12,160,282

…and that's just
the people in Ontario
who are entitled to open,
accountable government and
strong privacy protection

INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

2006 ANNUAL REPORT

Information and Privacy
Commissioner/Ontario
Commissaire à l'information
et à la protection de la vie privée/Ontario

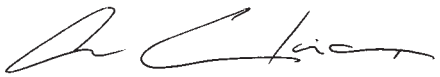
May 29, 2007

The Honourable Michael Brown,
Speaker of the Legislative Assembly

I have the honour to present the 2006 annual report of the Information and Privacy Commissioner of Ontario to the Legislative Assembly.

This report covers the period from January 1, 2006 to December 31, 2006.

Sincerely yours,



Ann Cavoukian, Ph.D.
Commissioner

2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

Tel: 416-326-3333
1-800-387-0073
Fax/Téléc: 416-325-9195
TTY: 416-325-7539
www.ipc.on.ca

Commissioner's Message

WHILE THERE WERE SOME PROGRESSIVE STEPS TAKEN IN 2006 IN BOTH THE ACCESS AND PRIVACY FIELDS, NEW CHALLENGES AROSE. Among the positive steps was the first *Right to Know Week* in Ontario, which my office used as a springboard to promote the underlying principles of freedom of information. Another was the groundswell of support – which has continued to grow – for the *Privacy-Embedded 7 Laws of Identity*, which I unveiled in October. These 7 Laws are about the need to have control over our personal information in the digital world, just as we do in the real world. And, later in October, Privacy and Data Protection Commissioners from around the world accepted the *Global Privacy Standard (GPS)* that a committee of international commissioners, which I chaired, brought forward. The GPS represents a harmonization of fair information practices into a single instrument, and for the first time, includes the language of data minimization.

CULTURE OF PRIVACY

I need to raise a truly regrettable situation that occurred at an Ontario hospital to drive home the point that having a privacy policy, in and of itself, is not enough: A culture of privacy must be developed so that everyone handling personal information understands what may or may not be done with it.

A patient admitted to the Ottawa Hospital made a specific request to ensure that her estranged husband, who worked at that hospital, and his girlfriend, a nurse at the hospital, did not become aware of her hospitalization, and that steps be taken to protect her privacy. She learned later that the nurse had repeatedly gained access to her personal information.

Despite having clearly alerted the hospital to the possibility of harm, the harm occurred nonetheless. While the hospital had policies in place to safeguard health information, they were not followed completely, nor were they sufficient to prevent a privacy breach from occurring. In addition, the fact that the nurse chose to disregard, not only the hospital's policies, but her ethical obligations as a registered nurse, and continued to surreptitiously access a patient's electronic health record,

disregarding three warnings alerting her to the seriousness of her unauthorized access, is especially troubling. Protections against such blatant disregard for a patient's privacy by an employee must be built into the policies and practices of all health care institutions.

As I emphasized in the postscript to the order I issued, HO-002:

> "This speaks broadly to the culture of privacy that must be created in health care institutions across the province. Unless policies are interwoven into the fabric of a hospital's day-to-day operations, they will not work. Hospitals must ensure that they not only educate their staff about the *Act* and information policies and practices implemented by the hospital, but must also ensure that privacy becomes embedded into their institutional culture."
>
> "As one of the largest academic health sciences centres in Canada, the Ottawa Hospital had properly developed a number of policies and procedures; but yet, they were insufficient to prevent members of its staff from deliberately undermining them."

I urge all health information custodians and access and privacy staff to read this order, available on our website, **www.ipc.on.ca**, and to develop a culture of privacy in their organizations.

Upholding compliance with Ontario privacy legislation is not simply a matter of following the provisions of enacted legislation, but ensuring that the use and disclosure of sensitive personal information is strongly monitored, and access controlled to those who truly need it in the performance of their duties.

Regardless of the type of institution or health care provider – from a town hall to a police service, from a library board to a school board, from a university to a hospital, a doctor's office or a health clinic – predicating access to personal information on a "need to know" basis is vital.

THE PRIVACY-EMBEDDED 7 LAWS OF IDENTITY

I was struck by the growing disconnect between the real and the digital worlds when it came to disclosing personally identifiable information and proving identity. Surveillance and fraud appear to be far more rampant in the online world. Individual users are losing control over what personal information is collected about them, by whom, and for what purposes, resulting in profound consequences for privacy. With the loss of control comes a loss of confidence and trust in the Internet as a beneficial medium for enriching our lives. And the tension is mounting, because the next generation of intelligent and interactive web services ("Web 2.0") will require more, not fewer, verifiable identity credentials, and much greater mutual trust in order to succeed.

This is why I published a set of privacy-embedded "laws of identity" to help guide the development of interoperable identity management systems in a privacy-enhanced way. I wanted to help minimize the risks that one's online identities and activities would be recorded and linked together, without one's knowledge or consent. Just as important, identity systems that are consistent with the *Privacy-Embedded 7 Laws of Identity* will help consumers verify the identity of legitimate organizations before they decide to proceed with an online transaction.

The privacy-embedded laws were inspired by the 7 Laws of Identity formulated through a global dialogue among security and privacy experts, headed by Kim Cameron, Chief Identity Architect at Microsoft. The *Privacy-Embedded 7 Laws of Identity* offer individuals:

- easier and more direct user control over their personal information when online;
- enhanced user ability to minimize the amount of identifying data revealed online;
- enhanced user ability to minimize the linkage between different identities and actions; and
- enhanced user ability to detect fraudulent messages and websites, thereby minimizing the incidence of phishing and pharming.

We have called upon software developers, the privacy community and public policy-makers to consider the *Privacy-Embedded 7 Laws of Identity* closely, to discuss them publicly, and to take them to heart.

