fight terrorism. But the need for national and international security must be balanced against the fundamental human right to privacy and the individual's right to control the collection, use and disclosure of personal information.

New technologies are emerging that threaten our privacy in ways previously unimagined. We will continue to monitor the use and impact of technologies such as video surveillance, spyware, radio frequency identification devices (RFIDs), global positioning systems, wireless communication devices, and biometric identifiers such as face recognition, DNA and fingerprints. Our Office is working with our federal partners on finding appropriate legal, regulatory, and technical measures to address these issues.

For example, we have seen spam – those ubiquitous unsolicited e-mail messages – rapidly become a real risk to Canadians' privacy and the integrity of their personal information. Spam messages often carry malicious computer code into your computer system, creating programs that can read your e-mail, track your Internet use, and even steal your passwords and credit card numbers. Our Office is working closely with Industry Canada and its anti-spam task force to develop ways to tackle this insidious problem, and to help consumers take pro-active measures to protect themselves. Similarly, we will pursue opportunities to protect the privacy rights of consumers in dealing with the potential negative impact of new technologies that pose privacy concerns.

In the coming year, our Office will continue to focus on outreach and communications to help Canadian individuals and businesses to understand their rights and obligations under the *Privacy Act* and *PIPEDA*. We continue to seek input from Canadians in a variety of ways to help us better serve their needs, and to help strengthen the Office of the Privacy Commissioner as a seminal force in protecting and promoting privacy rights.

Above all, I would like to take this opportunity in my first report as Privacy Commissioner to praise the staff of this Office, which has laboured under unprecedented challenges, personally and administratively, to get the work done. I commend them for their professionalism, their dedication to upholding privacy rights for Canadians, for upholding the principles of the Public Service and for their grace under pressure. It has been a difficult year, but, as the saying goes, crisis creates opportunity. I am proud to say this Office has seized the opportunity to rebuild on a stronger foundation, and is confidently moving forward with renewed energy to meet the many privacy challenges ahead.

OVERVIEW

By most measures, the past year was a challenging year for privacy. As threats to privacy proliferated, the fight to protect the privacy rights of Canadians and to protect personal information was at times an uphill battle. The outlook however is not entirely bleak.

Surreptitious surveillance technologies

Every day, we read media stories about new technologies, or new uses of existing technology, that threaten our privacy. Global positioning systems that track the location and movements of vehicles by satellite are being installed in rental cars and in employees' vehicles. Cell phone cameras that can surreptitiously capture and transmit images of people are being used to violate the privacy of individuals. An increasing number of municipalities are considering installing video surveillance cameras in their downtown areas.

During the past year, we have become familiar with the term "radio frequency identification chips" or "RFIDs". These miniature computer circuits outfitted with tiny antennae that vibrate their presence and a unique ID code are getting a lot of attention right now, but they are not new. RFIDs are already being used in a number of ways. For example, the *key chains* issued by gasoline retailers that allow customers to pay for their purchases at the pump contain RFIDs. Now, retailers and governments are proposing to insert these tiny chips in everything from travel documents to paper currency and even items of clothing. Since RFIDs can be read at a distance, this raises a number of privacy concerns.

A retailer may be able to identify you when you walk into the store wearing an RFID-chipped garment. A government may one day be able to monitor the movements of visitors after they enter the country.

Spyware, a new surveillance technology, has replaced "cookies" as the latest Internet privacy villain. Spyware is software that surreptitiously installs itself on your computer and then secretly forwards information about your online activities without your permission or even knowledge. Because spyware can arrive as part of an unsolicited e-mail, you may not know how the programs arrived onto your machine or how to remove them.

Protecting your privacy rights

While these technologies have received a great deal of attention over the past year, the privacy threats they pose can, for the most part, be addressed by applying fair information principles. These principles can be found in *Personal Information Protection and Electronic Documents Act (PIPEDA)* which guides how your personal information can be collected, used and disclosed.

Although there are various ways of expressing these fair information principles, they can be distilled to a few key points:

- Personal information should only be collected, used or disclosed with the individual's knowledge and consent;
- Organizations should only collect as much information as they need;
- Organizations should explain why they are collecting the information and the information should only be used for those purposes;
- Individuals should be able to correct or amend information about themselves; and
- Organizations should have policies and practices governing the collection, use and disclosure of personal information, including destruction policies and procedures to safeguard the information.

While there is no doubt these surveillance technologies have a great potential to invade our privacy and compromise our personal information, there are ways to mitigate their impact. A coalition of consumer privacy and civil liberties organizations has released a position paper on the responsible use of RFIDs; our Office is preparing guidelines on the use of video surveillance by law enforcement agencies; individuals can become more familiar with spyware to protect themselves.

Enhancing security: at what cost?

Ultimately, the enhanced security actions of governments worldwide can pose a more fundamental and troubling challenge to our fundamental rights, including our right to privacy. Recent attempts to make us safer and more secure, both from international terrorism and more traditional public safety threats, raise serious privacy concerns.

Governments throughout the world, including the Government of Canada, continue to introduce measures to increase security based on the premise that if law enforcement and national security agencies have access to enough personal information about all of us we will have a safer, more secure society. In December 2003, the Government of Canada created the Canada Border Services Agency (CBSA), bringing together the border security and intelligence functions of the Canada Customs and Revenue Agency, Citizenship and Immigration Canada and the Canadian Food Inspection Agency. CBSA, in turn, is part of the new Department of Public Safety and Emergency Preparedness, along with the Canadian Security Intelligence Service (CSIS) and the Royal Canadian Mounted Police (RCMP).

In April 2004, the Government of Canada issued its first ever National Security Policy. Among other things, it proposed to create an "Integrated Threat Assessment Centre" to facilitate the collection and analysis of intelligence and other information. According to the policy document, this "will help to reduce the risk that information held by one part of Government will fail to be provided in a timely fashion to those who can utilize it."

The Government of Canada has announced that it will start issuing passports with facial recognition biometric technology in 2005. Although it was never an official government proposal, at least one Cabinet Minister has advocated the introduction of a national identification card.

Redefining borders

A border has become more than simply a river or a line on a map and a series of physical checkpoints. Borders are becoming virtual, posing privacy concerns. As the creation of the CBSA suggests, much of the Government of Canada's national security agenda is focussed on the border. The result is a new concept of what constitutes a border. In December 2001, Canada and the United States signed the "Smart Borders" Declaration. The National Security Policy talks about "building a 21st century border" and "developing a next generation smart borders agenda with the United States and Mexico."

Decisions about who can enter our country or who might pose a threat to security are increasingly being made long before the individuals arrive in Canada. In many cities, travellers flying to the United States can clear United States Customs at a Canadian airport. In the case of cyber-threats, the traditional notion of a border is irrelevant—cyber-attacks can originate from anywhere in the world. Recognizing this, Canada's new national security policy notes that "The Government will also convene a high-level

national task force, with public and private representation, to develop the National Cyber-security Strategy to reduce Canada's vulnerability to cyber-attacks and cyber-accidents."

National borders are becoming less important. The border security policy of the United States is based on the creation of a buffer zone or a "cordon sanitaire" around North America – increasingly, Canadian policies are following suit. Our border security is becoming integrated with U.S. border security. Canada and the United States have created several integrated border enforcement teams. We share watch lists and the Government of Canada has been under pressure to share information with the U.S. government about all people travelling to Canada from abroad.

Smart borders or virtual borders require the collection of personal information—large amounts of personal information. This information is used to verify identity and to determine who should be allowed to enter the country without scrutiny, who needs to be watched and who should be refused entry. This is most evident from looking at various initiatives that have been implemented or proposed in the United States—the Total Information Awareness initiative (renamed Terrorism Information Awareness), the Computer Assisted Passenger Prescreening System (CAPPS II) which has since been abandoned due to privacy concerns, and the US-VISIT program. The Terrorism Information Awareness system is designed to integrate commercial and government databases – allowing access to credit card purchases, travel reservations, telephone records, e-mail records, medical histories, financial information – even public library use.

This emphasis on the collection of large amounts of personal information is also being seen in Canadian initiatives. CBSA is now collecting personal information about all airline passengers arriving in Canada—the Advanced Passenger Information/Passenger Name Record (API/PNR) initiative discussed in previous Annual Reports. Personal information is used in the NEXUS and FAST border-crossing programs to allow pre-approved low-risk travellers and commercial shipments to move back and forth between Canada and the United States.

More information = more security?

Much of the anti-terrorism legislation passed in Canada and abroad is based on the premise that the more information governments have about everyone, regardless of whether they have done anything to incur suspicion, the safer we will be.

We are told that collecting and using this information to identify threats is the price we have to pay to avoid racial and ethnic profiling and a reliance on stereotypes. Risk assessment tools, we are assured, do not recognize colour or religion, they simply analyze information.

As law enforcement and national security organizations collect more information, from more sources, about more individuals, and use that information to identify possible threats, there is an increasing possibility that people will be subjected to unnecessary scrutiny, that people will be wrongly singled out, and that people will be treated unfairly. Mistakes have occurred and will continue to occur. And because of a lack of transparency, we may never know why these individuals were wrongly targeted or where the system broke down.

The Office of the Privacy Commissioner does not think that we should have to choose between two bad options. There has to be a middle ground between racial profiling and collecting more information on everyone and subjecting everyone to increased scrutiny. Our Office is not convinced that reducing the freedoms of all individuals in society will prevent further threats to public safety by terrorists.

Our Office is not opposed to improving security. The question is how to do it in a way that does not destroy the fundamental values of our society. We are not opposed to the sharing of information among agencies, provided there are procedures and policies in place to protect this information, to ensure it is only used or disclosed for specific stated purposes which are reasonable, retained no longer than necessary.

Part of the answer to increasing security may lie in using the information we already have more effectively rather than collecting more information. This message came through very clearly in the Auditor General's March 2004 Report. That Report cites several situations in which Canadian agencies and departments failed to share or use existing information that would have enhanced security. The Report notes, for example, that although more than 25,000 Canadian passports are lost or stolen every year, officials at our borders are not equipped with lists of these lost and stolen documents.

Another troubling feature of the national security measures that are being introduced is the involvement of the private sector. Traditionally, national security has been carried out by government agencies relying primarily on intelligence information collected by these agencies. Increasingly, national security agencies are using personal information collected from individuals by the private sector for purposes unrelated to national security. This data is added to existing intelligence information and private sector expertise is being relied upon to develop the necessary analytical tools.

This raises a number of troubling questions. One set of concerns has surfaced in British Columbia as a result of the proposal that a Canadian subsidiary of an American company take over administration of the province's Medical Services Plan and PharmaCare programs. Critics of this proposal worry that this could potentially allow American

agencies such as the Federal Bureau of Investigation to obtain personal information about Canadians from U.S. companies under the *USA PATRIOT Act*. David Loukidelis, the British Columbia Information and Privacy Commissioner, has launched a public consultation process to examine the issue. Our Office submitted a position paper on the *USA PATRIOT Act* in the context of these public consultations.

Various anti-terrorism measures in the United States involve using private sector databases to confirm identity or to detect patterns of behaviour that might indicate someone poses a threat. Many of these initiatives, such as the Terrorism Information Awareness program, involve "data mining" — the use of database technology and sophisticated algorithms to sift through masses of information in an attempt to find hidden patterns and connections.

The *Public Safety Act*

This blurring of the line between government and the private sector can also be seen in Canada, most notably in the recently passed Bill C-7, the *Public Safety Act*.

Bill C-7 was a highly controversial piece of legislation that took two and a half years and four attempts to pass.

In March 2004, the current Commissioner appeared before the Senate Standing Committee on Transportation and Communications to comment on Bill C-7. Our comments focussed on two aspects of the bill: the amendments to the *Aeronautics Act* authorizing the Commissioner of the RCMP and the Director of CSIS to require air carriers and operators of aviation reservation systems to provide them with information about passengers; and a provision amending *The Personal Information Protection and Electronic Documents Act (PIPEDA)* to allow organizations to collect personal information, without consent, for the purposes of disclosing this information to government, law enforcement and national security agencies.

The RCMP and CSIS will use this passenger information to identify individuals who might pose a threat in terms of transportation safety and national security—purposes directly related to the legislation. However, the information can also be used for the enforcement of arrest warrants for offences punishable by five years or more of imprisonment—a purpose that has no direct connection to the legislation.

The amendment to *PIPEDA* is even more troubling because its implications are potentially far greater. Allowing private sector organizations to collect personal information without

consent for the sole purpose of disclosing this information to government, law enforcement and national security agencies effectively permits these organizations to act as agents of the state. It is one thing to allow an organization to disclose information already in its possession to government agencies without consent; it is quite another to allow – indeed to encourage — a private sector organization to collect this information without consent and then disclose it without consent. The amendment applies to any organization subject to *PIPEDA*, not just air carriers, it does not limit the amount of information that can be collected without consent, and it does not place any limits on the sources of information.

These provisions dangerously blur the line between the private sector and government by enlisting businesses, not only in the fight against terrorism, but in conventional law enforcement.

Despite our opposition, the opposition of several of our provincial and territorial colleagues and the opposition of a large number of other organizations, the Senate passed C-7 and the *Public Safety Act* received Royal Assent in May 2004.

"For every action…"

But for all the challenges this year, we also had reason for cautious optimism. If the threats to our privacy are increasing so too is the interest in defending our privacy.

If we are hearing more about RFIDs, cell phone cameras, event data recorders in cars and video surveillance cameras, it is because the office of the Privacy Commissioner, civil liberties groups, privacy advocates and others charged with protecting privacy are voicing these concerns. And the media are writing about these technologies because they know that the public is interested in privacy.

Opposition from U.S. privacy advocates, the media and politicians from both parties has forced the American government to abandon, scale back or delay a number of anti-terrorism measures. Operation TIPS, a program intended to enlist workers such as cable installers and parcel delivery employees to report suspicious activity was abandoned. The Total Information Awareness Project, which would have allowed the government to utilize "data-mining" to aggregate and analyze public and private commercial database information to track potential terrorists and criminals, never got off the ground. The Computer Assisted Passenger Prescreening System (CAPPS II) program that was supposed to identify foreign terrorists or persons with terrorist connections was abandoned due to privacy concerns.

In Canada, vocal public opposition to a national identification card has, at least for the moment, pushed this proposal onto the back burner. The Office of the Privacy Commissioner of Canada raised serious objections to this idea and we remain opposed.

In September 2003, Robert Marleau, the Interim Privacy Commissioner, appeared before the Standing Committee on Citizenship and Immigration to discuss our Office's opposition to a national identification card. Denis Coderre, the then Minister of Citizenship and Immigration, argued that a national identification card would provide a more secure and reliable proof of identity, help combat identity theft, make it easier for Canadians to travel abroad, and prevent racial profiling at the border.

The Interim Commissioner urged the Committee to reject the proposal on the grounds that:

> "The privacy risks associated with a national identification card are substantial. The challenges of putting in place a national identification system that is workable, affordable, and respectful of the privacy rights of Canadians are enormous. A strong case for the benefits has not been made; to the extent that benefits would exist, they would be marginal at best."

More than 60 witnesses appeared before the Committee. Almost all opposed the introduction of a national identity card. Privacy and human rights groups, consumer lobby groups, religious and ethnic organizations, and major newspapers across the country have also opposed the concept.

We have also seen progress in terms of legislated efforts to protect privacy. We now have an official in every province and territory with a mandate to protect personal information contained in government records. Three provinces—Alberta, Saskatchewan and Manitoba—have laws specifically dealing with the protection of personal health information. Ontario has just passed similar legislation that is scheduled to come into force later in 2004. Quebec, Alberta and British Columbia now have laws in force governing the collection, use and disclosure of personal information in the private sector.

Ultimately the decisions we make now about privacy and whether or not we truly value it will shape the kind of society our children will inherit in the future. As an agency charged with protecting privacy, we must confront those who would trade away individual rights, for the promise of national security or privacy invasive technologies. We must ensure that the high value Canadians place on their privacy rights, is not lost or submerged in the chorus of voices calling for more security, and more information about all of us and work together in the future to meet the challenges that are surely coming our way.

POLICY PERSPECTIVE

One of the key roles of the Office of the Privacy Commissioner is to identify and analyze emerging privacy issues, and develop policies and positions that address them to advance the protection of privacy rights. Our research and analysis of important issues stimulates and informs public debate, engages Canadians and raises awareness. This enables our Office to serve as Parliament's window on privacy issues and to provide timely and knowledgeable advice on the impacts of legislative and regulatory initiatives, and to apprise the public of risks to privacy and ways to respond to them.

Our Office has undertaken a concerted effort to strengthen our relations with Parliament and to better serve its needs. To this end, we have created a new Parliamentary Liaison function specifically dedicated to briefing Members of Parliament and Senators on specific privacy issues, monitoring legislative and regulatory initiatives, and arranging for the Commissioner and senior staff to provide informed advice to Parliamentarians on the privacy implications of emerging law and policy.

In the 2003-2004 reporting period, the Office effectively advocated for the protection of privacy rights on a range of social, technological, and political issues including:

- Identity cards
- Surveillance technologies and video surveillance
- Governmental access to commercial holdings of personal information
- The privacy of personal health information
- Regulating privacy in a federal system

Identity cards

Identity cards have been a long-standing concern for our Office and for privacy and data protection commissioners worldwide. An identity card, and the identity system in which it is embedded, is not simply a convenient tool to confirm the identity of an individual. It is also an information management tool to access, combine, and manipulate personal information. A single card, used as an identifier in a wide variety of transactions with government and the private sector, can be a powerful means of amassing and mining information about an individual, and ultimately tracking and monitoring the individual. It is this power that makes identity cards a threat to privacy.