And we see evidence of that already happening. Some of the largest companies and groups in the technology field have stepped forward to present their own identity management projects and to explain how their solutions are user-centric, privacy-respectful and privacy-enhancing. The IPC is currently holding talks with several collaborative, open-source identity management initiatives, such as members

of Liberty Alliance (including companies such as Oracle, Sun Microsystems, and Hewlett-Packard) and members of Project Higgins (which includes IBM among many others), to further advance privacy in the identity age.

For our foundation paper on the *Privacy-Embedded 7 Laws of Identity*, go to: **http://www.ipc.on.ca/images/Resources/up-7laws_whitepaper.pdf.**

TRANSPARENCY AND ACCOUNTABILITY

The rights of citizens to access government-held information is essential in order to hold elected and appointed officials accountable to the people they serve. In my last annual report, I focused on the need for public accountability on the expenditure of public funds and recommended that all contracts entered into by government institutions for the provision of programs or services be made public on a routine basis.

That would only be the initial step. I am now calling on government organizations to make the full procurement process much more transparent – releasing information not only about the winning bid, but of all bids. Ensuring the integrity and effectiveness of the procurement process is an essential element of government accountability.

This issue is reviewed in depth in the *Issues* section of this annual report (including a look at how several provinces and states provide accountability). I also make a very specific recommendation in the *Commissioner's Recommendations* section.

KEY COURT DECISIONS

In two landmark decisions released in late 2006, the Divisional Court affirmed, for the first time, that I have the authority as part of my "legislative" functions to investigate and report on privacy complaints brought by members of the public against government institutions, despite the absence of an explicit grant of power under either the *Freedom of Information and Protection of Privacy Act* or the *Municipal Freedom of Information and Protection of Privacy Act*. I have been making the case for this outcome for many years and I am pleased to see the Court rule in our favour. At the same time, the Court held that my privacy rulings are protected by "Parliamentary privilege" and are not subject to judicial review by the courts because they fall within my general oversight and reporting mandate as an Officer of the Legislature.

Also in 2006, in its first judgment relating to an application for judicial review of an IPC decision, the Supreme Court of Canada established new guidelines governing the Ontario Courts' processes on judicial review of the IPC's decisions on access appeals.

More information on these and other key 2006 court decisions is presented in the *Judicial Reviews* section of this annual report.

CREATION OF A GLOBAL PRIVACY STANDARD

In 2005, at the 27th International Data Protection Commissioners Conference, I chaired a Working Group of Commissioners, which was convened for the sole purpose of creating a single Global Privacy Standard. With globalization and the convergence of business practices, and massive developments in technology, which knows no borders, I believed there was a pressing need to harmonize various sets of fair information practices into a single Global Privacy Standard. Once such a foundational policy piece was in place, businesses and technology companies could turn to a single instrument for evaluating whether their business practices or information systems were actually privacy enhancing, both in nature and substance.

My office embarked on the preliminary work of conducting a "gap analysis" – examining the leading privacy practices and codes from around the world to compare their various attributes, and the scope of the privacy principles enumerated therein. We identified the strengths and weaknesses of the major codes in existence and then tabled our gap analysis with the Working Group of Commissioners.

In the ensuing months, we embarked upon the work of harmonizing the privacy principles into a single set of fair information practices. This led to the development of the Global Privacy Standard (GPS), which builds upon the strengths of existing codes containing time-honoured privacy principles and, for the first time, reflects a noteworthy enhancement by explicitly recognizing the concept of "data minimization" under the collection limitation principle.

The final version of the GPS was formally tabled and accepted on November 3, 2006 at the 28th International Data Protection Commissioners Conference, in the United Kingdom.

The Global Privacy Standard reinforces the mandate of privacy and data protection authorities by:

- focusing attention on fundamental and universal privacy concepts;
- widening current privacy awareness and understanding;

- stimulating public discussion of the effects of new information and communication technologies, systems, standards, social norms, and laws, on privacy; and
- encouraging ways to mitigate threats to privacy.

The GPS addresses privacy concerns for decision-makers in any organization that has an impact on the way in which personal information is collected, used, retained, and disclosed. The GPS is intended to enhance, not pre-empt, any laws or legal requirements bearing upon privacy and personal information in various jurisdictions.

BUILDING EXTERNAL RELATIONSHIPS

One of this office's strengths is in forging external relationships; in this way, we are able to extend our influence and more effectively fulfil our research and educational responsibilities, and thus create "win-win" outcomes with partners from both the public and private sectors. In 2006, in addition to the GPS, we had the privilege of working with numerous organizations on projects covering a wide range of topics. They include:

- **The *Privacy-Embedded 7 Laws of Identity***, described above, with Microsoft's Chief Identity Architect, Kim Cameron, and subsequent discussions with other interested parties, including IBM, Oracle and Sun Microsystems;
- **Two papers on RFID (radio frequency identification) systems**. We worked with EPCglobal Canada, an industry association that sets standards for electronic product codes. After discussing core privacy principles and learning more about the technological potential of RFIDs, I released a video early in 2006, *A Word about RFIDs and your Privacy in the Retail Sector* (which, in addition to being available from my office, is being aired at the RFID Information Centre in Markham, Ontario). In June, I released *Privacy Guidelines for RFID Information Systems* and a second paper, *Practical Tips for Implementing RFID Privacy Guidelines*, explaining how responsible businesses can implement RFID systems in a privacy-protective manner;
- **Ontario's first *Right to Know Week***. We worked with the Toronto Region branch of the Institute of Public Administration of Canada and the Canadian Newspaper Association to organize the sold-out luncheon that was the focal point of the week.
- ***Reduce Your Roaming Risks – A Portable Privacy Primer***, released in September, was the result of a collaboration between my office and the BMO Financial Group. This practical, hands-on brochure outlines specific steps that people working away from the traditional office – and using mobile devices such as laptops and PDAs – can take to reduce the chances that the personal information in their care will be lost or stolen;
- ***When Online Gets Out of Line – Privacy: Make an Informed Online Choice***, a brochure released in October, encourages users of online social networking sites to carefully consider their privacy options. Social networking websites quickly became a significant technological and social phenomenon in 2006, with a number of media reports about the security and privacy issues involved. We met with officials from Facebook, one of the largest social networking sites, and also set up a focus group of college and university students, to find out directly from both the creators and users what this phenomenon was all about, and then produced our brochure.
- ***Breach Notification Assessment Tool.*** This structured assessment tool was jointly produced by my office and that of my counterpart in British Columbia, Commissioner David Loukidelis, in mid-December. It will guide organizations through a review of notification issues if a privacy breach occurs.
- **Ethics at Ryerson Speaker Series**. We were pleased to be the presentation partner for the first year of Ryerson University's *Faculty of Arts Ethics Network Speaker Series*. The 2006-7 theme was *Privacy and Access Issues Across the Professions*. The opening lecture in this series, which I delivered, was the launch event for our *When Online Gets Out of Line* brochure about online social networking. Among the other speakers were Alan Borovoy of the Canadian Civil Liberties Association, CBC Ombudsman Vince Carlin, and my Assistant Commissioner for Privacy, Ken Anderson.
- Among other interactions, I was very pleased to accept the invitation of Ontario Government Services Minister Gerry Phillips to sit on the Independent Advisory Committee to provide advice to the provincial government on best practices for managing business transformation of the public service through information and

information technology (I&IT). This is the next phase of a process of transforming how the Ontario Public Service handles large I&IT projects. Previously, I served on the Chair's Advisory Committee on e-Government.

- I am also serving on the International Biometric Advisory Council, which was established in 2005 to provide advice and expert opinion to the European Biometrics Forum, its members and partners, on the most pertinent issues facing biometrics globally. A charter has been developed and fruitful discussions begun about testing, certification, privacy and data protection.

Many of these relationships underline a belief I have held ever since I first joined the IPC in its very early days, some two decades ago: *technology transcends jurisdiction*. Along with the Dutch Data Protection Authority, we co-developed the concept and methodology recognized around the world today as *privacy-enhancing technologies*, or *PETs*. I have consistently spoken out, across Canada and internationally, in favour of building privacy directly into technology at the design stage, not added on as an afterthought, or later "fix." We affectionately call this "*privacy by design*."

Similarly, privacy must be built into organizational cultures in the most pervasive ways possible – whether the setting be a corporate boardroom, a hospital nursing station, a government ministerial office or a town hall – through widely dispersed written policies, employee orientation and update seminars, evaluation, shareholders meetings, management retreats, etc. Good privacy practices must become the norm, not the exception – build them in!

MY PERSONAL THANKS

Again, I would like to sincerely thank all of the wonderful staff in my office. With the external changes and vast pressures in the FOI and privacy fields in recent years, the demands on my office have grown significantly. My staff have not only met, but repeatedly exceeded the growing expectations placed upon them. Everyone at the IPC takes their responsibilities, and the mandate of this office, very seriously, and I am both very proud of my team, and exceedingly grateful. You have my heartfelt thanks, now, as always.

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner of Ontario

Your identity, your choice: make these work for you

Table of Contents

The Purposes of the Acts

The purposes of the *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act* are:

a) To provide a right of access to information under the control of government organizations in accordance with the following principles:

- information should be available to the public;
- exemptions to the right of access should be limited and specific;
- decisions on the disclosure of government information may be reviewed by the Information and Privacy Commissioner.

b) To protect personal information held by government organizations and to provide individuals with a right of access to their own personal information.

The purposes of the *Personal Health Information Protection Act* are:

To protect the confidentiality of personal health information in the custody or control of health information custodians and to provide individuals with a right of access to their own personal health information and the right to seek correction of such information, with limited exceptions.

Role and Mandate

Ontario's *Freedom of Information and Protection of Privacy Act (FIPPA)*, which came into effect on January 1, 1988, established an Information and Privacy Commissioner (IPC) as an officer of the Legislature, who is appointed by and reports to the Legislative Assembly of Ontario and is independent of the government of the day.

The *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA),* which came into effect January 1, 1991, broadened the number of public institutions covered by Ontario's access and privacy legislation.

The *Personal Health Information Protection Act, 2004 (PHIPA)*, which came into force on November 1, 2004, is the third of the three provincial laws for which the IPC provides oversight. *PHIPA* governs the collection, use and disclosure of personal health information within the health care system.

The Commissioner's mandate is to provide an independent review of the decisions and practices of government organizations concerning access and privacy; to provide an independent review of the decisions and practices of health information custodians in regard to personal health information; to conduct research on access and privacy issues; to provide comment and advice on proposed government legislation and programs; to review the personal health information policies and practices of certain entities under *PHIPA*; and to help educate the public about Ontario's access, privacy and personal health information issues and laws.

The Commissioner plays a crucial role under the three *Acts*. Together, *FIPPA* and *MFIPPA* establish a system for public access to government information with limited exemptions, and for protecting personal information held by government organizations at the provincial or municipal level. *PHIPA* establishes privacy rules for the protection of personal health information held by health information custodians and provides a right of access to an individual's own personal health information.

FIPPA applies to all provincial ministries and most provincial agencies, boards and commissions, and to universities and colleges of applied arts and technology. *MFIPPA* covers local government organizations, such as municipalities; police, library, health and school boards; public utilities; and transit commissions.