OPC Position

The Office raised serious objections when the Minister of Citizenship and Immigration proposed a debate on the subject of a national identity card in the fall of 2003.

Our efforts resulted in positive coverage and a number of editorials and columns in major newspapers rallying behind our views on the issues, including an editorial by the *Globe and Mail* on September 22, 2003, commending Interim Privacy Commissioner Robert Marleau's "cogent, thoughtful analysis," of the issue presented to the House Standing Committee on Citizenship and Immigration. Our presentation raised a number of questions, including the considerable risks and costs of setting up a national identification system, and the significant challenge of making it practical, affordable, and respectful of privacy. The advantages of such a system were, in his view, marginal, and overwhelmed by the cost to privacy.

The Office continues to hold this view, and while the proposal for a national identity card appears for the time being to be on the back burner, we remain vigilant.

Surveillance technologies

Technology can threaten privacy and is a growing preoccupation of privacy advocates and privacy commissioners. This is particularly true when increasingly powerful technologies for observing and recording information about people's location, movements, behaviour, and actions are combined with increasingly powerful computers for storing, sorting, mining, and analyzing this information. Think, for instance, of the information that could be collected about you if you drove to a store in your Global Positioning System (GPS) equipped car, used your credit card to pay for a buggy-full of goods individually identifiable by their radio frequency identification tags ("RFIDs"), in a store using video cameras equipped with facial recognition technology. Now imagine all that information about you linked together by a computer, linked with all the other data from your credit card, black box, GPS, RFIDs, and exposure to video cameras, and analyzed for patterns. The example is hypothetical, but it is by no means inconceivable.

OPC Position

This challenge has led the Office to focus on strengthening its capacities for understanding and dealing with new technologies. The Office has also launched a Privacy Lecture series which has brought a number of distinguished guests to speak to staff and interested members of the community on issues of technological change and policy responses. The Office also recently launched a Contributions Program to encourage research projects that focus on the intersection of privacy and technology.

We recognize, however, that the problem is not technology itself, but the failure to control its uses properly. Our basic position with respect to these technologies is that at a minimum their use must be governed by the principles of fair information practices. This approach applies to technologies as varied as smart cards, event data recorders ("black boxes") and RFIDs. People should be told what information is being collected about them, by whom, for what purposes; they should be told what is being done with it and who it is being disclosed to; they should be able to control the collection, use and disclosure of the information through the power of granting or withholding consent; the information should be securely held and treated as confidential; people should have a right of access to their information, and a right to correct it where necessary.

When technologies are used for surveillance, they are subject to an even higher standard. Their deployment and use should be limited to special circumstances where they are justified as a proportionate response to a pressing and substantial problem. Claims that they are justified should be subject to close scrutiny and stringent tests.

Video surveillance

Video surveillance is perhaps the best-known and most obvious example of surveillance technologies. Some people have difficulty articulating or even understanding how they might have a sense of "privacy" in the middle of a public park or walking on a city street, surrounded by other people, and fully visible and audible to them. Yet few people have difficulty understanding that there is something wrong with cameras watching them, perhaps recording their actions, perhaps focusing on them in minute detail, whenever and wherever they go in public. We have not reached that point in Canada – not like the U.K., with its estimated 4 million cameras, one for every 14 residents. But in the course of a typical day, we are repeatedly caught on camera in banks, shopping malls, parking garages, staircases, convenience stores, and, increasingly, in public places such as parks or city streets.

OPC Position

Our Office and most privacy commissioners and privacy advocates are in agreement that video surveillance presents a grave challenge to privacy. It subjects everyone to the scrutiny of police or other authorities, regardless of whether they have done anything to arouse suspicion. At the very least it circumscribes, if it does not eradicate outright, the "shell" of privacy and anonymity that we are entitled to as we go about our law-abiding business. There are good reasons to suspect that video surveillance has a chilling effect on behaviour.

In 2001, the Office investigated a complaint regarding the RCMP's video surveillance of a public park in Kelowna. The conclusion of the investigation was that this surveillance was not justified. This led to protracted discussions with the RCMP, which insisted on continuing the system, although it did agree to stop recording and use the system simply for monitoring. An attempt to have the question addressed in court became mired in procedural issues, and in July 2003 the Office took the decision to withdraw the case. Meanwhile, municipal police forces in a significant number of major Canadian cities indicated an interest in installing public video surveillance systems, and in some cases moved forward with them.

Shortly after taking office, the current Commissioner decided on an enhanced approach to this issue, and developed guidelines for the use of video surveillance by public authorities. These guidelines set out principles for evaluating the necessity of resorting to video surveillance and for ensuring that, if it is conducted, it is done so in a way that minimizes the impact on privacy. So, for example, video surveillance should only be a response to a real and pressing problem, where less-privacy invasive methods will not suffice; video surveillance systems should be designed to have the least possible impact on privacy, running for limited periods and avoiding capturing images of areas such as office or apartment interiors where people have an even greater expectation of privacy.

Government access to commercial holdings of personal information

Another matter of concern to our Office, privacy advocates and commissioners is access by law enforcement and national security agencies to personal information collected by private sector organizations. Many people object to the private sector collecting information about them specifically because they worry about it finding its way into governmental hands.

There can be times when this collection is legitimate, but without controls and oversight, it can tip over into what is in effect deputizing private sector organizations as law enforcement agents, and commandeering personal information that they have collected from individuals for entirely different reasons, in violation of the most basic fair information practices.

OPC Position

The Office's concern about this came to a head in 2003 over the issue of the requirements for airlines to disclose personal information about passengers – including their itinerary, companions, method of payment for tickets, contact addresses and telephone numbers, and even dietary and health-related requirements – to what was

then the Canada Customs and Revenue Agency, so that customs and immigration agents could assess security risks that they might present. While that specific issue was partially resolved with a compromise agreed to between our Office and the CCRA, the larger issue of access by security agencies to the personal information of passengers is still present.

The *Public Safety Act, 2002* which received Royal Assent on May 6, 2004, (shortly after the end of our reporting period) allows the RCMP and CSIS to use passenger information provided by air carriers and operators of aviation reservation systems to identify not just individuals who might pose a threat to transportation safety and national security, but any individual named in an arrest warrant for an offence punishable by five years or more of imprisonment. Moreover, the *Act* amends *PIPEDA* to allow private sector organizations to collect personal information, without consent, for the purposes of disclosing this information to government, law enforcement and national security agencies – effectively permitting these organizations to act as agents of the state, and not only in the fight against terrorism, but in conventional law enforcement.

It was for this reason that the current Commissioner appeared in March 2004 before the Senate Committee charged with examining the proposed law, and raised her concerns. Although Parliament chose to pass the law in spite of opposition from our Office and other privacy advocates, it has not lessened our concern about the issue.

The privacy of personal health information

The application of *PIPEDA* to personal health information is something that was troubling to many in the health care sector even before *PIPEDA* was passed, and it was partly in the interest of resolving uncertainties around the issue that Parliament chose to exempt personal health information from the coverage of the *Act* for the first year after it was passed.

By 2003, various health care sector groups, along with provincial and territorial ministries of health, were looking with increasing apprehension at the looming January 2004 expansion of *PIPEDA*'s scope to all commercial activity. They expressed renewed concern about the impact of the *Act* on the health care sector, and some parties formally asked for an amendment to the *Act* to either "carve out" health information from it or delay the scheduled next phase of its implementation.

Physician's offices, and the offices of other health care providers such as dentists and chiropractors, are engaged in commercial activity. Thus, the personal information that they

collect, use and disclose is subject to *PIPEDA*. The *Act* does not extend to the core activities of hospitals – that is, patient care. This is clearly something within the jurisdiction of the provinces (although *PIPEDA* would apply to clearly commercial peripheral activities, such as a parking lot operated by the hospital if it collected personal information).

OPC Position

The Office's position is that *PIPEDA* is a quite workable instrument to protect personal health information, without imposing an unreasonable burden on health care providers. Overall, the traditional doctor-patient relationship will not have to change significantly. While patient consent to the collection, use, and disclosure of their personal information has to be based on knowledge, this does not mean that doctors must hold conversations with every patient. Patient understanding can be achieved through notices, posters, brochures, and information on the forms people typically fill out when providing a medical history.

Moreover, there are many uses or disclosures that a patient would reasonably expect for care and treatment – for example, disclosures from a general practitioner to a specialist or laboratory, or between a physician and a pharmacist in discussing a prescription. For these reasonably expected uses and disclosures of a patient's personal information, health care providers can rely on implied consent, as long as it is based on a general understanding of how personal information will be used and disclosed. More explicit consent would be necessary for uses or disclosures that a patient would not reasonably expect. The disclosure of information for research purposes is one such example.

In order to address concerns, and to promote this common-sense view of the way *PIPEDA* will work, our Office has joined Health Canada, Industry Canada, and the Department of Justice Canada in an interdepartmental working group to develop communications tools and guidance, respond to questions, and to meet with health care associations to address their concerns and explain our position.

We have noted that not all of the health care sector foresees significant problems complying with *PIPEDA*. For example, the Royal College of Dental Surgeons of Ontario has developed an excellent compliance package that it has distributed to every dentist's office in Ontario.

Regulating privacy in a Federal system

In a modern economy, where personal information flows back and forth across territorial boundaries – where, for example, information about customers in Madrid of a company based in Montreal can be processed in Berlin and stored in Vancouver – privacy protection

has to be seamless and harmonized. Individuals need protection of their personal data, and rights with respect to it, regardless of what jurisdiction it travels to.

That is a complicated task internationally, one that requires constant negotiation and adjustment. But even when the personal information never leaves the country it is a challenge in a federal system like Canada's, with its varying jurisdictional responsibilities. The year in review marked a number of important developments in the movement towards full, harmonized privacy protection in Canada.

In October, 2003, the B.C. government passed its *Personal Information Protection Act* to apply to private sector commercial activity. Alberta followed in December, 2003, with an identically-named and very similar statute. On January 1, 2004, *PIPEDA* came fully into effect, extending to cover commercial activities throughout Canada except where substantially similar provincial legislation applies. Quebec's *An Act Respecting the Protection of Personal Information in the Private Sector* had already been declared substantially similar by the Governor in Council in November 2003; as we go to print, similar declarations are expected with respect to the B.C. and Alberta laws.

OPC Position

The "substantially similar" provision in *PIPEDA* ensures consistent levels of privacy protection in all sectors of the economy throughout the country, but it does not make problems magically vanish. Harmonized privacy protection has its own special challenges.

Conscious of this, federal and provincial privacy commissioners and staff have worked together to help businesses understand which law applies to them, and helped individuals understand their rights, and how to seek redress under the appropriate law. The Offices of the B.C. and Alberta Information and Privacy Commissioners have jointly released a guide (available on their websites, and linked to from ours) to help businesses and individuals sort through what can be an initially confusing picture. This complements the work done by our Office in making available various materials, such as a video streaming speech by the Commissioner, and an E-kit for businesses, that help to ease the implementation of *PIPEDA*.

In an increasingly connected and technologically sophisticated world, potential new threats to the privacy of our personal information seem to arise daily – if not by the minute. As we look ahead, our Office is dedicated to fostering a clear understanding of emerging privacy issues for Parliamentarians, the public and lawmakers, and to continue providing a cogent analysis of national and international privacy risks and challenges as they evolve.

SUBSTANTIALLY SIMILAR PROVINCIAL LEGISLATION

Under the *Personal Information Protection and Electronic Documents Act (PIPEDA)*, the Governor in Council can issue an Order exempting an organization, a class of organizations, an activity or a class of activities from the application of *PIPEDA* with respect to the collection, use or disclosure of personal information that occurs within a province that has passed legislation that is substantially similar to *PIPEDA*.

The intent of this provision is to allow provinces and territories to regulate the personal information management practices of organizations operating within their borders, provided that they have passed a law that is substantially similar to *PIPEDA*.

If an Order is issued, *PIPEDA* will not apply to the collection, use or disclosure of personal information by organizations subject to the provincial act. Personal information that flows across provincial or national borders will continue to be subject to *PIPEDA* and the *Act* will continue to apply within a province to the activities of federal works, undertakings and businesses that are under federal jurisdiction such as banks, airlines, and broadcasting and telecommunications companies.

Process for assessing provincial and territorial legislation

On September 22, 2001, Industry Canada published a notice setting out the process that the department will follow for determining whether provincial/territorial legislation will be deemed substantially similar.

The process will be triggered by a province, territory or organization 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 designated as substantially similar.

The Minister has stated that he will seek the Privacy Commissioner's views on whether or not legislation is substantially similar and include the Commissioner's views in the submission to the Governor in Council. The process also provides for an opportunity for the public and interested parties to comment on the legislation in question.

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

- incorporate the ten principles in Schedule 1 of the *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.

Provincial and territorial legislation passed to date

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

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 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, other than federal works, undertaking or businesses, from the application of *PIPEDA*.

In the spring of 2003, the provinces of British Columbia and Alberta introduced similar legislation, Bills 38 and Bill 44 respectively. The two Bills were passed by their respective legislatures and they both came into force on January 1, 2004.

The two laws — both called the *Personal Information Protection Act* — are similar to *PIPEDA*, but they are not identical. The application of the two provincial *Acts* is broader. Unlike *PIPEDA*, they apply to all organizations, with a few exceptions, not just those that are engaged in commercial activities. They also differ from *PIPEDA* in that they contain different rules for employee personal information than for other personal information. As well, the *Acts* give the two provincial commissioners authority to issue orders, for example, to require an organization to give an individual access to his or her personal information or to require an organization to cease collecting, using or disclosing certain personal information. By comparison, the Privacy Commissioner of Canada does not have order-making powers.

Using the criteria set out in the 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 have concluded that, on balance, the British Columbia and Alberta *Acts* are substantially similar to *PIPEDA*.

The other legislative initiative of note was the introduction and passage of Ontario's Bill 31, the *Health Information Protection Act*. The *Act* received Royal Assent on May 20, 2004 and is scheduled to come into force on November 1, 2004. We are still reviewing the *Act* and we are not yet in a position to comment on whether or not we consider it to be substantially similar to *PIPEDA*.

PART ONE

Report on the *Privacy Act*

INTRODUCTION

The *Privacy Act* has been in force in Canada since 1983, protecting the personal information of individuals held by institutions of the federal government. The *Act* governs the collection, use, disclosure, retention and disposal of personal information by federal government departments and agencies. It gives individuals the right to request access to and correction of their government-held personal information. The *Act* also sets out the duties, responsibilities and mandate of the Privacy Commissioner of Canada.

The Commissioner receives and investigates complaints from individuals who believe their *Privacy Act* rights have been violated. The Commissioner may herself initiate a complaint and investigation in any situation where she has reasonable grounds to believe the *Act* has been violated.

The Privacy Commissioner of Canada works as an ombudsman to resolve complaints through mediation, negotiation, and persuasion whenever possible.

However, the *Act* gives the Commissioner broad investigative powers in order to carry out her mandate. She may subpoena witnesses, compel testimony, and enter premises to obtain documents or to conduct interviews. It is an offence under the *Act* to obstruct an investigation. The *Act* does not grant order-making powers to the Commissioner.

However, the Commissioner can and does make recommendations for changes in the information-handling practices of government institutions when necessary. The Commissioner may conduct audits of any federal department or agency at any time, and may recommend changes to any practices that are not in compliance with the *Privacy Act.*

The Commissioner is required to submit an Annual Report to Parliament, detailing the activities of the Office in the previous fiscal year. This Report covers the period from April 1, 2003 to March 31, 2004 for the *Privacy Act*.

INVESTIGATIONS AND INQUIRIES

The Office of the Privacy Commissioner is responsible for investigating complaints received from individuals under section 29 of the *Privacy Act* (and section 11 of the *Personal Information Protection and Electronic Documents Act*, known as *PIPEDA*)

Investigations serve to establish whether individuals have had their privacy rights violated and whether they have been accorded their rights of access to their personal information. Where privacy or access rights have been violated, the investigation process seeks to provide redress for individuals and prevent violations from reoccurring.

Last year the Office received 4,206 new complaints – an all-time record representing a 250 per cent increase over last year. There were several contributing factors:

- 472 members of Canada's aboriginal communities complained that they were required by Health Canada to sign a broadly worded consent form in order to receive government-funded health benefits;

- 608 correctional officers lodged more than 1,100 complaints against Correctional Service Canada (CSC) for refusing to give them copies of their employee personnel files;

- 107 employees at the Joyceville Institution complained that CSC failed to protect their personal information, after learning that a list containing their home addresses and phone numbers had been found amongst the inmate population; and,

- 38 offenders in British Columbia filed a total of 950 complaints against CSC for not providing timely responses to requests for their personal information held in the 25 standard personal information banks CSC maintains on offenders.

It was also a record year in terms of productivity with investigators concluding 3,134 complaints.

Complaints under the *Privacy Act*

It was also a record year in terms of productivity with investigators concluding 3134 complaints. Although we did close 3483 cases last year, 2323 of these represented investigative work done two years earlier. This year's statistics represent active investigative work completed in 2003/2004. They were concluded as follows:

Not well-founded	1,243
Well-founded	1,180
Well-founded/resolved	69
Resolved	11
Settled	265
Discontinued	366

Definitions of findings under the *Privacy Act*

Not Well-founded: This finding means that the investigation uncovered no or insufficient evidence to conclude that the government institution violated the complainant's rights under the *Privacy Act*.