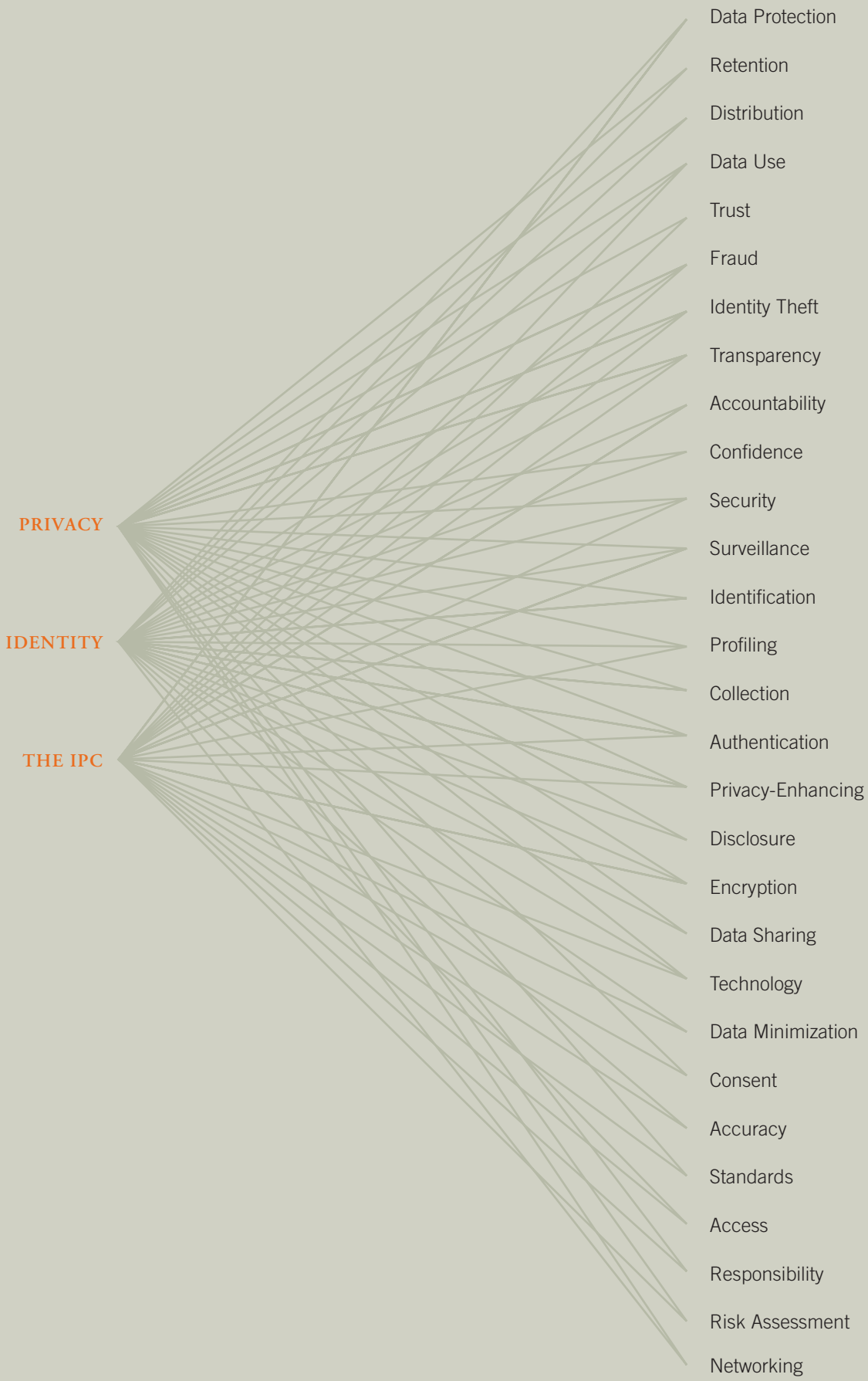
Freedom of information refers to public access to general records relating to the activities of government, ranging from administration and operations to legislation and policy. The underlying objective is open government and holding elected and appointed officials accountable to the people they serve.

Privacy protection, on the other hand, refers to the safeguarding of personal information – data about individuals held by government organizations, and personal health information in the custody or control of health information custodians. The three *Acts* establish rules about how government organizations and health information custodians may collect, use and disclose personal data. In addition, individuals have a right of access to their own personal information – and to seek correction of these records, if necessary.

To safeguard the rights established under the *Acts*, the IPC has seven key roles:

- resolving appeals when government organizations refuse to grant access to information;
- investigating privacy complaints related to government-held information;
- ensuring that government organizations comply with the *Acts*;
- conducting research on access and privacy issues and providing advice on proposed government legislation and programs;
- educating the public about Ontario's access, privacy and personal health information laws and access and privacy issues;
- investigating complaints related to personal health information;
- reviewing policies and procedures, and ensuring compliance with *PHIPA*.

In accordance with the legislation, the Commissioner has delegated some of the decision-making powers to various staff. Thus, the Assistant Commissioner (Privacy), Assistant Commissioner (Access) and selected staff were given the authority to assist her by issuing orders, resolving appeals and investigating privacy complaints.


PRIVACY
IDENTITY
THE IPC
Data Protection
Retention
Distribution
Data Use
Trust
Fraud
Identity Theft
Transparency
Accountability
Confidence
Security
Surveillance
Identification
Profiling
Collection
Authentication
Privacy-Enhancing
Disclosure
Encryption
Data Sharing
Technology
Data Minimization
Consent
Accuracy
Standards
Access
Responsibility
Risk Assessment
Networking

Identity, the IPC, and the Future of Privacy

IDENTITY MANAGEMENT IS AT THE HEART OF PRIVACY. THERE IS EVERY REASON TO BELIEVE AND EXPECT THAT IDENTITY-RELATED ISSUES WILL DOMINATE THE PRIVACY AND DATA PROTECTION AGENDA IN THE COMING YEARS.

In the public sector, government, health care and educational organizations are all undergoing large-scale IT-enabled transformations in their operations that depend critically upon concepts of identity and the use of identifiers. These institutions are also evaluating why and how to identify citizens, their stakeholders and clients.

In the private sector, with the advent of networked databases and real-time data collection, retrieval and processing, we are witnessing a tremendous explosion in the creation, storage and distribution of personally-identifiable information. Most of this data is controlled by others.