Well-founded: This finding means that the government institution failed to respect the *Privacy Act* rights of an individual.

Well-founded/Resolved: This finding means that the allegations are substantiated by the investigation, and the government institution has agreed to take corrective measures to rectify the problem.

Resolved: This finding is used for those complaints where *well-founded* would be too harsh to fit what essentially is a miscommunication or misunderstanding. It means that this Office, after a full and thorough investigation, has helped negotiate a solution that satisfies all parties.

Settled during the course of the investigation: This disposition is used when 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 was terminated before all the allegations were fully investigated. A case may be *discontinued* for any number of reasons – for instance, the complainant may no longer be interested in pursuing the matter or cannot be located to provide additional information critical to reaching a conclusion.

Early resolution: This is a new type of disposition, which the Office will begin using in April 2004. It will be applied to situations where the issue is dealt with before a formal

investigation is undertaken. For example, if an individual lodges a complaint about an issue that the Office has already investigated and found to be compliant with the *Privacy Act*, we would explain this to the individual. We also receive complaints where proceeding with a formal investigation could have adverse implications for the individual, which are discussed at length with the individual. In these situations, where the individual chooses to not proceed further, the file is closed as "*early resolution*".

Select cases under the *Privacy Act*

HEALTH CARE

Health Canada's Non-Insured Health Benefits Program

Overview

In the summer of 2003 the OPC received several hundred complaints, as well as numerous inquiries, about Health Canada's decision to require First Nations and Inuit recipients of certain government-funded health benefits to sign a consent form endorsing the department's practices with regard to the collection, use, and disclosure of their personal information. The complainants objected to the complex language of the form, its broad scope, and the lack of adequate measures to protect personal information held by third-party service providers.

Several aboriginal associations, including the Assembly of First Nations and the Inuit Tapiriit Kanatami, supported the complaints and made representations on behalf of their membership.

The impetus for the campaign was a recommendation from the Auditor General that Health Canada improve its tracking mechanisms to prevent the misuse of prescribed drugs. Health Canada also worked to respect the right of benefit recipients to be fully informed about the possible consequences of a drug utilization review.

The complainants felt that the program benefits were and had always been a matter of treaty rights, and that they had no real choice but to agree to review practices that Health Canada was now planning to impose or lose their benefit coverage. They objected to the complex language of the form, its broad scope, and the lack of adequate measures to protect personal information held by third-party providers.

Actions taken by the OPC

We accepted the complaints under the provisions of the *Privacy Act*, and subsequently determined that there was no infringement of a provision of that *Act*. However, our Office continued to work with the aboriginal associations and the department to craft a new approach to the consent initiative that would address privacy concerns. We jointly identified the critical points in the health benefits program requiring fully informed consent of recipients. In addition, we agreed that the privacy provisions of the contracts with third-party providers needed to be strengthened, and Health Canada committed to do so. We also agreed the language of the consent forms needed to be as simple and clear as possible.

Outcome of OPC Actions

Health Canada subsequently proposed an alternative approach to the consent initiative, one that has been supported by aboriginal stakeholders. The approach is as follows:

- the department will continue to promote consent as a matter of best practice (a position that our Office endorses), but will no longer require that everyone sign a form;

- it will implement a mechanism to obtain the express consent of benefit recipients where there are patient safety issues or concerns that the program is being used inappropriately;

- it has established a Health Canada/ First Nations Drug Utilization Review Committee, composed of licensed health care professionals, experts in drug use evaluation, Aboriginal health issues and drug utilization;

- it is developing a Privacy Code that sets out the program's collection, use and disclosure practices. The Code meets the higher standard of consent embedded in the *Personal Information Protection and Electronic Documents Act*, as many of the third-party providers associated with Health Canada's program are subject to that *Act*.

Our Office has offered continuing support to achieve an appropriate balance between the privacy interests of benefit recipients, and the program imperatives of Health Canada.

RCMP medical questionnaire too intrusive for civilian applicants

Overview

A woman was denied a civilian telecommunications officer position with the RCMP after refusing to answer certain questions posed on a medical history questionnaire she was asked to complete during the recruitment process. The questions included:

- "*Do you have monthly menstrual periods?*"
- *"What was the date of your last period?"*
- *"Are your menstrual periods painful?"*
- *"When was your last Pap smear test?"*
- *"How many times, including abortion and miscarriage have you been pregnant?"*

Candidates were also asked if they had varicose veins, arthritis, phlebitis, hay fever, venereal disease, and whether any of their family members had diabetes, cancer, high blood pressure, tuberculosis or heart disease.

Actions taken by the OPC

We established that the woman was required to submit to the same testing process as a candidate applying to be a police officer. The RCMP, however, could not demonstrate how such questions were relevant to a civilian desk job. We concluded that the complaint was well-founded.

Outcome of OPC Actions

Following discussions with the RCMP, its Health Services officials agreed to suspend the use of this questionnaire for civilian candidates. It has undertaken to create a new form specifically for telecommunications officer candidates and geared to the medical requirements of the job, such as hearing, upper body movement, and diseases that could affect cognitive thinking and speech recognition.

While the woman also objected to having to undergo a psychological assessment, the RCMP explained to our satisfaction that telecommunications officers are often the only lifeline between victims and the police officers handling emergency calls. The RCMP therefore needs to ensure that candidates are able to withstand the pressures of the job and deal comfortably with the situations they encounter. Collection of personal information to assess candidates' ability to deal with those stresses is therefore reasonable and appropriate.

SURVEILLANCE TECHNOLOGIES

Video surveillance cameras at Nanaimo Harbour Front scaled back

Overview

A British Columbia resident, aware of the former Commissioner's position on video surveillance on the streets of Kelowna, lodged a complaint about the Nanaimo Port Authority's plans to install video surveillance cameras within its Harbour Front.

The Port Authority provides, among other things, mooring facilities for a fee. The customers paying for this service expect the Port Authority to protect their property. Several customer complaints about vandalism and thefts from vessels prompted the Port Authority to consider installing cameras on its piers. Other areas of the property were also earmarked for surveillance – the Port Authority's offices, the parking lots, a boardwalk, the laundry facilities, and the area where fishers and other boat owners deposit pollutants from their vessels that could endanger the environment.

Actions taken by the OPC

While we did not object to the cameras installed in most of these areas for security purposes, we had concerns about monitoring activities along the publicly accessible boardwalk.

Outcome of OPC Actions

The Port Authority's officials readily agreed to move the cameras away from that area. It also agreed to post signs alerting the public of the presence of surveillance cameras at the Harbour Front.

The investigation helped the Port Authority put safeguards in place to ensure that data collected by the cameras is adequately protected, that it is retained no longer than necessary, and that access and disclosure of the information is closely restricted. Given the Port Authority's willingness to address our concerns, the complaint was deemed resolved.

A different kind of fishing expedition?

Overview

The Office received two complaints about the Fisheries and Oceans Canada Observer Program that requires fishers as a condition of their licence, to allow an observer to stay

on board their commercial fishing vessels, including during the evening and overnight hours, and during non-fishing hours. Some fishers have only family members on board, and their vessels are too small to accommodate a stranger. One of the complaints also concerned the intrusiveness of an alternative to having the observer on board – electronic monitoring by use of video cameras and global positioning systems.

Actions taken by the OPC

The investigation established that the Observer Program is authorized by regulation. Observers' duties are to monitor fishing activities by, among other things, examining and measuring fishing gear, verifying the weight and species of fish caught, inspecting fishing records and conducting biological samplings of fish. The only personal information observers would normally collect include the names, addresses and contact numbers of vessel personnel. All of the remaining information collected relates to the fishing activities under observation.

While having a stranger on board vessels is intrusive by nature, the issue is one of "personal" privacy, which does not fall under the *Privacy Act*, rather than one of protection of personal information.

Outcome of OPC Actions

The Office concluded the complaints were not well-founded. Although the complaints were not well-founded, we discussed the complainants' concerns with Fisheries and Oceans Canada officials who maintained that the department must retain the ability to monitor the fishery. However, they agreed to consult the fishing industry, and we encouraged them to recommend other less intrusive options to carry out this program activity.

HANDLING OF PERSONAL INFORMATION

Where were you born?

Overview

An individual complained that the practice of the Department of Foreign Affairs and International Trade of displaying a passport holder's place of birth on the passport was discriminatory and violated individual privacy.

Actions taken by the OPC

Our investigation determined that more than 85 countries require that the place of birth be indicated on the passport before entry is permitted. Foreign Affairs officials

indicated that when negotiating reciprocal visa-waiving agreements, the place of birth on the passport is often a condition stipulated by other countries. The International Civil Aviation Organization also recommends including place of birth on travel documents.

Nevertheless, passport holders have had the option of having this information displayed or not since 1986. Those choosing to have it excluded must sign statements that they were informed they might encounter difficulties at border points, such as additional questioning by customs officers, the requirement to obtain a visa, or even denial of entry.

Outcome of OPC Actions

We concluded that the complaint was not well-founded.

Correspondence to CRTC posted on Web site

Overview

An individual wrote to the Canadian Radio-television & Telecommunications Commission (CRTC) supporting the licence application of a cultural broadcasting company.

The CRTC posted the individual's correspondence on its Web site exactly as it had been received, including her name, address, phone number and e-mail address. This practice is explained on the Web site, but unfortunately the individual had not noticed this and had no idea that her correspondence would be published in this fashion. She was also not aware that she could ask the CRTC to remove personal identifiers before the correspondence was posted.

When the individual learned that her personal information was on the Web site, she immediately asked that it be removed. The CRTC complied within 48 hours. However, in the meantime, the search engine Google (and possibly others) had picked up the data. When the individual's name was "Googled," her original correspondence to the CRTC would come up.

The individual contacted Google requesting that it too remove her personal information. It replied that it would not do so without a formal request from the webmaster of the site that originally posted the information on the Internet. The individual forwarded her correspondence to the CRTC for appropriate follow-up action, but her personal information remained on the Internet.

Actions taken by the OPC

Following our Office's intervention, the CRTC's webmaster made three requests to Google. None of these requests received a formal response. However, Google did eventually remove the individual's personal information – to her relief and satisfaction.

Outcome of OPC Actions

We closed the file as "settled during the course of investigation."

Taxpayers must comply with Canada Revenue Agency demands for information

Overview – Case One

Two cases the Office investigated last year illustrate the Canada Revenue Agency's (CRA's) authority to require taxpayers to provide very private information.

In the first case, during a routine audit of an Ontario man's 2001 tax return, the CRA asked him to provide a copy of the separation agreement with his former spouse to substantiate the amounts he claimed as child support payments. Although he agreed to provide those portions of the separation agreement that dealt specifically with the payments, he objected to the CRA's insistence that it be given a complete unsevered copy.

Overview – Case Two

In the second case, a Quebec woman complained about the detailed questions posed by a CRA officer attempting to collect an outstanding tax debt. She had been unable to pay the full amount of her tax debt within a reasonable period and requested an extended payment arrangement.

Actions taken by the OPC

Following our investigation of the first case, we explained to the complainant that the CRA had the legal authority under the *Income Tax Act* to demand this information in order to satisfy itself that there were no other clauses in the agreement about child support that might have an impact on his tax situation.

In the second case, we determined that the CRA tries in such cases to reach a mutually acceptable payment schedule with tax debtors based on their financial situation. This requires the individual to make full disclosure of his/her income and his/her monthly expenses as well as assets and liabilities. If an acceptable arrangement is not reached, the CRA may take legal action to recover the debt, including seizing and selling the debtor's assets.

Outcome of OPC Actions

In the first case, in an effort to limit the privacy intrusion, the CRA agreed to keep for its records only those portions of the agreement pertinent to the man's child support payments that it needed to determine his entitlements. The man was pleased with the compromise, and the case was closed as "settled during the course of investigation."

In the case at hand, the CRA officer questioned the woman's expenses for costly prescription drugs to deal with her medical condition, which she claimed precluded her from making significant advances in reducing the debt. The officer asked the woman to obtain a note from her treating physician confirming her condition, which would be factored into the CRA's assessment of her monthly expenses. The complainant accepted our explanations about the CRA's rationale for such an unusual request and the implications should she not comply. The file was closed as "settled during the course of investigation."

Incidents under the *Privacy Act*

Incidents of mismanagement of personal information that warrant further review are brought to the attention of our Office. We conducted 30 such reviews last year. Of note, seven of the incidents related to clients of government departments receiving another client's personal information in error.

Health Identification Cards forwarded to wrong address

In one such case, Veterans Affairs Canada (VAC) was in the process of re-issuing approximately 143,000 client health identification cards with a new National Contact Centre toll-free number. A corrupted data file used during production assigned to about 12,000 clients in Ontario contained the addresses of other clients and before the error was detected, the new cards were incorrectly forwarded to the wrong addresses. VAC officials told us that as soon as they learned about the problem, they immediately halted production until enhanced quality control procedures were implemented. The department contacted all the clients affected by the error.

Misdirected passports

The Office also reviewed two instances of misdirected passports. In one case, an Alberta man received an envelope from the Passport Office containing the passport, birth certificate, credit card information and driver's licence of a woman from Quebec, along with his own documents. In the second case, a Canadian citizen living in Colorado, USA, was mistakenly sent the passport, green card, birth certificate and credit card number

belonging to woman living in Wisconsin, USA. The Wisconsin resident received the documents belonging to the Colorado woman. We determined that human error was the contributing factor in both cases; the passports were prepared and mailed on the same day, along with several thousand others.

With that many mailings in one day, mistakes in stuffing envelopes can happen. The Passport Office indicated that in the six-month time frame between incidents, it had processed in excess of 500,000 applications. The increased volume was a result of additional security procedures and travel restrictions put in place internationally after the events of 9/11. Since enhancements to the mailing procedures were implemented in January 2004, neither the Passport Office nor this Office has received further complaints about misdirected passport documentation.

Stolen computers raise privacy concerns

In another case, six computers were stolen from the CRA's Laval, Quebec tax services office. One of the computers was being used to test computer applications. It was password protected, and contained approximately two million records from four confidential databases. These databases contained personal information, but not tax return information. More than 120,000 affected individuals were advised of the security breach, and given tips on what to do to reduce the possibility of identity theft, such as:

- review and verify all bank account, credit card and other financial transaction statements;
- report any problems/delays with mail delivery to Canada Post;
- report to Human Resources and Skills Development Canada any suspicion about use of the social insurance number (SIN); and
- contact a credit reporting agency such as Equifax or Trans-Union, which are experienced in helping individuals in such matters.

Sixteen individuals later lodged formal complaints with our Office, alleging that the CRA had not adequately protected their information. The CRA indicated that as a result of a lapse in security procedures, the computer had not been stored in a secure room at the end of the day. Appropriate disciplinary action, consistent with CRA policies, was taken.

Public interest disclosures under the *Privacy Act*

Paragraph 8(2)(m) of the *Privacy Act* gives heads of government institutions the discretion to disclose personal information without the individual's consent where the disclosure

would benefit the individual or where there is a compelling public interest that outweighs the invasion of the individual's privacy. Under subsection 8(5), the head of the institution is required to notify the Privacy Commissioner of such disclosures, preferably in advance unless there is some urgency that dictates otherwise.

Last year we received 67 such notices. Correctional Service Canada (CSC) topped the list with 20 notices, most of them related to the disclosure of personal information about offenders who died in custody. CSC routinely relies on the public interest provisions of the *Privacy Act* to share information with family members wanting access to the reports prepared by CSC staff who reviewed the circumstances surrounding the offender's death.

The RCMP sent 15 notices of impending public interest disclosures. Most of these concerned individuals released from custody at the end of their sentences who were considered at high risk to re-offend. The RCMP intended to issue press releases in communities where the offender planned to live to alert residents of the individual's presence and of specific conditions attached to the individual's release. For example, such a condition might bar the offender from school grounds, parks or playgrounds or the company of under-age children.

National Defence sent nine notices. Seven concerned sharing information with family members following the death of a Canadian Forces member.

The remaining notices came from Transport Canada, Public Works & Government Services Canada, Agriculture & Agri-Food Canada, Health Canada, Indian & Northern Affairs Canada, the Immigration & Refugee Board, the Treasury Board Secretariat, Solicitor General Canada, the Office of the Auditor General of Canada, the Public Service Commission of Canada, the Ombudsman for National Defence/Canadian Forces, the Commission for Public Complaints against the RCMP, CSIS and the National Parole Board.

Inquiries

The Office responds to thousands of inquiries from the general public seeking advice and assistance on a wide variety of privacy-related issues dealing with federal government institutions.

The most common inquiry our Office received during the 2003/2004 year about the *Privacy Act* regarded accessing personal information held by a federal department. These inquiries were made by federal employees and citizens alike. Inquirers were also concerned about how well certain federal departments were protecting their personal information.

Inquiry statistics

(April 1 2003 to March 30, 2004)

Telephone inquiries received	2,580
Written inquiries received (letter, e-mail and fax)	2,148
Total number of inquiries received	4,728

Top ten departments by complaints received

For the year ending March 31, 2004

Organization	Total	Access to Personal Information	Time	Privacy	Other
Correctional Service of Canada	2,760	1,235	1,335	190	
Health Canada	485	2	3	480	
Canada Customs and Revenue Agency	255	103	72	80	
Citizenship and Immigration Canada	132	48	75	9	
Royal Canadian Mounted Police	129	78	34	17	
National Defence	80	32	17	31	
Canada Post Corporation	72	13	24	35	
Human Resources Development Canada	65	21	10	34	
Justice Canada	23	8	10	5	
Foreign Affairs and International Trade	22	4	10	8	
Others	183	91	39	53	
Total	**4,206**	**1,635**	**1,629**	**942**	**0**

Complaints received by complaint type

For Complaints Received between 01/04/2003 and 31/03/2004

Complaint Type	Count
Access	1,612
Collection	535
Correction – Notation	20
Correction – Time Limits	27
Extension Notice	28
Inappropriate Fees	1
Language	2
Retention and Disposal	17
Time Limits	1,574
Use and Disclosure	390
Total	**4,206**

Complaints received by respondent

For Complaints Received from: 01/04/2003 to 31/03/2004

Agriculture & Agri-food Canada	8
Auditor General of Canada, Office of	1
Bank of Canada	1
Business Development Bank of Canada	1
Canada Revenue Agency	265
Canada Post Corporation	72
Canada Firearms Centre	4
Canadian Food Inspection Agency	4
Canadian Heritage	1
Canadian Human Rights Commission	2
Canadian Museum of Civilization	4
Canadian Radio-Television and Telecommunications Commission	3
Canadian Security Intelligence Service	20
Canadian Space Agency	4
Canadian Tourism Commission	4
Citizenship & Immigration Canada	132
Commissioner of Official Languages, Office of the	1
Correction Investigator Canada, The	5
Correctional Service Canada	2,760
EDULINX Canada Corporation	1

Complaints received by respondent (cont.)

For Complaints Received from: 01/04/2003 to 31/03/2004

Environment Canada	1
Finance Canada, Department of	1
Financial Transactions & Reports Analysis Centre of Canada	1
Fisheries & Oceans	5
Foreign Affairs & International Trade Canada	22
Health Canada	485
Human Resources Development Canada	65
Immigration & Refugee Board	15
Indian & Northern Affairs Canada	2
Industry Canada	2
Justice Canada, Department of	23
Military Police Complaints Commission	5
National Archives of Canada	4
National Defence	80
National Gallery of Canada	1
National Parole Board	19
National Research Council Canada	3
Ombudsman National Defence and Canadian Forces	1
Pension Appeals Board Canada	1
Privy Council Office	5
Public Service Commission Canada	4
Public Works and Government Services Canada	5
Royal Canadian Mint	1
Royal Canadian Mounted Police	129
Solicitor General Canada	8
Statistics Canada	4
Status of Women Canada	2
Transport Canada	10
Treasury Board of Canada Secretariat	5
Veterans Affairs Canada	4
Total	**3,134**

Closed complaints by complaint type

For Complaints Closed between 01/04/2003 and 31/03/2004

Complaint Type	Count
Access	782
Collection	539
Correction – Notation	14
Correction – Time Limits	16
Extension Notice	30
Inappropriate fees	1
Language	2
Retention & Disposal	15
Time Limits	1,511
Use and Disclosure	224
Total	**3,134**

Closed complaints by origin

For complaints closed between 01/04/2003 and 31/03/2004

Province/Territory	Total
Alberta	658
British Columbia	1,128
International	18
Manitoba	65
National Capital Region (ON)	140
National Capital Region (QC)	22
New Brunswick	41
Newfoundland	8
Nova Scotia	27
Nunavut	1
Ontario	315
Prince Edward Island	1
Quebec	560
Saskatchewan	150
Total	**3,134**

Complaints by complaint type and finding

For complaints closed between 01/04/2003 and 31/03/2004

	Discon-tinued	Not well-founded	Resolved	Settled in course of investigation	Well-founded	Well-founded & Resolved	Total
Access	40	477	6	177	19	63	782
Collection	6	503	3	14	12	1	539
Correction – Notation	0	10	0	2	0	2	14
Correction – Time Limits	1	1	0	0	14	0	16
Extension Notice	0	16	0	0	14	0	30
Inappropriate fees	1	0	0	0	0	0	1
Language	0	2	0	0	0	0	2
Retention & Disposal	1	5	0	6	1	2	15
Time Limits	294	140	0	11	1,066	0	1,511
Use & Disclosure	23	89	2	55	54	1	224
Total	366	1,243	11	265	1,180	69	3,134

Closed complaints by respondent

For complaints received from 01/042003 to 31/03/2004

Federal Institution	Total
Agriculture & Agri-food Canada	6
Bank of Canada	1
Business Development Bank of Canada	1
Canada Customs & Revenue Agency	252
Canada Post Corporation	46
Canadian Firearms Centre	3
Canadian Food Inspection Agency	4
Canadian Heritage	3
Canadian Human Rights Commission	1
Canadian International Development Agency	1
Canadian Museum of Civilization	3
Canadian Radio-Television and Telecommunications Commission	4
Canadian Security Intelligence Service	48
Canadian Space Agency	1

Closed complaints by respondent (cont.)

For complaints received from 01/042003 to 31/03/2004

Citizenship & Immigration Canada	92
Commission for Public Complaints Against the RCMP	1
Commissioner of Official Languages, Office of the	1
Communication Canada	1
Correctional Investigator Canada, The	4
Correctional Service Canada	1,636
Environment Canada	6
Finance Canada, Department of	1
Fisheries & Oceans	11
Foreign Affairs and International Trade Canada	16
Health Canada	488
Human Resources Development Canada	51
Immigration & Refugee Board	18
Indian & Northern Affairs Canada	3
Industry Canada	7
Justice Canada, Department of	56
Military Police Complaints Commission	4
Montreal Port Authority	1
Nanaimo Port Authority	1
National Archives of Canada	3
National Defence	109
National Parole Board	23
National Research Council Canada	4
Natural Resources Canada	1
Natural Sciences and Engineering Research Council of Canada	1
Office of the Superintendent of Financial Institutions Canada	2
Ombudsman National Defence & Canadian Forces	1
Privy Council Office	3
Public Service Commission Canada	9
Public Works & Government Services Canada	14
Royal Canadian Mounted Police	164
Solicitor General Canada	11
Statistics Canada	1
Transport Canada	5
Treasury Board Of Canada Secretariat	8
Veterans Affairs Canada	3
Total	**3,134**

Completed investigations and results by respondent

For Complaints Closed between 01/04/2003 and 31/03/2004

Respondent	Discon-tinued	Not Well–founded	Resolved	Settled in course of investiga-tion	Well-founded	Well-founded & Resolved	Total
Agriculture & Agri-food Canada	1	1	0	2	2	0	6
Bank of Canada	0	0	0	1	0	0	1
Business Development Bank of Canada	0	1	0	0	0	0	1
Canada Customs & Revenue Agency	5	94	2	65	60	26	252
Canada Post Corporation	7	14	1	14	7	3	46
Canadian Firearms Centre	0	1	0	2	0	0	3
Canadian Food Inspection Agency	1	2	0	0	1	0	4
Canadian Heritage	0	2	0	1	0	0	3
Canadian Human Rights Commission	0	0	0	0	1	0	1
Canadian International Development Agency	0	1	0	0	0	0	1
Canadian Museum of Civilization	3	0	0	0	0	0	3
Canadian Radio-Television & Telecommunications Commission	0	2	0	2	0	0	4
Canadian Security Intelligence Service	1	43	0	4	0	0	48
Canadian Space Agency	0	0	0	0	1	0	1
Citizenship & Immigration Canada	12	25	0	13	41	1	92
Commission for Public Complaints Against the RCMP	0	1	0	0	0	0	1
Commissioner of Official Languages, Office of the	0	0	0	0	1	0	1

Completed investigations and results by respondent (cont.)

For Complaints Closed between 01/04/2003 and 31/03/2004

Respondent	Discon-tinued	Not Well–founded	Resolved	Settled in course of investiga-tion	Well-founded	Well-founded & Resolved	Total
Communication Canada	0	1	0	0	0	0	1
Correctional Investigator Canada	0	0	0	0	4	0	4
Correctional Service Canada	308	357	2	46	911	12	1,636
Environment Canada	3	1	0	2	0	0	6
Finance Canada, Department of	0	1	0	0	0	0	1
Fisheries & Oceans	2	5	0	3	0	1	11
Foreign Affairs & International Trade Canada	3	6	1	5	1	0	16
Health Canada	0	481	0	4	2	1	488
Human Resources Development Canada	1	25	1	9	9	6	51
Immigration & Refugee Board	0	3	0	1	10	4	18
Indian & Northern Affairs Canada	0	2	0	1	0	0	3
Industry Canada	0	6	0	0	1	0	7
Justice Canada, Department of	0	7	0	41	7	1	56
Military Police Complaints Commission	0	4	0	0	0	0	4
Montreal Port Authority	0	1	0	0	0	0	1
Nanaimo Port Authority	0	0	1	0	0	0	1
National Archives of Canada	0	0	0	1	2	0	3
National Defence	7	21	0	19	52	10	109
National Parole Board	2	19	0	0	2	0	23
National Research Council Canada	1	2	0	0	1	0	4
Natural Resources Canada	0	1	0	0	0	0	1

Completed investigations and results by respondent (cont.)

For Complaints Closed between 01/04/2003 and 31/03/2004

Respondent	Discon-tinued	Not Well–founded	Resolved	Settled in course of investiga-tion	Well-founded	Well-founded & Resolved	Total
Natural Sciences and Engineering Research Council of Canada	0	1	0	0	0	0	1
Office of the Superintendent of Financial Institutions Canada	0	2	0	0	0	0	2
Ombudsman National Defence and Canadian Forces	1	0	0	0	0	0	1
Privy Council Office	0	2	0	0	1	0	3
Public Service Commission of Canada	0	4	0	1	4	0	9
Public Works and Government Services Canada	2	7	0	1	4	0	14
Royal Canadian Mounted Police	4	79	1	25	52	3	164
Solicitor General Canada	0	10	0	1	0	0	11
Statistics Canada	0	1	0	0	0	0	1
Transport Canada	2	2	0	0	0	1	5
Treasury Board of Canada Secretariat	0	4	2	0	2	0	8
Veterans Affairs Canada	0	1	0	0	2	0	3
Total	**366**	**1,243**	**11**	**265**	**1,180**	**69**	**3,134**

PRIVACY PRACTICES AND REVIEWS

The Office of the Privacy Commissioner promotes compliance with Canada's two privacy laws through the conduct of privacy audits and compliance reviews. The Office serves as a source of in-house expertise providing assistance and advice to both public and private sector institutions. With the introduction of the Treasury Board Secretariat's *Privacy*

Impact Assessment (PIA) *Policy* in May 2002, the Office has also assumed responsibility for reviewing and commenting on the PIAs prepared by federal government institutions.

Audits and compliance reviews under the *Privacy Act*

During the past year, the Office conducted Section 37 reviews of the personal information-handling practices of the Canada Industrial Relations Board (CIRB) and the Canadian Forces Grievance Board (CFGB). We selected these two institutions not because of any suspicion of non-compliance with acceptable privacy practices, but rather because they are small institutions which have in the past escaped the kind of scrutiny given to larger government institutions with significant personal information holdings.

The purpose of the CIRB and CFGB reviews was to provide guidance and education on privacy matters. This is particularly important in small institutions, where the resources available to devote to privacy are relatively limited. We looked at the practices surrounding the collection, use, disclosure, protection, retention and disposal of personal information, both in hard copy files and electronic format. We also examined the institutions' public listings in Info Source, contracting-out activities, staff awareness of their rights and obligations under the *Privacy Act*, tele-work arrangements, workplace surveillance and the security issues relating to the electronic transmission of information.

The Canada Industrial Relations Board

The CIRB is the independent, quasi-judicial tribunal which interprets and administers Part 1 (Industrial Relations) and certain provisions of Part II (Occupational Health and Safety) of the *Canada Labour Code*. The Board certifies trades unions, investigates unfair labour practices, orders an end to unlawful strikes and lockouts, decides jurisdictional issues, deals with the complexities of corporate mergers and sales and offers mediation and arbitration services for dispute resolution.

The compliance review was conducted at the CIRB's head office in Ottawa and at its regional offices in Toronto and Vancouver. The review found that the Board's personal information handling practices generally comply with the fair information principles established in sections 4 to 8 of the *Privacy Act*. However, our Office identified several matters requiring remedial attention, including the need to develop policies and protocols regarding the protection of operational files and information contained in portable computers carried outside the physical confines of the CIRB. As well, case files required proper identification according to their respective security designations, and attention was needed to properly dispose of records in accordance with established retention and disposition schedules.

The Canadian Forces Grievance Board

Our examination of the Board's operations revealed a high level of compliance with the *Privacy Act* and its fair information principles. However, the review did remark some forms used by the Board to collect personal information required enhancements to ensure that individuals were informed of the purpose of the collection. The review also indicated the need to establish a policy governing the use of faxes to transmit personal information.

At the end of the reviews, the CIRB and the CFGB were issued reports with our findings. We have recently issued our final reports and are awaiting responses from the CIRB and the CFGB to the recommendations contained therein.

Anti-terrorism survey

In addition to these two audits, our Office followed through with an undertaking, discussed in last year's Annual Report, to assess the impact of anti-terrorism measures adopted in the wake of September 11 2001 on the privacy of Canadians. To this end, we conducted reviews of the Royal Canadian Mounted Police (RCMP), the Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment Service (CSE).

The objectives of the reviews were: to determine what had changed in terms of the legislative authorities and operational programs of the RCMP, CSE and CSIS as a result of the anti-terrorism measures introduced by the Government of Canada under its Anti-Terrorism Plan; to examine any new initiative planned or implemented by the organizations subsequent to September 11, 2001, which would impact on the privacy of Canadians; and to assess the extent to which the management of personal information under the new initiatives are in compliance with the fair information practices enunciated in the *Privacy Act*.

Reviews of CSIS and CSE

With regards to CSIS and the CSE, it should be noted that the scope of the reviews did not include commenting on the broader issues of the Government of Canada's national security or foreign intelligence gathering activities. Rather, the focus was to assess the impact of anti-terrorism measures on the personal information handling practices of these institutions. Our inquiries suggest that the events of September 11, 2001, have not resulted in fundamental changes to the management of personal information held under the control of the CSIS and the CSE. Based on our examination of selected documentation and on the responses of CSIS and CSE officials who were interviewed, no substantive *Privacy Act* issues or concerns were identified.

Reviews of the RCMP

The compliance review at the RCMP involved an examination of three primary initiatives: Integrated National Security Enforcement Teams (INSETs); Integrated Border Enforcement Teams (IBETs); and the creation of the Financial Intelligence Branch. While our review revealed a high degree of compliance with the *Privacy Act*, we did have concerns regarding the agreements or arrangements governing the sharing of personal information between the RCMP and its INSET and IBET partners. The matter has been the subject of ongoing discussions with the RCMP.

Cross-border flow of personal information

On the subject of disclosure, a number of programs and activities established by federal Government institutions and agencies provide for the disclosure of personal information about Canadian citizens and residents to departments and agencies of the United States government. During this fiscal year, the Office completed an examination of agreements, arrangements and memoranda of understanding between Canada and the United States that include provisions for the sharing of personal information. Our review found that many of the sharing agreements were deficient in terms of containing adequate privacy protection provisions.

The cross border flow of personal information raises serious privacy risks relating to the jurisdictional differences affecting the protection of personal information, the security of personal information in transit, and the adequacy of legal instruments governing the management of the information shared. Issues related to the trans-border flow of personal information will be a key area of review for the Office during the next fiscal year. To this end, we are conducting an audit of the trans-border information sharing activities of the newly constituted Canadian Border Services Agency (CBSA).

The Canadian Firearms Program

During the course of the year, we continued close monitoring of the Canadian Firearms Program, which was subject to a review by this Office in 2001. Some of the recommendations we made in 2001 have been implemented. The RCMP, for example, adopted our 2001 recommendations to limit Firearms Officer access to the Police Information Retrieval System (PIRS) system and to operational files. We have also followed up on a number of outstanding issues referred to in our 2001 comprehensive Firearms Report, such as outsourcing, international information sharing agreements and the use of supplementary questionnaires.

One of the difficulties in reviewing the Firearms Program is that it has been very much a moving target due to persistent legislative, policy, administrative and information technology (IT) changes to the Program. In the past year, for example, the Auditor General issued her report on the value for money of the program which recommended changes to it; the program was transferred from the Minister of Justice to the Minister of the Solicitor General (now the Department of Public Security and Emergency Preparedness Canada (PSEPC); a new position of Firearms Commissioner has been created; Bill C-10 was passed by Parliament; and Minister Guarnieri was given the mandate in January 2004 to conduct a full program review.

Some of our observations and findings from the 2001 report, and from our more recent review have been affected by these on-going changes. That said, we have made some significant progress with the Canada Firearms Centre to address the outstanding issues in light of the current state of affairs. We will report on further progress in next year's Annual Report.

Other compliance activities

In addition to compliance audits, our Office also undertakes reviews of submissions from both federal government and private sector organizations and offers advice on a broad range of compliance issues. Some of these compliance review activities are mandated under the *Privacy Act* and the *PIPEDA*, while others are mandated under federal government policy. Other review activities have come about through institutional arrangements involving voluntary consultation with the Office on privacy matters. Human Resources and Skills Development Canada's (HRSDC) - formally the Department of Human Resources Development Canada (HRDC) - *Governance Protocol for the Databank Review Committee* is a case in point.