At the same time, identification requirements are growing stronger and more ubiquitous in both the real and online worlds. Increasingly, we are required to prove who we are – and this identity data is being recorded in database files and dossiers.

Inaccurate information in our files can result in poor inferences and bad decisions that impact us adversely. We can be denied a service, or credit, or perhaps a job or promotion, medical insurance or treatment, or even our freedom to travel, because of poor identity data. As well, identity theft and fraud are Information Age crimes that are fuelled by the theft and misuse of personal information. Without openness, transparency and accountability on the part of all organizations that collect and use our personally-identifiable information, individuals will pay the price of errors, incompetence and poor security, yet rarely be in a position to understand what is happening to their data, or be able to take effective counteraction.

We are generating and leaving behind detailed data trails that contain personal identifiers that may later be linked to us. These data trails can and are being correlated into dossiers and profiles that constitute our "digital shadows." These shadow identities are accessible to more and more entities, and may be used for a variety of different purposes – with growing impacts on real individuals. The era of privacy by practical obscurity is over. The locked filing cabinets of yesteryear have nearly vanished, and their data contents have long been digitized and connected to the grid, to serve as yet another feed into the global information commons, to be indexed, mirrored, and matched, at will.

In today's digital world, individuals are losing control over what information is collected about them by others, and for what purposes. Entirely new industries have arisen in the past generation that are based upon the collection, processing and sale of personally-identifiable information products. This is an industry that is largely opaque to the average individual.

The collection, use and disclosure of identifiers by public and private entities impacts our ability to lead private lives. In part, this is because identifiers are very useful for matching and correlating – and for making decisions that affect us. And, the more identifiable we are to others (and our activities, thoughts, etc.), the more we become susceptible to surveillance and profiling.

PROTECT IDENTITY

There is no question that we must protect identity. We may not be able to put the information genie back in the bottle, but we can collectively set and enforce limits on permissible levels of collection, use and disclosure of personally-identifiable information by organizations, vest individuals with certain rights that organizations must observe, and hold those organizations accountable for actions that impact negatively on the privacy of individuals and the security of our freedoms.

Personally-identifiable information is a special category of sensitive data that, more than ever, organizational custodians must treat as both an asset and a liability, and manage in a principled and verifiable manner.

This office has consistently advocated that the collection, use and disclosure of identifiable data:

- must be minimized wherever possible. The best privacy protection means not collecting, using or disclosing personal data in the first place, wherever possible. Fair information practices that *limit* purposes, collection, use and retention, express this requirement;
- must involve the individual data subject in a meaningful manner throughout the data's entire life cycle. Fair information practices of accountability, openness, informed consent, accuracy, access and the availability of redress mechanisms promote such involvement; and
- must be managed responsibly, credibly, and securely, because the negative impacts of poor information management fall disproportionately on the individual; in turn, confidence and trust in the organization may be seriously undermined.

IPC ACTIVITY

Many of the IPC's privacy activities and accomplishments in 2006 have been targeted at identity-related information issues and concerns.

1. **Privacy-Embedded 7 Laws of Identity:** In October, the IPC began advancing a set of design principles for interoperable identity management systems to help fight online fraud, empower users, and minimize surveillance by putting Internet users in maximal control of their own identities and their identifying data online. The Commissioner's ground-breaking white paper, *7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity in the Digital Age*, outlines the pressing need to minimize the risk that one's online identities and activities will be linked together.

WHO'S WATCHING WHOM?

ARE YOU TRULY SECURE?

2. **Radio Frequency Identification (RFID):** In June 2006, the IPC unveiled a set of privacy guidelines and practical tips, modeled after the CSA Privacy Code, for deploying item-level RFID tags and information systems. RFID tags contain globally-unique identifiers that may be linked with individual consumers at the point of sale.

3. **Online Social Networking:** In October 2006, the IPC initiated a public education campaign targeted at university students to drive home the message that personal information, when posted online in social networking environments, can be broadcast and may persist forever on the Internet, only to come back and haunt them years later. We advise the careful use of pseudonyms, restraint in posting personal identity information, and granting a limited circle of friends access. The IPC has since launched a public education campaign aimed at high schools.

4. **Identity Theft:** Throughout 2006, the IPC repeatedly emphasized that organizations – not just victims – must do a better job of managing their information assets and in protecting their customers. In this regard, privacy insights can help strengthen security and foster consumer trust and confidence. Commissioner Cavoukian has been an active champion in communicating to government the need of Ontarians for legislation to combat identity theft and fraud, and to protect identity.

5. **Used Goods:** Throughout 2006, the IPC was a strong critic of efforts to require mandatory identification, recording and national reporting of sellers of used goods. The untrammelled creation and use of a national, searchable database of law-abiding sellers' identities by law enforcement lies at the heart of our concerns.

6. **Identity Cards/Border Control:** During 2006, the IPC raised a number of issues related to the possible creation of identity cards for use at the U.S. border, notably by advocating directly to the Premier that Ontario drivers' licences be an acceptable means of strong identification for border crossings. Ontario citizens should have a choice of which identity documents they present to prove identity, and the Ontario driver's licence is a credible alternative to a passport.

7. **Biometrics:** Throughout 2006, the IPC remained a strong advocate for local *one-to-one* biometric authentication over *one-to-many* identification uses and the creation of central databases. The IPC has advanced this view in national and international forums and in biometric advisory councils. Work has begun to demonstrate the privacy and security-enhancing benefits of biometric encryption technologies.

8. **Health Care:** Many pilot projects are under way in Ontario for the sharing of health information over electronic mediums in the form of *electronic health records*

WHEN ONLINE GETS OUT OF LINE: PRIVACY – MAKE AN INFORMED ONLINE CHOICE.

PRINT THIS... REALLY... AND KEEP IT IN A DATABASE?