HRSDC databank review

As described in our earlier reports, HRSDC developed a review procedure to deal with policy analysis, research and evaluation activities involving the linking of separate databanks. Part of this procedure includes consultation with our Office. During the past year, the Office has analyzed and commented on 20 HRSDC submissions, including an evaluation of the Employment Insurance program since the 1996 reforms, the success of various Labour Market Development Agreements and studies relating to the Canada Student Loans Program. Over the course of the last several years we have witnessed a marked improvement in the completeness and quality of the submissions we have received. This is evidence of the seriousness with which HRSDC regards its data linkage activities, and its dedication to ensuring that such linkages are undertaken in accordance with privacy best practice principles.

Policy on Data Matching

Under the Treasury Board Secretariat of Canada's *Policy on Data Matching*, federal government departments and agencies are required to notify the Office of any data matching proposal. The purpose of this notification is to afford the Office an opportunity to review and comment on the proposal so as to ensure that the data matching complies with the requirements of the *Policy*. Over the course of the last fiscal year, our Office received 10 data matching submissions. These submissions complied with the nominal requirements of the *Policy,* though we have found it necessary to remind departments of their duty to inform the public when their personal information is to be matched against other government information holdings. In most cases such notification will not prejudice the use of the information.

Disclosure of personal information to a third party

Pursuant to paragraphs 7(2)(c) and 7(3)(f) of the *PIPEDA,* private sector organizations are required to notify our Office when personal information is to be disclosed to a third party without the consent of the individual for "statistical, scholarly study or research purposes."

Our role is to provide advisory services to a number of federal government departments and to serve as a resource for private sector organizations seeking information on the application of privacy best practice principles to their respective commercial activities.

Organizations must demonstrate in their submissions that; 1) the information contemplated for disclosure will be used solely for "statistical, scholarly study or research purpose; 2) the purpose of the disclosure cannot be achieved without the information being in an identifiable format; 3) obtaining consent from the individuals involved would be "impracticable"; and 4) the disclosing organization has taken such measures as are appropriate to ensure that the information will be used in a manner that preserves its confidentiality.

In the course of the last fiscal year the Office has received 4 notifications under paragraph 7(3)(f) of the *PIPEDA*. Most of these submissions involved the use and disclosure of medical information for health research purposes. These submissions have been of varying levels of completeness and quality. While relying on a very small sample, it is evident that organizations are unsure of their obligations under paragraph 7(3)(f) of the *PIPEDA*. Particularly problematic is the question of when and under what circumstances obtaining consent would be "impracticable." Over the course of the next fiscal year, the Office will commit resources to develop a guide to assist organizations in understanding their obligations under section 7 of the law, and in preparing their submissions to the Office of the Privacy Commissioner.

Other consultation and advisory services

The Office also provides less formal advice, comments, and recommendations to numerous federal departments as needed. Departments aided in this way include the Treasury Board of Canada, Statistics Canada, Health Canada, Human Resources and Skills Development Canada, Indian and Northern Affairs Canada, the Canada Revenue Agency and the Canadian Border Services Agency.

Consultations were undertaken on a wide variety of issues, including

- A Privacy Impact Assessment Audit Guide
- Data matching policies
- Policies for use of the Social Insurance Number (SIN)
- Privacy best practices for departments
- Legislative and policy reform
- Privacy risks of specific programs and initiatives

The Office also assists private sector organizations in assessing privacy risks, instilling best practices and developing appropriate privacy policies.

Privacy Impact Assessments

The Treasury Board Secretariat of Canada's *Policy on Privacy Impact Assessments* (PIA) has now been in effect since May 2002. When first launched, the *Policy* was enthusiastically welcomed by members of the professional privacy community, and with good reason. For the first time federal Government departments and agencies were equipped with a tool that could be used to forecast the impacts on privacy relating to a given initiative, to assess and weigh the impacts in a consistent fashion, and to come up with strategies to mitigate those impacts or risks. By requiring privacy principles to be considered in the planning, design, and implementation phases of a project, the *Policy* helps to give effect to those principles in a way that is tangible and demonstrable.

The *Policy* was the first of its kind to make PIAs mandatory for all new federal government programs or services that raise potential privacy issues. The *Policy* requires that federal government departments and agencies notify the Privacy Commissioner when undertaking a PIA, giving the OPC an opportunity to review and comment on the project. This provides added assurance that risks relating to a given initiative have been properly identified and that mitigating measures proposed to deal with those risks are reasonable and appropriate.

OPC perspective on PIAs

Since the *Policy* came in effect in May 2002, the OPC has received over 100 PIAs and Preliminary Privacy Impact Assessments (PPIA) reports for examination. As could be expected with the launch of any new policy directive, many of the PIA and PPIA submissions we received for review in the first year ranged in completeness and quality. Common errors and omissions we observed with those early submissions were itemized in the Commissioner's Annual Report for fiscal year 2002-2003.

In the course of the last fiscal year, however, we have observed a marked improvement in the completeness and quality of the PIA and PPIAs we have received. We see this improvement as evidence that departments are learning from consultations with our Office. This improvement can also be attributed to the efforts of the Treasury Board Secretariat to educate departments on the requirements and methodologies of the *Policy*. Treasury Board's "PIA e-learning tool" which became available on-line in the fall of 2003, has been a valuable resource. We would encourage anyone interested in learning more about the PIA process to visit Treasury Board's web site at: www.tbs-sct.gc.ca.

Looking ahead

While we have been impressed by the general improvement in the quality of the PIA and PPIA submissions we receive, there is one frequent omission that continues to give us cause for concern. Many PIAs fail to include an action plan to actually address and resolve the privacy risks they identify. Our Office will be working with departments and agencies to encourage the inclusion of such action plans in all PIAs, and to help departments identify the appropriate next steps.

However, there are strong indications that the *Policy* is achieving its primary purpose; that of increasing awareness among government personnel at all levels of the importance of privacy in day-to-day administrative functions. Departments can no longer create new databases, link information holdings, enter into information sharing arrangements with other departments, or launch new programs or services, without considering their potential impact on privacy.

Just as departments have struggled with limited resources to comply with the *Policy's* requirements, so too has the OPC challenged to allocate sufficient resources to effectively perform its advisory role under the *Policy* without supplementary resources.

The reduction of staff available within the OPC to review PIAs and PPIAs, combined with an increase in the volume of submissions over the last fiscal year has led to delays in providing departments with feedback. The OPC is endeavouring to address this resource deficit and we are optimistic that a remedy will be found.

We believe no other government initiative since the enactment of the *Privacy Act* itself has made as significant a contribution to fostering a privacy-sensitive culture within the federal public service.

However, our Office has found it a challenge to perform its advisory role under the PIA Policy without the allocation of supplementary resources. A lack of human and monetary resources for this purpose for this purpose and a great increase in the volume of submissions over the fiscal year has led to unfortunate delays in providing departments with the feedback they need. OPC will continue to press for a resolution to this resource deficit so that we may avoid further delays, clear the current backlog, and adequately support departments in applying the TBS PIA Policy.

IN THE COURTS

Section 41 of the *Privacy Act* allows an individual, following the results of an investigation of a complaint by the Privacy Commissioner, to apply to the Federal Court for review of the decision of a Government institution to refuse the individual access to personal information. From the time the *Privacy Act* came into force in 1983 to March 31, 2004, approximately 141 applications for review have been filed in the Federal Court. Eleven of these were filed in the year ending March 31, 2004.

Section 42 of the *Privacy Act* allows the Commissioner to appear in Federal Court. The Commissioner can apply to the Federal Court for review of the decision of a Government institution to refuse access to personal information, with the consent of the individual who requested the information. The Commissioner can appear before the Court on behalf of an individual who has applied for review under section 41. Or, with leave of the Court, the Commissioner can appear as a party to any review applied for under section 41.

The Commissioner has also intervened on numerous occasions in other litigation arising outside of the *Privacy Act* in which issues involving interpretation of the *Act* were raised.

In last year's annual report we reported on the conclusion of a number of cases in which the Commissioner had been actively involved. In the past fiscal year there has been no significant litigation concerning interpretation of the *Privacy Act* that required the intervention of the Commissioner.

PART TWO

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

INTRODUCTION

The Personal Information Protection and Electronic Documents Act (PIPEDA) sets out ground rules for how private sector organizations may collect, use or disclose personal information in the course of commercial activities.

Since the *Act* took effect on January 1, 2001, it has applied mainly to the commercial activities of what are known as federal works, undertakings or businesses, such as transportation and telecommunications companies, banks and broadcasters. It also applies to the personal information of employees in those companies, and it applied to personal information that is sold, leased, or bartered across provincial or national boundaries by provincially regulated organizations.

As of January 1, 2002, the personal health information collected, used or disclosed by these organizations is also covered.

On January 1, 2004, *PIPEDA* extended to cover the collection, use or disclosure of personal information in the course of all commercial activities in Canada, except in intraprovincial collection, use and disclosure where there is substantially similar legislation.

PIPEDA now also covers all cross border collection, uses and disclosures and federal works, undertakings and businesses.

INVESTIGATIONS AND INQUIRIES

This Office received 302 complaints under *PIPEDA* between January 1 and December 31, 2003, which is approximately the same number as in 2002. As in previous years, complaints were filed against a variety of organizations and dealt with allegations that individuals' privacy rights had been violated. Once again, the largest number of cases, 42%, were filed against organizations in the banking sector; the telecommunications and

broadcasting sector accounted for 26% of cases. The percentage of complaints against transportation companies rose slightly to 19%. Credit reporting agencies accounted for a further 4% of the total, and the remaining 9% involved rewards programs, internet service providers and aboriginal band councils.

The number of cases finalized in 2003 rose to 278, a 58% increase from the previous year. Complaints were concluded as follows:

Not well-founded	115	(41%)
Well-founded	97	(35%)
Resolved	14	(5%)
Settled	4	(2%)
No jurisdiction	5	(2%)
Discontinued	43	(15%)

Definitions of findings under *PIPEDA*

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

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

Resolved: This finding means that the allegations are substantiated by the investigation; however, the organization has taken or has committed to take corrective action to remedy the situation, to the satisfaction of this Office.

Settled during the course of investigation: This disposition is used when 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 was terminated before all the allegations were fully investigated. A case may be discontinued for any number of reasons – for instance, the complainant may no longer be interested in pursuing the matter or cannot be located to provide additional information critical to reaching a conclusion.

No jurisdiction: This means that it has been determined during investigation 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, which the Office will begin using in 2004. It will be applied to situations where the issue is dealt with before a formal investigation is undertaken. For example, if an individual files a complaint about an issue that the Office has already investigated and found to be compliant under *PIPEDA*, we would explain this to the individual. This disposition would also be used when an organization, upon learning of the allegations, addresses the issue immediately and to the satisfaction of the complainant and this Office.

Select cases under *PIPEDA*

SAFEGUARDING OF PERSONAL INFORMATION

Wedding bell blues

Overview

She was only trying to be helpful. That is what the bank employee in this case undoubtedly believed when she gave the fiancée of a customer a copy of his student loan application, containing information about his loans and credit card, from the previous year. She thought it could assist him in filling out another form for the new school term. She also probably thought it was not a big deal to leave his banking file out on her desk, where the fiancée could see it, while she went to search for a document.

It was, in the end, a very big deal. The young woman knew that her boyfriend had a student loan, but she did not know the full amount of his debt – until she saw it in the file. As a result, she called the wedding off.

The employee acknowledged her error. She thought the fiancée was acting as the boyfriend's agent because the woman, who had attended the bank to drop off some documents for him, referred to herself as his "go-between." The employee stated that in the future, she would ensure that she had a signed document indicating that someone was acting on another's behalf before discussing any personal information.

Actions taken by the OPC

We noted that despite the "go-between" comment, the bank employee did not have the student's authorization in writing, contrary to the bank's own policy. Without documentary evidence that the student authorized the disclosure, we found that the bank had contravened the requirement for consent under the *Act*, and concluded that the complaint was well-founded.

Although it was a one-time incident, it was an example of the serious ramifications that privacy disclosures – however inadvertent or well-intentioned – can have.

More than just fruits and vegetables

Overview

An individual had hoped to conduct some business at her bank's kiosk located in a nearby supermarket. While she waited for service, she noticed a computer terminal in an open area. The monitor was live, and assuming that it was for the public to use to obtain general banking information, she typed in her name and address as prompted. The computer displayed information related to her accounts with the bank, including credit card numbers, limits, and balances. She had not been asked for any password or user identification.

Later, when she was sitting with a bank employee, she was able to see him entering his password, which she claimed appeared on screen in clear text, when he logged onto another computer. (She stated that the screen was positioned such that she could see it.) Concerned about the bank's apparent lack of safeguards, she brought her concerns to our attention.

The kiosk branch in question comprised an ABM for public use, an enclosed business office with a computer terminal for employee use only, and one other computer terminal situated in an open area. This terminal was also intended for employee use, but there was no sign posted to that effect. On the day in question, two employees were working. One was away at the time of the incident, and the other was busy with a customer in the enclosed office.

According to the bank, this incident was a simple case of employee error. The last employee to use the open-area computer had forgotten to log off – an infraction of the bank's own security policy and procedures.

The bank took two remedial measures as a result of the complaint. First, it sent advisories to employees of in-store offices, placed a message on its intranet site, and included some formal guidelines in training manuals for new employees. Second, it installed a new computer system with a password-protected screensaver that activates automatically if the keyboard remains untouched for 15 minutes.

As for the allegation that she could discern the password used by the bank employee, the bank said that, with the computer system in use at the time, passwords appeared on screen in the form of symbols, not in recognizable clear-text characters. The bank suggested that the complainant had either mistaken the employee's user ID or other log on information for his password. It also suggested that she perhaps had recognized the password by looking at the keyboard while the employee was typing rather than from the computer screen.

The complainant countered that it did not matter how she had recognized the characters. Bank employees logging on to computers should not allow customers to see either the computer screen or the keyboard.

Actions taken by the OPC

We considered this complaint well-founded. We noted that the bank had created a considerable risk of unauthorized access to customers' personal information when it installed in open areas of its kiosk branches computers that were often left unattended. In considering whether the bank had instituted appropriate safeguards to mitigate this risk and protect the information, we determined that:

- The bank's primary safeguard at the time of the incident was an instruction in a security manual to the effect that employees should log off when about to leave a computer unattended.

- A bank employee's failure to follow this instruction resulted in the complainant gaining unauthorized access to sensitive personal information.

- Although no improper disclosure to a third party occurred, the same neglect by the employee had created a significant potential for such a disclosure.

In the circumstances, the safeguard upon which the bank relied was ineffective and inappropriate. We therefore found the bank in contravention of the requirement under *PIPEDA* for appropriate safeguards.

As for the remedial measures taken by the bank, we felt that, although the automatic shutoff was an improvement, this measure would not prevent access during the 15-minute time delay and therefore could not be considered an adequate safeguard. A safeguard was needed that would protect sensitive personal information at all times.

As for the second remedial measure, we noted that even though the employee in this incident knew the rule he had neglected to follow it. Taking the human factor into account, we were not convinced that a reinforced instruction was likely to provide any more effective protection than the original form of instruction. Indeed, we were concerned that relying on the new 15-minute cut-off would actually make employees complacent and less likely to follow the rule of logging off manually.

In spite of the remedial measures, we felt there continued to be an unacceptable potential for unauthorized access to customer information via the computers placed in areas open to the public.

We recommended that the bank:

- Review its information security policy and procedures specific to the operation of its kiosk branches and take appropriate measures to ensure that access to any computers whereby customers' personal information may be obtained is restricted to authorized bank employees; and

- Take appropriate measures to ensure that customers are prevented from seeing passwords and other identifiers used by employees to log on to computers.

The Office is currently following-up with the organization to ensure that recommendations have been implemented.

Lost and found

Overview

An employee of a company complained to us when a co-worker found a letter concerning the complainant in a reference binder. The binder in question was reserved for employee use and was accessible to anyone on the work site. The letter summarized a meeting the complainant had, some six years earlier, with his superiors regarding problems he was having at work. In the letter was a recommendation for a new posting, as well as certain measures to help him with a number of personal problems he was having at the time.

Two letters, relating to two other employees, were also found at the same location. These documents concerned personal problems that these individuals had been having at work.

The company could not explain how these letters ended up in a reference binder, suggesting that the binders had been misplaced or moved and then reopened several years later. We noted that the way the company handled documents containing the personal information of employees had completely changed over the last several years.

Actions taken by the OPC

In our view, such highly sensitive personal information, referring to an employee's personal problems, required special protection. Although our investigation could not determine how these letters ended up in the binder, we concluded that there had been gaps in the company's safeguards to protect the personal information of employees. We also noted that such documents had been kept far longer than necessary to fulfil the company's stated purposes.

While we concluded that the complaint was well-founded, we were pleased that the company sent the complainant a letter of apology during the investigation.

IDENTIFYING THE PURPOSE OF THE COLLECTION OF PERSONAL INFORMATION

The baggage we carry

Overview

All she wanted was to find her missing baggage. She certainly did not expect that to do so, she would have to provide the airline that misplaced it with her SIN, her date of birth, and her occupation on the baggage claim form.

Though not happy about giving this information, the complainant in this case did eventually complete and submit a baggage declaration form so that the airline would pursue the matter. None of the items of personal information requested on the form were designated as optional. The form did identify two purposes for collecting the information – tracing baggage and serving as the basis of a claim.

Actions taken by the OPC

What the form did not identify, but our investigation revealed, was that the information collected would be filed in a tracing system used by air transport organizations worldwide and therefore accessible to other parties. In addition, the form did not specify that serving "as the basis for a claim" actually meant not only processing a claim, but also investigating the credibility of the claimant.