(EHR). The IPC devotes extensive staff time to a variety of consultations with organizations working in Ontario on existing or proposed EHR projects, such as System Design Principles for Information Technology in co-operation with the Ministry of Health and Long-Term Care and the e-Health Council, and in the development of electronic information-sharing approaches for laboratory and diagnostic imaging information, as well as emergency department access to drug information. As well, in August the IPC completed an investigation into possible CIA access to personal health information via software being used in provincial electronic health records. The investigation concluded that no personally-identifiable health information flows outside of Ontario.

9. **Global Privacy Standard (GPS):** In 2006, the IPC led a year-long initiative by the International Community of Data Protection (data minimization) Commissioners to harmonize the multitude of existing sets of fair information practices (FIPs) currently in use around the world. The result, the Global Privacy Standard, a single, harmonized set of privacy principles, is the first set of FIPs that explicitly specifies the requirement to minimize all identifiable data used in the design and operation of information systems.

10. **Breach Notification Project:** The IPC believes that the loss or theft of personally-identifiable information held by a public (or private) organization entails a duty to notify affected individuals. In late 2006, the IPC worked with the Information and Privacy Commissioner of British Columbia on a joint project to develop a *Risk Assessment/Decision Tool* regarding notification of privacy breaches. This document is intended to assist public and private sector organizations in determining their obligations in the event of a breach. The document offers guidance on who should be notified (those affected); how the notification should be carried out; and in the absence of legislation mandating notification, what factors (including severity of harm; assessment of risk) should come into play in making a decision as to whether to notify.

LOOKING AHEAD

The IPC is involved in the Ontario government's newly-created Task Force for Large-scale IT projects. We are gratified that the Ontario government saw fit, following recommendations by the Commissioner, to create a new position of Chief Information and Privacy Officer to help oversee the design and deployment of information and communication technologies across the public sector.

Single-window citizen-service and other online portals (all part of e-Government) are being designed to offer one-stop, real-time convenient access to personalized government services. Such projects raise profound questions about how Ontarians should identify themselves, to whom, and under what circumstances.

In the digital world, how will Ontarians identify themselves when conducting online transactions with their government agencies and institutions? Wouldn't it be efficient if Ontarians could easily access all their government files, in order to update them, to interact online with the agencies and departments, and to hold the latter more accountable? What if doing so opened the door to wide-scale identity fraud? The IPC will continue to work and advocate in this area.

Likewise, the ongoing digitization of – and networked access to – medical data offers enormous benefits to Ontarians, but profoundly difficult questions need to be answered about what personal information will be stored, where, who will have access to it, under what conditions, and what it will be linked to. The degree of confidentiality of the records is of great interest to the IPC, especially if data can be correlated with other records and re-identified. Ontarians expect and deserve the strongest privacy assurances when it comes to their personal health information.

The IPC will continue to be active in raising – and finding solutions to – important identity-related questions involving the privacy of Ontarians that are certain to arise in the coming months and years, and to bring these issues to the attention of the public for consideration, and public debate.

The Evolution of the Commissioner's Role with the Advent of *PHIPA*

SINCE THE ENACTMENT OF THE *PERSONAL HEALTH INFORMATION PROTECTION ACT (PHIPA)* IN LATE 2004, THE COMMISSIONER'S ROLE HAS BEEN UNDERGOING A FAIRLY DRAMATIC AND RAPID TRANSFORMATION. A NUMBER OF FACTORS HAVE CONVERGED TO CREATE THIS CHANGE. FIRST, *PHIPA* HAS BROADENED THE COMMISSIONER'S MANDATE IN A NUMBER OF IMPORTANT WAYS. SECOND, EXPECTATIONS ON THE PART OF THE GOVERNMENT FOR THE IPC AS AN OVERSIGHT BODY HAVE EXPANDED. THIRD, FOR THE FIRST TIME, PRIVATE SECTOR INDIVIDUALS AND ORGANIZATIONS FROM THE HEALTH CARE SECTOR HAVE COME WITHIN THE SCOPE OF THE IPC'S OVERSIGHT.

Traditionally, in addition to other key roles, the IPC has functioned as an independent tribunal with a mandate to resolving appeals about access to government-held information and complaints about privacy. In carrying out this role, the IPC has developed a certain degree of expertise in access and privacy issues in general. The government and the public have come to rely on this expertise in addressing a wide array of access and privacy issues. Accordingly, it came as no surprise when the government decided to make use of the IPC's independence and expertise to provide assurances in other areas.

Canada has a publicly-funded health care system. In an effort to make the system as efficient and effective as possible, personal health information derived through the provision of health care has been used and disclosed for a broad array of secondary purposes, such as health research and planning and managing our publicly-funded health care system. Such secondary uses are justified as being in the public interest. However, the use and disclosure of personal health information for secondary purposes, without the consent of the individuals to whom the information relates, is inconsistent with generally accepted fair information practices.

All health privacy legislation must balance the public interest in making personal health information available for secondary purposes and the public interest in respecting the privacy rights of citizens. In an effort to achieve this delicate balance, the use and disclosure of personal health information for secondary purposes, such as public health, is generally permitted, provided that strong safeguards are put in place to protect privacy. One such safeguard is to have an **independent third party** provide assurances that the organizations entrusted with personal health information adhere to good privacy practices. This is the approach that was adopted in *PHIPA*.

NEW MANDATE

PHIPA provided the IPC with a new mandate to review and approve the information practices of certain organizations in the health sector. Prescribed persons, who compile or maintain registries of personal health information for the purposes of facilitating or improving the provision of health care, are required to have their information practices reviewed and approved by the IPC. Similarly, prescribed entities that receive personal health information from custodians for the purpose of analysis or compiling statistical information for the planning and managing of the health care system are required to have their information practices reviewed and approved by the IPC. Four prescribed entities and four persons who compile or maintain registries have had their information practices reviewed and approved by the IPC.

OVEREXPOSED

It should be noted that, traditionally, independent tribunals such as the IPC have been reluctant to engage in such approval processes since there is the potential for a complaint to be raised in relation to one or more of the information practices that have been approved. The concern is that, where the IPC has approved an information practice, the IPC may not be a neutral party in resolving privacy complaints about such practices. To address this issue and ensure that the complaint resolution process remains unbiased by these other activities, our reviews and approvals are conducted completely outside of the activities of the Tribunal Branch (responsible for investigating complaints), by the IPC's Policy Department.

In order to conduct these reviews and approvals effectively, the IPC had to develop entirely new policies and procedures. It was decided that the new process should include, at a minimum, a review of relevant documentation and an on-site visit to the primary site where personal health information is retained by the organization. The site visit would provide an opportunity for the IPC to observe the physical security safeguards of the organization and to interview relevant staff from the organization. In addition, since the IPC had to actually approve the information practices of these organizations, it was decided that an iterative approach would be appropriate. Specifically, there would be successive rounds of comments by the IPC and revisions by the organization, until the information practices of the organization met the required standard set by the IPC. This iterative approach proved to be very effective and all prescribed entities and persons who maintain registries were successful in having their information practices approved by the November 1, 2005 deadline.

In developing the new review and approval process, the IPC started with a broad checklist of safeguards that we believed would form a solid foundation for any good privacy program. The initial checklist was constructed based on our past experience, but was continuously revised and expanded as the IPC gained more experience with the review and approval process. At the beginning of the process, organizations are informed that the IPC does not expect every organization to have every possible safeguard in place, but rather an appropriate combination of safeguards that is commensurate with the amount and nature of the personal health information retained by the organization.

In addition to developing new policies and procedures, the IPC found that it was necessary to acquire and develop certain expertise. Since a good privacy program consists of a combination of administrative, technical and physical safeguards, it was essential that the IPC have a certain level of expertise about information technology and security, especially as it relates to the health care sector. Accordingly, since the introduction of *PHIPA*, the IPC has worked to acquire and develop this technical expertise in-house, along with general health-sector-specific privacy expertise.

In addition to the review and approval of the information practices of prescribed entities and prescribed persons who maintain registries, *PHIPA* requires the IPC to review certain information practices of persons whose functions include the collection and preservation of records of historical or archival importance and who wish to act as recipients of personal health information from health information custodians. Before collecting any personal health information from a custodian, such persons must register their intention to act as an archive of personal health information with the IPC.

While only one such archive has come forward to date, the IPC has had to develop a new protocol for the registration of archives. It was decided that the registration process would involve a review of the information practices of the archive to ensure that they meet the requirements set out in section 14 of Ontario Regulation 329/04. The process that evolved was much more streamlined than the process that was developed for reviewing and approving the information practices of prescribed entities and prescribed persons who maintain registries. However, from the IPC's perspective, this was appropriate given the nature of the personal health information that would typically be transferred to such archives.

In 2006, a new regulation was passed requiring the Smart Systems for Health Agency, a health information network provider under *PHIPA*, to have its information practices reviewed by the IPC. This review was somewhat unique in that there was no requirement for the IPC to approve the information practices of the Smart Systems for Health Agency. Since health information network providers have a unique set of obligations under *PHIPA*, new policies and procedures for conducting the

review were required. In this case, it was determined that some expertise external to the IPC would be needed.

CHANGING EXPECTATIONS

The increasing demand for independent reviews, registrations and approvals reflects the changing expectations of the IPC on the part of the government. The IPC is no longer viewed only as an independent tribunal with a mandate for resolving complaints and appeals, but also as an independent third party with privacy and security expertise that can be used to provide assurances to the government and the public that organizations provided with privileged access to personal health information are handling the information with which they have been entrusted, in accordance with good privacy practices. The IPC has welcomed this new challenge.

Another factor that has contributed to the Commissioner's changing role is the nature of the individuals and organizations that fall within the scope of IPC's oversight. For the first time in its history, the IPC has a mandate to oversee the activities of individuals and organizations from the private sector. This required a shift in our approach and focus in a number of areas. First, with respect to education, the IPC recognized soon after the introduction of *PHIPA* that health information custodians, some of whom have limited resources, would require a significant degree of assistance from the IPC in implementing this novel and complex piece of legislation. To facilitate the implementation process, the IPC committed to providing health information custodians with a wide array of information resources and tools, to providing as much feedback as possible on the information practices of custodians, and to responding to all inquiries from custodians and the general public about the new law.