Our Office learned that the tracing system included an investigation component whereby the airline, following an unsuccessful trace, could crosscheck for prior claims and any suspicious informational inconsistencies possibly indicating fraudulent intent on a claimant's part. The airline acknowledged that most of the personal information it collected from its form was used as much for the purpose of claims verification as for the purpose of tracing baggage. The airline maintained that not all the information on its form was mandatory. Claimants had discretion to decline to provide an item if they did not feel comfortable in doing so. However, the form itself did not indicate that any of the information it requested was optional, nor did it appear that the airline made a practice of informing claimants that they had any discretion in the matter.

In discussions with the airline, our Office took the following position:

- it is not appropriate for an organization to require the provision of a SIN as an identifier;

- an individual's occupation is not an appropriate item to request as a means of verifying a claim nor is "company name";

- date of birth and several of the other items of personal information requested on the claims form should be designated as optional; and

- the form should be revised so as to specify that collected personal information is recorded in a tracing system available to other users, and clarify that claims verification is one of the purposes.

While the airline agreed to revise its form as proposed, to remove SIN from it, and to designate date of birth, passport number, and passport name as optional, it was reluctant to make further concessions.

In our findings, we determined that the airline had not stated its purposes for collecting personal information in such a way that the customer could reasonably understand how

the information was to be used or disclosed. In our view, the airline should have clarified that tracing baggage would involve putting personal information into a tracing system and creating a potential for disclosure to other users of that system. We also stated that the airline should have clarified that serving as the basis of a claim meant verifying the claim as well as processing it. The vaguely stated purposes did not, therefore, constitute a reasonable effort on the company's part to inform individuals of the purposes for which their personal information was to be used or disclosed.

As for the counter agent who had initially collected the complainant's personal information, we determined that she had made no effort to explain to the complainant what was to be done with the information. Although the agent might well have assumed that the complainant would understand that it would be used to trace her baggage, we believed that the agent should have at least informed the complainant of the means by which the information was to be recorded and by which the tracing would be done – that is, the worldwide tracing system.

Noting that knowledge is required as a basis for consent, we stated that the airline should have first informed the complainant of the specific reasons for collecting her personal information. As the company had not done so, it had no valid basis for consent.

Finally, with respect to the fact that the company had required the complainant to complete the entire form as a condition for pursuing the missing baggage, we noted that the purposes for which the information was collected had not been properly specified, as required under *PIPEDA*. We also determined that the airline's collection of SIN, birth date, occupation and company name was excessive and we were satisfied that a reasonable person would not have considered it appropriate to collect such information in the circumstances.

We therefore concluded that this was a well-founded complaint and recommended that the airline:

- follow through with the undertakings previously agreed to;
- designate "business address," "business telephone," "e-mail," and "frequent flyer ID" as optional;
- remove "occupation" and "company name" from the form;
- group all optional items on the form under one heading so that passengers may choose to complete some, all or none of the items;

- specify, at the items "prior address" and "prior telephone number," that these requests are made solely for the purpose of verifying the claim; and

- instruct its baggage claims agents to explain to the individual the use to be made of personal information collected at the time missing baggage is first reported; to specify that the information is to be filed in the tracing system and made available to other users of the system; and to limit initial information requests to those items that are justifiable in terms of the strict purpose for the initial collection – that is, tracing baggage reported as missing.

The Office is currently following-up with the organization to ensure that recommendations have been implemented.

UNAUTHORIZED USE OF PERSONAL INFORMATION

The cart before the horse

Overview

This Office learned that one branch bank manager had instructed her employees to conduct credit checks on customers, without their knowledge and consent, to determine who might be eligible for overdraft protection. Customers were then later informed that they had been pre-approved for the service. If they accepted, they were asked to sign an authorization for a credit check that had already been performed.

By the time we became aware of it, the bank had already initiated corrective action. During a regular "spot check" conducted by the bank to ensure compliance with bank policies, a deviation in policy at this particular branch was noted. The policy in question stated that employees must obtain a customer's consent to a credit check when offering him or her overdraft protection. The branch manager was notified, and she corrected the situation immediately.

The bank stated that the manager had misread the consent language for accounts. She mistakenly believed that she could use the consent language referring to a credit update to justify pre-screening for the overdraft protection.

Outcome

As there was no dispute that the branch manager had authorized the collection and use of customers' personal information without their knowledge and consent, we found

the bank in contravention of the consent requirement under *PIPEDA*. However, as the bank had a proper policy in place, and discovered and corrected the deviation in policy even before the Office became interested in the matter, we concluded that the complaint was resolved.

OBTAINING CONSENT

The ex-wife, her lawyer, the daughter and the collection agent

Overview

One individual complained that a bank, through a collection agency working on its behalf, had been telling his family members and his ex-wife's lawyer about his financial woes. Our investigation established that the collection agent handling the file had indeed contacted the complainant's daughter, his former wife, and her lawyer. In fact, there were a number of telephone conversations between the agent and these individuals. Some calls were placed by the agent; others, by the individuals to the agent. All calls coming into and going out of the agency, as well as summary notes of the calls, were logged into the agency's electronic tracking system. The information in this system could only be altered within two hours after it was originally logged.

Actions taken by the OPC

We could find no evidence that the agent had disclosed specific information regarding the complainant's financial situation, or made any threats about seizing his property, as he alleged.

The bank audits the agency to ensure that its privacy practices are in keeping with those of the bank. The agent, a long-time employee of the company, had signed a number of confidentiality and ethics statements with the agency.

In our findings, we noted that, although *PIPEDA* allows an organization to disclose personal information without knowledge and consent to collect a debt owed by the individual to the organization, it does not confer a *carte blanche* upon an organization to disclose however much information it wishes in pursuit of a debt.

In this case, we established that the only information provided to the ex-wife was a reference to an outstanding debt. Her lawyer declined to provide written confirmation of what the agent disclosed to her. The daughter and the agent contradicted each other's testimony, and we could find no documentary evidence showing that there had been any

excessive disclosure of the complainant's personal information. Given this, we concluded that the complaint was not well-founded since the agent's actions were consistent with the exception to consent in the pursuit of a debt.

Measuring up

Overview

Two employees of a company protested when their employer decided to use statistical data about their work to measure job performance. The information in question – volume, duration, and type of call received by telephone operators – had long been collected to measure and manage workload at the office level. However, when the company began using this information to manage individual performance, the complainants, who were telephone operators, argued that the company was collecting and using statistical data about them without their consent.

We learned that the company had informed its employees of this policy change via group presentations, e-mail, and team and one-on-one meetings. The collection and use of statistics were also discussed in the company's privacy brochure for employees.

The employees received a monthly report containing their individual statistics as compared with predetermined targets or expectations. They also could receive a report containing statistics per shift.

Actions taken by the OPC

We found that the company's purpose, namely to monitor and evaluate the job performance of its employees, was appropriate, and that the company had adequately informed employees of this purpose. As for whether an employer required an employee's express consent to collect and use such information for performance-management purposes, we determined that when an individual agrees to work for a company, he or she is giving implied consent to the conditions of employment. Performance evaluation is one such condition, and one to which the complainants had given their implicit consent when they began working with the company. We concluded that the complaint was not well-founded.

Credit report check-up

Overview

When a couple checked their credit report, they noticed that the credit agency had disclosed their credit information to a particular credit grantor. They had never had any direct dealings with this credit grantor, and were suspicious that the grantor had accessed

their credit file on behalf of its parent company. The parent company was also the wife's former employer, and the adversary in a dispute.

The couple complained to the credit agency, and was told that their concerns would be investigated and the results made known to them. However, when they called three weeks later for an update, a different representative told them that no internal investigation had been initiated.

This same representative told them that they should look into the matter themselves since the parent company in question was not a client of the agency, and the agency therefore had no jurisdiction to investigate. Yet a third representative subsequently promised that the agency would investigate. Skeptical of this promise, the couple complained to us.

Actions taken by the OPC

Our investigation confirmed that the third representative had initiated an investigation. The owner of the parent company admitted to the agency that he had obtained the couple's credit information without their consent through his company's subsidiary. He knew he had broken the rules. But he stated that the circumstances relating to his company's dispute with the wife over possible wrongdoing on her part had compelled him to take such action.

The credit grantor's standard contractual agreement with the agency stipulated that it could only order consumer credit reports for permissible purposes and that it must first obtain all consumer consents required under the applicable provincial credit reporting legislation. The agreement also stated that the agency could immediately terminate or suspend service if it reasonably believed that its client had breached any condition.

The agency did not terminate or suspend service to the offending credit grantor, but rather placed it on a year's probation. The agency assured the Office that this punitive measure would include audits and monitoring of the client's credit information applications. It also promised that further failure to comply would result in termination of the contract.

After completing its investigation, the agency did not inform the complainants of the results for some eight weeks. The agency notified the complainants that the unauthorized credit inquiries had been removed from their files because the client had been unable to prove a legitimate purpose or valid consent. The agency apologized to the complainants for any inconvenience caused.

On the matter of consent, we determined that the credit agency disclosed the couple's personal information without their consent. The issue we had to consider was whether the agency could reasonably be held responsible in the circumstances.

It was clear to us that the agency had not known that the complainants' knowledge and consent were lacking. It was also clear that the agency had presumed, on the basis of a contractual agreement, that the company's purpose was permissible and that consent had been obtained. Therefore, in our opinion, the agency's disclosure had been made in good faith and on reasonable presumption of consent, given the obligations set out in the contract, and thus did not in itself offend the *Act*.

However, when it came to the agency's investigation and the follow-up to its investigation, we were more critical. Under the *Act*, an organization must investigate all complaints it receives and take *appropriate* measures if the investigation shows the complaint to be justified. The agency had found the complaint to be justified and had eventually taken certain measures against its client, but the measures taken – notably, that of putting the client "on probation" – fell short of being appropriate for the following reasons:

- In the first place, the evidence strongly suggested that the measures against the credit grantor had been taken only at the Office's prompting.

- Secondly, it was reasonable that one immediate measure an organization should take at the end of its investigation was to inform the complainant of the results. It appeared, however, that the agency only notified the couple of the results after this Office suggested that it was the appropriate thing to do.

- Thirdly, and most importantly, the measures taken by the agency had not been appropriate in relation to the seriousness of the offence. The agency's agreement warned of "suspension" or "termination" of services for clients reasonably believed to be in breach, but the agency had imposed "probation." We did not believe that this sanction conveyed a strong enough message to the company that its actions were unacceptable. We noted that punitive measures regarding such privacy breaches should reflect due regard for the integrity of personal information in its care — and ideally should serve as a deterrent to further similar breaches.

We made the following recommendations:

- The agency should consider imposing and enforcing tougher penalties for client organizations in breach of contract relating to access to consumers' personal information. Penalties could begin with suspension of services, followed by a probationary period involving frequent and rigorous audits.

- The agency should develop and strictly apply a policy stipulating the timing and method of informing a complainant of the results of an internal complaint investigation.

The Office is currently following-up with the organization to ensure that recommendations have been implemented

USE OF SOCIAL INSURANCE NUMBERS

To SIN or not to SIN

Overview

A customer objected to a bank using social insurance numbers (SINs) to confirm the identity of credit card applicants with the credit bureaus. The complainant believed that the bank was doing this without properly informing applicants, and obtaining their consent. She also felt that the language of the credit card contract did not clearly indicate that customers had the option of not providing their SINs. Instead, she said the language left the impression that if you did not provide your SIN, you would not get the card.

The bank maintained that its purpose for using the SIN, which was to accurately match the credit history file of creditors was a legitimate one. The bank told us that providing the SIN for this purpose was optional. A customer could refuse to provide it, or ask the bank to remove it from its records.

Both the electronic and the hard copy versions of the application form included a statement about the SIN being used for identification purposes. But neither form mentioned that its provision was optional. In fact, both forms stated that all information must be provided, and that signing the form or clicking the appropriate box indicated agreement to all terms by the applicant.

Actions taken by the OPC

Since the bank had not made a reasonable effort to ensure that the customer was properly informed that providing a SIN was optional, we found that the bank was not obtaining valid, meaningful consent from applicants.

The bank acknowledged that the language on its forms was a problem, and agreed to make changes indicating that the provision of the SIN for credit history file matching purposes was optional. While we were pleased with the bank's undertaking, we stressed that the SIN is not a piece of identification and should not be used as such.

Use of SIN in the private sector

This complaint was representative of the many complaints our Office received in 2003 regarding the use of the SIN for identification purposes by private-sector organizations.

The legislated uses of the SIN have expanded since its creation in 1964 as a client account number in the administration of the Canada Pension Plan and various employment insurance programs. The federal government, in an effort to prevent the SIN from becoming a universal identifier, issued a policy limiting the collection and use of the SIN to specific acts, regulations and programs.

The following summarizes the extent to which the collection of SINs is permissible in the private sector:

- Employers are authorized to collect SINs from employees in order to provide them with records of employment and T-4 slips for income tax and Canada Pension Plan purposes.

- Organizations such as banks, credit unions, brokers and trust companies are required under the *Income Tax Act* to ask for customers' SINs for tax reporting purposes (e.g., interest earning accounts, RRSPs, etc.).

- No private-sector organization is legally authorized to request a customer's SIN for purposes other than income reporting. In the case of a financial institution, there is no legal requirement for the organization to collect the individual's SIN, and no obligation for the individual to supply it, if a customer's account is not of a type that earns interest (e.g., if it is a credit account as opposed to a savings account).

- There is no law prohibiting an organization from *asking* for a customer's SIN, or a customer from supplying the SIN, for purposes other than income reporting.

While there is no legislation that prevents organizations from asking for the SIN for other purposes, such as identification, organizations that are subject to *PIPEDA* must clearly indicate to the customer that provision of the SIN is optional and not a condition of service.

USE OF WEB MONITORING TOOLS

The way the "cookie" crumbled

Overview

An individual was unhappy with one organization's Web site. He told us that he was unable to access the site because he had configured his browser to disable "cookies." He also claimed that the company's Web site was collecting the personal information of visitors without their knowledge and consent because it did not inform visitors that it placed a cookie on their computers' hard drives.

The organization used both permanent and temporary cookies on its Web site. Cookies collect and store a variety of information. Permanent cookies are stored indefinitely on a user's hard drive unless manually deleted, while temporary cookies are automatically deleted from the user's browser upon logging off a site. Web browsers typically allow users to disable permanent or temporary cookies. The complainant, who had disabled permanent cookies, was unable to proceed through the site in question because it was coded in such a way that it would not let him in until a cookie had been stored on his computer. The company acknowledged that this was caused by an "application glitch" and took steps to ensure that visitors who had programmed their computers to refuse permanent cookies could still use the site.

The organization also admitted that it did not indicate on its Web site or in its company privacy policy that it used cookies. The company, however, told our Office that it was in the process of creating and publishing a comprehensive policy on its use of cookies.

Actions taken by the OPC

In this well-founded complaint, we determined that the information stored by the temporary and permanent cookies was personal information for the purposes of *PIPEDA*.

Although the company did not intentionally deny access to individuals who had disabled permanent cookies and had taken steps to fix the problem, the company had nonetheless denied the complainant access. We also noted that the company had not met the requirement for knowledge and consent under *PIPEDA* regarding its use of cookies. Our Office was pleased, however, that the company agreed to publish a comprehensive policy on its Web site regarding cookies.

EMPLOYEE MEDICAL INFORMATION

The *Personal Information Protection and Electronic Documents Act* applies to the personal, including medical, information of employees in federal works, undertakings, or businesses. In 2003, the Commissioner received a number of complaints from employees alleging that their employers were collecting too much medical information or inappropriately disclosing it. The following are summaries of some notable cases. Also included at the end is an overview of our Office's position to date.

Diagnosis: Too much information

Overview

Several employees of a company complained when their employer required them to provide medical diagnoses for sick leave. These individuals had exceeded the number of days allowed every year for uncertified sick leave, or had what their employer considered a suspicious leave pattern.

The complainants had no problem with their employer asking whether or not they were under a doctor's care, what if any restrictions they might have, and whether they were taking any medications that might affect their ability to work safely. What they did not like was their employer forcing them to provide a *diagnosis* of their illness to justify their sick leave.

The company countered that it needed the diagnosis information for two purposes. One reason involved "at risk" employees. These individuals work in safety-sensitive positions, often in isolation, with long shifts, and physically demanding duties. The company maintained that an employee's physician may not be aware of the employee's job requirements. It believed the company's health and safety officer would be in a better position to judge if it was safe for the employee to return to duty. However, the company could not provide any evidence that it routinely used diagnostic information for such a purpose. Indeed, in one case, it allowed an "at-risk" employee to return to duty even though his doctor had not provided the company with a diagnosis.

The other reason for requiring a medical diagnosis concerned "suspicious absences." An absence was considered suspect if taken immediately prior to or following vacation leave or during a period when the company had previously refused time off. If the company found the absence questionable, it reserved the right to demand a medical certificate with a diagnosis from the employee.

Following discussions with the Office, the employer decided it would no longer require employees to submit a diagnosis for suspicious absences and to re-examine the requirement for diagnoses in respect of "at risk" employees.

Actions taken by the OPC

In our determinations, we commented that while it was appropriate and reasonable for the employer to require medical certificates when the employees' absences exceeded the allowable limit for uncertified sick leave, a medical certificate without a diagnosis should have been sufficient. As the employer ultimately acknowledged, it was not necessary to require employees to provide diagnostic information in cases of suspicious absences.

In our opinion, the company did not satisfactorily demonstrate the need to inquire into the nature of the illness to ensure the complainants' fitness to resume regular duties or to otherwise accommodate their return to the workplace.

Indeed, in the circumstances of these complaints, namely, where the employees had exceeded their allotted annual uncertified sick leave or their absence was suspect, we found it unnecessary and inappropriate for the company to have demanded this information. We therefore concluded that the complaints were well-founded.

We recommended that the company drop its requirement for mandatory inclusion of diagnoses in the medical certifications of employees designated "at risk" and limit its collection of employees' diagnostic information to cases of clear necessity in the fulfillment of legitimate purposes. We also recommended that the company amend its sick leave policy accordingly.

Finally, we recommended that the organization review its decision to deny medical leave to individuals who refused to provide a medical diagnosis when they had exceeded their allotted annual uncertified sick leave.

The Office is currently following-up with the organization to ensure that recommendations have been implemented.

Diagnosis: Purposes reasonable

Overview

The need for diagnostic information, and to whom medical information is disclosed, were the subjects of complaints made by an individual against her former employer.

At the start of an extended sick leave, the complainant submitted a completed medical form to her employer containing a specific diagnosis from her doctor. Although she provided this information, she objected to the requirement for the diagnosis. She believed that her employer should be content with a general description, such as "illness," "injury," or "work-related."

To her surprise, a few months after submitting the form, the complainant received a letter from the provincial Workers' Compensation Board, rejecting her claim for compensation for lack of evidence. The Board determined that her disablement was not work-related. The letter referred to information that a WCB adjudicator had received from the complainant's employer. The complainant had not made a direct claim from the WCB, and believed that the information given by her employer was not relevant to the actual disability. She therefore believed that her employer's disclosures, made without her knowledge and consent, were inappropriate and unjustified.

The investigation established that her employer notified the WCB of an alleged work-related disablement and initiated a claim for compensation on the complainant's behalf. A WCB adjudicator obtained a copy of the complainant's original medical form and questioned the employer regarding the disablement. The employer's representative, a human resources coordinator, confirmed that the complainant had previously missed work for a similar reason. She stated that she believed the previous absence had been due to personal, not work-related, reasons. She could not say, however, whether the current absence was work-related or not.

Regarding the collection of medical information, the company contended that its request for specific diagnoses was necessary to manage both a short- and long-term disability plan for employees. Eligibility for benefits under the long-term plan is determined on the basis of short-term benefits drawn over a certain number of days for the same disablement.

The employer noted that its purposes for collecting the information are identified on its short-term disability policy and on its medical form. It maintained that the collection of information was limited to what was necessary for these identified purposes. Furthermore,

the company noted that since the medical form contains a consent statement and is signed by the employee, employee consent is being obtained.

As for the disclosures to the WCB, the company pointed out that these were not only appropriate, but required by provincial workers' compensation legislation to which the company is subject. The legislation requires that subscribers immediately notify the WCB of any work-related disablement or allegation of such. It also authorizes the WCB to make inquiries about claims and obligates subscribers to respond to such inquiries.

Actions taken by the OPC

We determined that the company's purposes for collecting diagnostic information, namely, to manage the disability program for employees, were reasonable and legitimate. We also found that these purposes were appropriately identified, that the collection was limited to what was necessary for the fulfillment of the purposes, and that the individual's consent was obtained.

With respect to the disclosure, which was clearly done without the complainant's knowledge or consent, we determined that the disclosures in question had been required by legislation and therefore allowed under a paragraph in *PIPEDA* that provides for disclosure without knowledge or consent if it is required by law.

We concluded that these complaints were not well-founded. Nevertheless, during the investigation, it was noted that the company lacked policy, procedures, guidelines, and staff training materials relating to employee information. It was therefore recommended that the company implement appropriate polices and practices, specific to the handling of employee personal information, in accordance with the accountability principles set out in *PIPEDA*.

The Office is currently following-up with the organization to ensure that recommendations have been implemented.

Diagnosis: Reasonable in the circumstances

Overview

An employee who wanted to be accommodated in another position for medical reasons felt that his employer was attempting to collect too much information from him. When he went on leave, his employer asked him to authorize his doctor to fill out a form indicating his prognosis, limitations, treatments and abilities. The doctor provided a diagnosis and information about treatment, but did not fill out the portion concerning limitations or

abilities. The doctor provided three similar reports over a period of time, all indicating that the prognosis was unknown.

Eventually, the doctor cleared the complainant to return to work on a part-time basis. The doctor supported the complainant's request that he be transferred to a different work environment. The complainant wanted operational duties, as opposed to office ones.

But the company had not received a request from him to this effect. So the occupational health services nurse asked the doctor for more information about the medical condition. She also wanted to know whether the complainant was able to do physical work since he had been injured some years prior, which had resulted in him being transferred to an office job.

The complainant then made a formal request for a transfer on medical grounds. The company wanted additional medical information. It also indicated that an independent medical evaluation might be required. When the company refused the complainant's request, his doctor wrote to the employer in support of the complainant. The company replied that it wanted to consult a specialist before reconsidering the request. The complainant and his union objected, arguing that the company should accept the medical evaluations of the complainant's physician. In the end, the complainant returned to his desk job.

The company had a formal policy on extended sick leave. Under this policy, the employee was requested to sign a consent form authorizing the physician to disclose medical information related to the employee's illness to the company's occupational health professionals and to discuss the matter directly with them. The form contained the purposes for collecting the information – namely, consideration for eligibility benefits and establishment of fitness to work. The form asked for information about the employee's medical condition, treatment and prognosis, including diagnosis.

The company's occupational health services staff were the only employees to see this information. They were bound by their respective codes of conduct to maintain confidentiality. They provided managers only with information relating to the abilities and limitations of the employee. Detailed information about the company's policy was available to all employees via the company intranet and in a brochure.

The company also had policies and procedures in place to safeguard employee medical information. Such information was kept in a file separate from the personnel file, and stored in secure areas. Computerized information was also protected.

Actions taken by the OPC

We determined that, in light of the company's liability to continue paying the complainant during the first six months of his absence and its obligations under Canadian human rights legislation to accommodate employees with disabilities, the purposes for collecting diagnoses were legitimate and appropriate.

In considering how well the company limited its collection of personal information, we noted that the guidelines of the Canadian Human Rights Commission indicate that an employer has the right under the *Canadian Human Rights Act* to seek enough information to determine if it has an obligation to accommodate an individual with a disability and that this may involve consultation with a medical specialist. We were satisfied that the medical documentation that the employer was seeking was clearly linked to the company's obligations to accommodate the complainant and was not excessive.

We were also satisfied that the company had appropriate policies and procedures in place that outlined the purposes for collecting health information, how it is handled and by whom, and the respective roles of the employer, employee and the health services department. This information was also made available to employees in a variety of formats, thus satisfying the company's obligations under *PIPEDA* to not collect personal information indiscriminately, and to specify the type of information collected as part of their information-handling polices and practices.

We therefore concluded that this complaint was not well-founded.

Summary of the Office's position to date on employee medical information

Employers collect employee medical information for a number of reasons. Such reasons must be appropriate and legitimate in the circumstances and must be clearly identified. The information collected must be limited to these purposes.

By far, the most contentious issue raised by employees in past year was the requirement to provide diagnoses. In cases where diagnostic information was sought, our Office recognized that an employer may need to collect such information in certain limited circumstances. Thus far, we acknowledge that it may be needed to determine an employee's fitness to work and to accommodate an employee with a disability. It may also be required to determine an employee's eligibility for benefits. The Office, however, did not consider it reasonable to require a diagnosis in the case of suspicious absences or when an employee had exhausted uncertified sick leave.

The Office was clear that employee medical information, especially diagnostic information, must be handled with strict safeguards in place. Specifically, medical information must be kept separate from the employee's personnel file, in a secure location. Where diagnostic information is provided, it should only be handled by qualified medical personnel, not human resources specialists. Managers should only be provided with limited information, such as the expected date of return. Supervisors do not generally need, as a matter of course, the specifics of the employee's illness.

Such measures, of course, speak to the need for clear policies and procedures. Under *PIPEDA*, organizations are required to establish and make available policies and procedures for the handling of personal information in their care.

It should also be noted that there may be other pieces of legislation, such as labour law, workers' compensation, or human rights laws, that have a bearing on the amount of information collected, used or disclosed by the employer.

The bottom line? Organizations must ensure that they:

- only collect employee medical information for reasonable purposes;
- identify these purposes;
- obtain meaningful consent; and
- limit their collection, use, and disclosure practices to these purposes.

Incidents under *PIPEDA*

The Office also conducted thirteen incident investigations. Incidents are matters that this Office learns of from various sources including the media and organizations which have themselves identified a problem. Usually a victim is not identified and a complaint has not been filed with the Office.

Dumpster disclosures

Through media reports, our Office learned that police had found the financial records of bank customers in a suspect's apartment. The man allegedly obtained the documents from dumpsters at branches of three banks.

Representatives from the three banks retrieved the documents, and analyzed them with a view to determining their origin, identifying affected customers, and taking the appropriate corrective action.

The first bank identified the personal information of 40 customers from seven branches. It determined that the documents were likely retrieved from the garbage. While the bank has a policy with regard to the destruction of personal information, garbage disposal arrangements vary from branch to branch. Some branches contract an outside shredding service, while others require staff to physically destroy documents, either by shredding or manually ripping up, before disposal.

The bank checked the accounts, and notified all affected customers by telephone that no unusual activity had been detected. It committed to continue monitoring their account activity and asked the affected customers to do the same. The bank also gave customers the option of closing their existing accounts and opening new ones. The bank reissued its policy and procedures on the disposal of personal information, and branches were advised to reiterate the policy and procedures to staff. The bank is considering a nation-wide supplier program for locked bins and regular destruction of confidential documents.

With respect to the second bank involved, the personal information of 44 customers was retrieved. The bank concluded that the documents were taken from internal and external garbage bins as well as internal recycling and shredding receptacles. Branches have receptacles at each desk and teller wicket, which are emptied into a confidential shredding bin on a daily basis.

The bank contacted all affected customers by telephone and in writing, informing them about the ongoing police investigation. The bank offered specific advice and extra protection according to the level of risk for identity theft that their situation presented. It also advised them to monitor their accounts for unusual activity, report any missing mail, and properly safeguard their financial records. The bank issued a reminder to branch staff in the affected region regarding the proper garbage disposal policies. The policy is to be reviewed by branch staff monthly. In addition, customer garbage receptacles have been removed and only built-in wall receptacles will be used.

With respect to the third bank, 575 customers in the area were affected. Four reports were recovered that contained multiple customer names, accounting for 438 of these customers. The personal information of the remaining customers was found in a variety of documents that pertained to individual customers.

The bank believed that some of the documents were taken from the garbage as they were soiled or manually shredded. Other documents were in good condition, and the bank was unable to conclusively determine whether they came from the garbage or whether the suspect stole them from shredding boxes inside the branch. These boxes are unlocked and located close to financial and business advisor workstations.

The affected customers were grouped according to whether the information disclosed about them placed them at higher, moderate or lower risk of identity theft and fraud. Branch representatives contacted customers by telephone and told them what specific information had been disclosed. The bank invited customers in the higher and moderate risk categories to meet with a branch representative in order to review their accounts for unusual activity and open new accounts. The bank also advised them to contact their credit bureaus or HRDC if a document containing their SIN was disclosed to mitigate the risk. The bank told all customers to monitor their account activity.

The bank reviewed proper procedures with the managers of the four affected branches. It also commissioned a working group to review branch procedures and practices for the destruction of confidential records and to recommend any required changes.

This incident yielded no complaints to our Office from affected individuals.

Bank computers containing client personal information sold

The media reported on a story about a computer re-seller who had purchased two computers from a bank and then posted them on an online auction site only to discover that the computers contained the personal financial information of the bank's customers. He subsequently contacted the bank.

It turned out that when the re-seller had gone to collect the computers he had bought, an employee of the company contracted to wipe off and dispose of the bank's computer equipment inadvertently took the two computers from a pallet of servers that had not yet been cleaned.

The bank identified 350 customers whose personal information was on one or both of the computers. A variety of personal financial information was found. The bank contacted the affected customers by telephone and participated in news media interviews to convey its message that the situation was under control and that customer accounts were secure. The bank also audited the contractor involved and identified a number of gaps. The bank reviewed the disposal process and drafted a new disposal guideline.

Our Office received no complaints from affected individuals regarding this incident.

Inquiries

The Office responds to thousands of inquiries from the general public and organizations seeking advice and assistance on issues about privacy in the private sector.

The majority of calls and correspondence during the last half of 2003 concerning *PIPEDA* were from businesses, large and small, that required guidance in gearing up for the implementation of the *Act* on January 1, 2004.

We also heard from individuals who called or wrote to express dissatisfaction with organizations, claiming that they either mismanaged their personal information in some way, refused them access to or corrections of their personal information, or did not have appropriate safeguards to protect personal information.

Inquiry statistics

(January 1 to December 31, 2003)

Telephone inquiries received	9,288
Written inquiries received (letter, e-mail and fax)	4,134
Total number of inquiries received	13,422

PRIVACY PRACTICES AND REVIEWS

Audits and Compliance Reviews under the *Personal Information and Electronics Document Act* (*PIPEDA*)

The Office's mandate to conduct audits of private sector organizations is derived from section 18(1) of *PIPEDA*. The *Personal Information Protection and Electronic Documents Act (PIPEDA)* enables the Commissioner to audit the compliance of private sector organizations if there are reasonable grounds to believe they are in contravention of the *Act* . Under *PIPEDA* the Commissioner may only undertake such an audit where there are "reasonable grounds" to believe that an organization is contravening a provision of the *Act*.

To date, no compliance audit of a private sector organization has been undertaken by the Office pursuant to section 18(1) of *PIPEDA*. Such evidence of non-compliance with *PIPEDA* that has come to the Office's attention has been through complaints and

inquiries. Most of the compliance issues brought to our attention deal with discrete incidents that lend themselves to remedy within the framework of the complaint and inquiry processes.

That said, in the upcoming year our Office plans to review completed investigations under *PIPEDA* to follow-up on those well-founded complaints where remedial action was recommended. The aim of this exercise will be to determine whether recommendations made by the Commissioner are being adopted. It is expected that this will be accomplished through correspondence. The Office will conduct further inquiries where there is evidence of non-compliance.

IN THE COURTS

Under section 14 of the *Personal Information Protection and Electronic Documents Act (PIPEDA)*, an individual complainant has a right, following the Commissioner's investigation and report, to apply to the Federal Court of Canada for a hearing in respect of any matter referred to in the Commissioner's report. These matters must be among those clauses and sections of *PIPEDA* listed in section 14. Under section 14 the Commissioner may also apply directly to the Federal Court in respect of a Commissioner-initiated complaint.

Section 15 of the *Act* also allows the Commissioner to apply to appear in Federal Court in the circumstances described below. The Commissioner may, with the consent of the complainant, apply directly to the court for a hearing in respect of any matter covered by section 14; appear before the Court on behalf of any complainant who has applied for a hearing under section 14; or, with the leave of the Court, appear as a party to any section 14 hearing.

Between January 1, 2001 and December 31, 2003 there were 20 Applications filed in Federal Court in relation to *PIPEDA*. The majority of these were discontinued, dismissed or settled prior to any pronouncement by the Court. Following are a selection of *PIPEDA* applications which raised issues of interest.

Mathew Englander v. Telus Communications Inc. and Privacy Commissioner of Canada

Federal Court Files No. T-1717-01 and A-388-03

Complaint

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, as well as inappropriately charging customers for choosing to have their telephone number "non-published". He claimed that these actions by Telus contravene subsections 5(1) and (3) of the *Act*, as well as several clauses of Schedule 1 of the *Act*.

On the question of consent, the Commissioner found that the company did obtain valid consent through implication and was in compliance with the regulations regarding publicly available information. He focused on the company's questioning of customers regarding 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 noted CRTC Telecom Order 98-109, which states that telecommunications companies can charge no more than $2.00 per month for non-published telephone service. He determined therefore that the company in question did have the authority to charge its monthly fee of $2.00 for non-publication, and that doing so was not unreasonable.

OPC involvement

The Privacy Commissioner was granted leave to intervene in the appeal on the issues that: (1) according deference to the finding of the Privacy Commissioner and (2) the jurisdiction of the CRTC to make privacy related Orders does not restrict the Federal Court's jurisdiction under *PIPEDA*.

Court status

This was the first application for judicial review to be filed in the Federal Court under *PIPEDA*. The Application was dismissed in June 2003 at the Federal Court level.

Mr. Englander filed an appeal in the Federal Court of Appeal on 28 August 2003. No hearing date has yet been set.

Ronald G. Maheu v. IMS Health Canada et al.

Federal Court Files No. T-1967-01 and A-31-03

Complaint

Mr. Maheu complained that IMS Health Canada was improperly disclosing personal information by selling data on physicians' prescribing patterns without the consent of the physicians.

The Commissioner focused on the question of whether the information was personal information within the meaning, scope and purpose of *PIPEDA* and found that "personal information" is not so broad as to encompass all information associated with an individual. Based on this interpretation, the Commissioner found that prescription information, whether in the form of an individual prescription or in the form of patterns discerned from many prescriptions, is not personal information about a physician. Instead, he conceptualized this information as being about the professional process that led to the issuance of the prescription and concluded it must therefore be understood as work product.

OPC involvement

The Commissioner submitted written arguments on the original Application. These arguments focused only on according deference to the Privacy Commissioner and took no position as to the appropriate outcome on the facts.

The Commissioner was also involved with the procedural appeal, appearing in order to assist the Court with respect to the proper interpretation of *PIPEDA*. The Commissioner explained that an individual may file a complaint concerning an organization's information practices regardless of whether that organization collects, uses or discloses personal information about the individual complainant.

Court status

Mr. Maheu applied for a hearing in the Federal Court in November 2001.

IMS brought a motion seeking either to strike out the Application on the grounds that it was brought for an improper purpose or to have Mr. Maheu post security for costs. The Court ordered Mr. Maheu to post security for costs in the amount of $12,000 and noted that there appeared to be reason to believe that Mr. Maheu was using the *Act* for a collateral and improper purpose given that his own personal information was not at issue. The Federal Court granted Mr. Maheu's appeal of this Order in January 2003. This decision was appealed in turn by IMS but after a hearing in November 2003 that appeal was dismissed.

The original Application in the Trial Division was discontinued in March 2004 as part of a settlement reached between Mr. Maheu and IMS.

Diane L'Écuyer v. Aéroports de Montréal and Privacy Commissioner of Canada

Federal Court Files No. T-2228-01 and A-259-03

Complaint

Madame L'Écuyer had submitted requests for access to information held by her employer. The employer refused her requests by letter, and copied the letter to three other persons – two union representatives and the coordinator of employee relations at the airport. Accordingly, she filed a complaint that her employer had, without her consent, disclosed her personal information to third parties.

Regarding the disclosure to the union representatives, the Privacy Commissioner was of the opinion that there could be implied consent for the employer to copy those parties only if the complainant had indicated that they had been copied on the original access requests. The Commissioner found that in this case no such implied consent existed, and that a reasonable person would have considered the disclosure to the union representatives to be unacceptable.

As for the employee relations coordinator, the Commissioner took note of the direct involvement of the individual in these access requests and therefore determined that it

had been appropriate for the employer to inform him of its decision to refuse access. This portion of the complaint was therefore considered to be not well founded.

OPC involvement

The Commissioner applied for and was granted leave to intervene in the appeal. In November 2003 the Commissioner submitted a factum arguing that: (1) both the Commissioner and the Court have the jurisdiction to consider privacy issues notwithstanding the fact that they are work-related; and (2) while implied consent may be appropriate in some union-involved complaints, it was not in this one and therefore the consent of the Applicant to the use and disclosure of her personal information was required.

Court status

Madame L'Écuyer filed her original Application in Federal Court in December 2001 asking that the organization correct its practices to conform with *PIPEDA*. The Privacy Commissioner was not involved in this Application. In May 2003 a decision was released, with the Court finding that the issue arose from the administration of a collective agreement and therefore was not within the jurisdiction of the Court or the Privacy Commissioner.

Madame L'Écuyer filed an appeal on 5 June 2003. The appeal was heard in June 2004 and was dismissed on the facts. The Court confirmed the trial finding the Mme. L'Écuyer had consented, at least implicitly, to the disclosure in question. The Court found it unnecessary to address the jurisdictional aspects of the appeal.

Privacy Commissioner of Canada v. Aéroports de Montréal

Federal Court File T-336-02

Complaint

An employee of an airport filed two separate complaints to the effect that her employer had refused several requests she had made for access to her personal information. In refusing access, the airport management cited two exceptions provided under *PIPEDA*, specifically s. 9(3)(a) solicitor client privilege and s. 9(3)(d) information generated in the course of a dispute resolution process.

With regard to s. 9(3)(a), the Commissioner noted that the complainant had not requested access to any lawyer's file, but rather to documents related to complaints and disciplinary measures concerning herself. He determined that the airport management had not been justified in invoking solicitor-client privilege to protect the information simply on the grounds that it had been gathered to respond to complaints and grievances or that lawyers had been consulted on the various files.

With regard to s. 9(3)(d), the Commissioner noted that the purpose of this exception is not to protect information gathered in the course of administrative processes for resolving complaints or grievances. In the Commissioner's view, a formal dispute resolution process implies the desire of parties to meet for the purpose of negotiating a resolution acceptable to each, which was not the case with the parties in question. Hence, he did not accept the employer's interpretation that the process was one of formal dispute resolution or that the information at issue had been gathered strictly for that purpose. He determined that the employer had been wrong in applying section 9(3)(d) to refuse the complainant access to her personal information.

OPC involvement

When airport management persisted with their refusal to provide access even after the Commissioner's report was issued, the Privacy Commissioner obtained the complainant's consent as required by s. 15 of *PIPEDA* and filed an Application in Federal Court.

Court status

The Aéroports, in the course of litigation, agreed with the Privacy Commissioner that the individual should be granted access to her personal information and released to the complainant all the available information to which she was entitled under *PIPEDA*. Accordingly, the Commissioner discontinued the Application in April of 2002.

Erwin Eastmond v. Canadian Pacific Railway and Privacy Commissioner of Canada

Federal Court File No. T-309-03

Complaint

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.

In making his determination, the Privacy Commissioner applied s. 5(3) 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 fashioned a four-point test for assessing reasonableness, namely: (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? Considering the company's stated purposes against this backdrop, the Privacy Commissioner did not believe that a reasonable person would consider these circumstances to warrant such an intrusive measure as digital video surveillance. As such, 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 s. 5(3) of *PIPEDA*.

OPC involvement

The Privacy Commissioner was added as a party pursuant to s. 15(c) of *PIPEDA*, however she took no position as to the appropriate outcome on the merits. Instead, she argued that the Court should accord some deference to the expertise of the Privacy 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 both the Privacy Commissioner and Court's jurisdiction over the issues, notwithstanding that they arose in a collective bargaining employment situation.

Court status

Mr. Eastmond filed an Application in Federal Court in February 2003. Among other things, the Application requested that the Privacy Commissioner send a certified copy of the Commissioner's Record of investigation to the Applicant and to the Registry. Upon objection on behalf of the Privacy Commissioner to this request, the Court decided in June 2003 that the *Federal Court Rules* do not allow an Applicant to request material in the possession of the Privacy Commissioner.

The Application was heard in April 2004 and on 11 June 2004 the court released its decision. On the question of jurisdiction, the Court found that the Privacy Commissioner did have jurisdiction, 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*. On the question of deference it was established that although this was a proceeding *de novo,* the Privacy Commissioner was entitled to a degree of deference in light of her expertise. Finally, the court adopted the Commissioner's four-point test for s. 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, and therefore that CP Rail had not contravened *PIPEDA*.

Robert Lavigne v. Canadian Union of Postal Workers

Federal Court File No. T-500-03

Complaint

After determining that day and month of birth was being used as a seniority "tie-breaker", Mr. Lavigne complained that CUPW was using his personal information in a way that was inconsistent with the purposes for which the information was originally collected. The Office determined that it did not have jurisdiction to accept Mr. Lavigne's complaint because CUPW was neither a federal work, undertaking or business nor was there disclosure across borders for consideration.

OPC involvement

The Privacy Commissioner was not formally involved in the proceeding. However, the Application raised interesting procedural issues about what constituted a "complaint" for the purposes of s. 13 and 14.

Court status

Although no complaint was accepted and no Commissioner's report issued, Mr. Lavigne filed a section 14 Application in Court, asking the Court to rule on the merits of the complaint and seeking damages from CUPW. CUPW brought a motion to strike the Application while Mr. Lavigne sought leave to convert the Application into an action. The Federal Court granted CUPW's motion and the Application was struck in August 2003 with costs to the Respondent.

Yukon Hospital Corporation v. Privacy Commissioner of Canada

Federal Court File T-1451-03

Complaint

The Office of the Privacy Commissioner received a complaint from an employee alleging that the Whitehorse General Hospital had refused a request for access to her personal information in its possession. The Hospital was accordingly notified that a complaint had been received and that an investigation was being commenced.

The Hospital took the position that in order for *PIPEDA* to apply, the hospital must either engage in commercial activities or operate a federal work, undertaking or business. It was their opinion that neither of these applied, and therefore that the hospital was not subject to *PIPEDA*. In contrast, the Commissioner took the position that intra-territorial enterprises in the three territories fall within the definition of "federal work, undertaking or business" by virtue of s. 2(1) definition of "federal work, undertaking or business", specifically subsection (i) "outside the exclusive legislative authority of the legislatures of the provinces" and thus that employees of organizations such as the Whitehorse General Hospital fall within the jurisdiction of *PIPEDA*. As such, the Office intended to continue with its statutorily mandated investigation.

OPC involvement

The Commissioner was required to respond to the judicial review application directed at the Office's assertion of jurisdiction.

Court status

The Hospital filed an Application under s. 18.1 of the *Federal Court Act*, requesting judicial review of the Privacy Commissioner's decision that the Whitehorse General Hospital was subject to *PIPEDA* and the subsequent decision to proceed with an investigation.

Ultimately, the complainant reached a settlement with the Hospital, part of which was the withdrawal of her complaints to the Office of the Privacy Commissioner. When her complaints were withdrawn, the Application for judicial review was formally discontinued in February 2004.

Blood Tribe Department of Health v. Privacy Commissioner of Canada

Federal Court File No. T-2222-03

Complaint

A complaint was filed with the Office of the Privacy Commissioner alleging (among other things) that the Blood Tribe Department of Health denied an individual access to her personal information and did not provide reasons for the denial. Although the Commissioner needs access to all documents in order to ensure that exemptions claimed have been properly applied and to guard against abuse, in the course of the investigation, the Blood Tribe Department of Health refused to provide the Privacy Commissioner with access to solicitor-client privileged documents. As a result of the refusal, the Office of the Privacy Commissioner issued an Order for the production of records pursuant to sections 12(1)(a) and (c) of *PIPEDA*.

OPC involvement

The Commissioner was required to respond to the judicial review application directed at the Office's assertion of jurisdiction.

Court status

The Blood Tribe Department of Health filed an Application for judicial review, under s. 18.1 of the *Federal Court Act*, of the decision of the Office to issue the Order for production. The Application was filed in Federal Court in October 2003 but incorrectly named the Respondent. The Notice of Application has been amended and was properly served on 3 June 2004. The Application is now progressing normally.

Canada (Attorney General) v. Canada (Information Commissioner), 2004 FC 431, [2004] F.C.J. No. 524

Although the Privacy Commissioner was not involved in the following proceedings, this was an important decision for the Office given that both the Information and Privacy Commissioners have the same investigative powers set out under their parallel Acts.

In March 2004 the Federal Court dismissed 25 applications for judicial review which had been filed by the government in an attempt to limit the investigative powers of the Information Commissioner.

The government had challenged the Information Commissioner's authority to investigate, arguing that the Prime Minister's Office and Ministerial offices are separate and distinct from the Privy Council Office or a Minister's department. The Court found that it was premature to rule on whether the records were subject to the *Act* and that the Commissioner should have been allowed to complete his investigation and report before such issues were raised. In so finding, the Court recognized the importance of the Commissioner's investigative role and independent review where rights of access are in dispute.

The government has appealed only one narrow legal point of the ruling dealing with whether the Information Commissioner has the right to see a legal memorandum.

PART THREE

Corporate Services

Our path toward institutional renewal

It has been a challenging year for our Office due to the chain of events surrounding the resignation of the former Commissioner in June, 2003. A Parliamentary Committee inquiry, Auditor-General's report, a Public Service Commission investigation and numerous internal reviews and audits took time and energy from normal office functions. These audits and reviews highlighted that there had been a major breakdown of external governance and internal control processes at the OPC. In response, our Office has taken substantial steps to rebuild and renew the agency.

A series of corrective measures have been and continue to be taken to improve our office management framework and processes. These include:

- The appointment of two Assistant Commissioners and a Chief Financial Officer
- The establishment of an External Advisory committee of national privacy experts
- A Modern Comptrollership action plan has been submitted to Treasury Board
- Training in financial management policies, as well as Values and Ethics, has been provided to managers and staff
- Appointment of the Assistant Commissioner as OPC Values & Ethics Champion
- Development of a Human Resources strategy and action plan has been developed
- The establishment of Health & Safety and union-management consultation committees
- A Canada School of Public Service learning program is being implemented for staff

An important part of our internal renewal was the strategic planning process that was launched in January 2004. This was a transparent planning exercise with considerable

staff involvement. The process established an overall framework for the development of OPC strategies, and key actions for the fiscal year 2004-2005. The resulting strategic framework formed the basis of our Report on Plans and Priorities, which was submitted to Treasury Board in April.

One of the key strategic outcomes identified by senior staff in the strategic planning exercise for the OPC is, "*To be a well-managed, effective and efficient Parliamentary agency*". The development and implementation of a modern comptrollership plan is at the heart of the OPC achieving this objective. The Modern Comptrollership Action Plan that was completed, and submitted to Treasury Board in March will help us ensure that adequate management processes and controls are in place, providing a strong foundation for the Office's activities. Regular communication to staff on Modern Comptrollership and status reports to senior management will instil a modern comptrollership culture, and ensure that modern comptrollership-related principles and practices are followed.

The Modern Comptrollership framework for the Office includes a strong human resources focus. Key elements include shared values and ethics — and motivated staff. We are placing emphasis on these important aspects of the modern comptrollership framework as part of the overall renewal of the OPC.

Some of the other major corporate services accomplishments in 2003-2004 were:

- Launch of Integrated Investigation Application (IIA), an integrated caseload management system that supports key business processes.

- Completion of an Information Technology (IT) threat and risk analysis looking at issues such as security and IT operations. Many of the recommendations highlighted in this analysis, including those specifically relating to the integration of the external and internal networks, have been implemented.

- Completion and roll out of a revised delegation of financial authority framework.

- Provision of training to OPC staff on important financial policies, such as delegation, travel and hospitality.

- Development of an accommodation strategy for OPC.

- Enhancement of controls in the contracting process.

In FY 2004-05 the Corporate Services group will be focusing on initiatives in areas such as performance measurement, the streamlining of business processes, and human resources planning and management within the OPC.

At the beginning of fiscal year 2003-2004, the Office's budget was $11.2 million, the same as our budget of the previous year. Included in our budget was $6.7 million for the Office's *PIPEDA* activities. Funding of OPC activities has been and continues to be an important issue.

Initially, *PIPEDA* funding was provided for a three year period ending March 31, 2004, to allow the OPC to administer the new *Act*. This *Act* first came into force for certain sectors, specifically federally-regulated business, in January 2001. As of January 2004, however, the scope of the *Act* has increased to include the entire private sector. When funding was provided for the first three years of *PIPEDA*, the expectation was that towards the end of the three year period the Office would evaluate its experience in undertaking *PIPEDA*-related activities, and would confirm with Treasury Board its on-going funding requirements for this work.

Unfortunately, as a result of the events of FY 2003-2004 relating to the resignation of the former Commissioner, we were unable to perform this review with Treasury Board. At the end of fiscal 2003-2004, we obtained one year bridge funding for the OPC *PIPEDA*-related activities for fiscal 2004-2005. The Office is currently reviewing its financial resources, and plans to make a submission to Treasury Board in the fall of 2004 for on-going funding under both the *Privacy Act* and *PIPEDA*.

Resources

April 1, 2003 to March 31, 2004

	Expenditure Totals ($)	% of Totals
Privacy Act	4,171,661	37.61 %
PIPED Act	4,768,650	42.99 %
Corporate Services	2,151,980	19.40 %
Total	11,092,291	100.00 %

Note that as of March 2004 there were 95 full time staff positions at the Office of the Privacy Commissioner of Canada

Detailed Expenditures [1]	*Privacy Act*	*PIPED Act*	Corporate Services	Total
Salaries	3,605,276	3,176,545	401,153	7,182,974
Employee Benefits Program	198,097	878,851	160,870	1,237,818
Transportation & Communication	108,074	93,266	238,789	440,129
Information	70,366	80,773	76,088	227,227
Professional Services	191,986	385,886	588,181	1,166,053
Rentals	16,328		82,277	98,605
Repairs & Maintenance			291,026	291,026
Materials & Supplies	8,613	3,330	82,454	95,397
Acquisition of Machinery & Equipment		150,000	230,985	380,985
Other Subsidies & Payments	-27,079		156	(26,923)
Total	$4,171,661	$4,768,651	$2,151,979	$11,092,291

[1] Total expenditure figures are consistent with the public accounts.

Financial statements

Over the past several years, as part of the Financial Information Strategy, the Receiver General for Canada and departments have worked to put in place new financial information systems and to acquire the accounting expertise required to implement full accrual accounting. Overseeing this initiative, the Treasury Board Secretariat also developed the necessary accounting policies and training programs to implement full accrual accounting government-wide.

Under full accrual accounting, an entity's financial statements provide a more comprehensive and up-to-date picture of its financial situation and better reflect the impact of economic events and decisions made during the fiscal year. Better information means improved transparency and accountability.

Publication of accrual-based financial statements is being phased in for departments and agencies. Departmental corporations began presenting accrual-based financial statements in Volume II Part II of the *2001-2002 Public Accounts of Canada*. For 2003-2004, the offices of the five agents of Parliament (the Offices of the Auditor General, Chief Electoral Officer, Commissioner of Official Languages, Privacy Commissioner and Information Commissioner) will report accrual-based financial statements in accordance with generally accepted accounting principles. Information on the use of their appropriations is contained in the preceding reports presented in the following tables.

In general terms, the use of appropriations focuses on spending and the acquisition of resources. Accrual accounting reports the cost of resources consumed during the year as well as reporting the assets and future financial obligations. For further details on the adoption of full accrual accounting, please refer to Annex 6 in *The Budget Plan 2003*.

The Management Responsibility letter and the audited financial statements as at March 31, 2004 are available on our web site http://www.privcom.gc.ca.