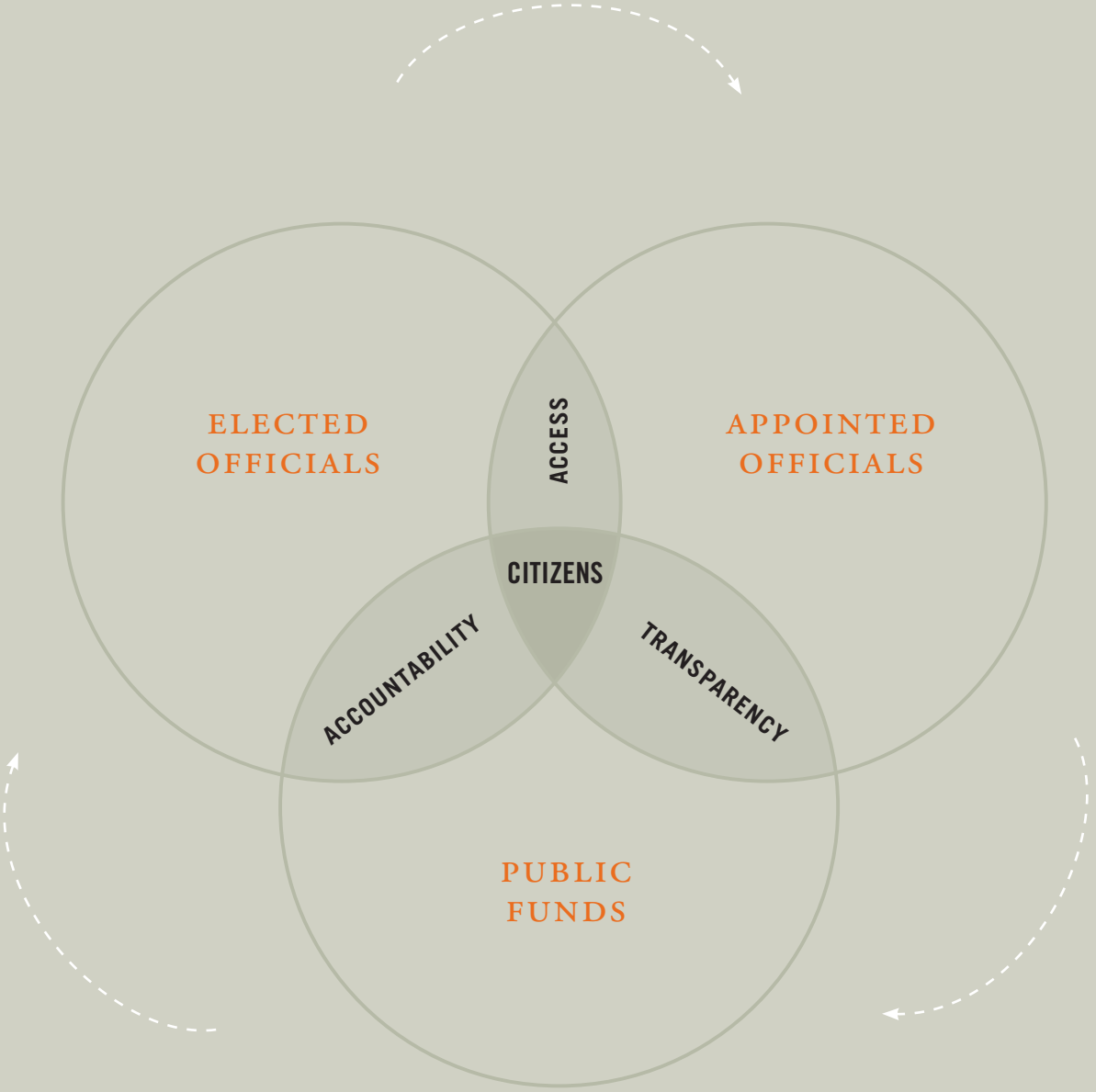
Consequently, for the past two years, a substantial portion of the IPC's resources have gone into developing educational materials to assist custodians in fulfilling their obligations under *PHIPA*, providing review and comment on the information practices of custodians, and responding to general inquiries about *PHIPA*. In assuming the extended role of educator and advisor, the IPC again stretched the boundaries of what has traditionally been accepted as part of the role of an independent tribunal. It is important to note, however, that these new functions are performed outside of the activities of the Tribunal Branch, to ensure that they do not interfere with the complaint resolution process.

With respect to the complaint resolution process itself, the health care community has shown a high degree of interest in working co-operatively with the IPC to resolve complaints and issues relating to *PHIPA*. This has allowed the IPC to focus

its resources on mediation and alternative dispute resolution. Consequently, through the first two years after enactment, only three orders were issued. This is a very positive development, as it has been the IPC's experience that the outcomes of complaints resolved by informal means are always more satisfactory to **all** parties than those resolved through an order.

Custodians have also demonstrated a commitment to privacy in their approach to dealing with privacy breaches. *PHIPA* includes a requirement for health information custodians to notify individuals of privacy breaches related to their personal health information. However, custodians have taken this requirement one step further, by reporting privacy breaches to the IPC and enlisting our assistance in ensuring that such breaches are responded to in an appropriate manner. This openness on the part of custodians has expanded the IPC's role beyond that which was anticipated by the drafters of the legislation. Accordingly, the IPC has had to develop new policies and procedures for handling such self-reported breaches. The IPC welcomes and encourages this openness on the part of custodians, and commends them for being so forthcoming.

In conclusion, the introduction of *PHIPA* has changed the role of the IPC quite dramatically. The IPC no longer restricts its activities to areas which are traditionally associated with an independent tribunal, created primarily to resolve complaints. The IPC now also provides assurances that the information practices of certain prescribed organizations meet acceptable standards and, more frequently, acts as an educator and advisor in a variety of matters relating to *PHIPA*. To meet these new challenges, the IPC has had to develop new policies and procedures and acquire and develop new in-house expertise. The IPC looks forward to growing into its new role and working co-operatively with the health care sector to ensure that *PHIPA* continues to operate as smoothly as possible.


ELECTED OFFICIALS
APPOINTED OFFICIALS
PUBLIC FUNDS
ACCESS
CITIZENS
ACCOUNTABILITY
TRANSPARENCY

Access by Default: Increased Accountability Needed Now in Public Procurement Process

IN HER 2005 ANNUAL REPORT, COMMISSIONER ANN CAVOUKIAN HIGHLIGHTED THE NEED FOR PUBLIC ACCOUNTABILITY FOR THE EXPENDITURE OF PUBLIC FUNDS. THE COMMISSIONER NOTED THAT THE RIGHT OF CITIZENS TO ACCESS GOVERNMENT-HELD INFORMATION IS ESSENTIAL IN ORDER TO HOLD ELECTED AND APPOINTED OFFICIALS ACCOUNTABLE TO THE PEOPLE THEY SERVE. THIS FUNDAMENTAL, DEMOCRATIC PRINCIPLE WAS THE BASIS OF THE COMMISSIONER'S RECOMMENDATION THAT CONTRACTS ENTERED INTO BY GOVERNMENT INSTITUTIONS, FOR THE PROVISION OF PROGRAMS OR SERVICES, BE MADE PUBLIC ON A ROUTINE BASIS.

Following up on that recommendation, the Commissioner is now calling on government organizations to make the full procurement process much more transparent.

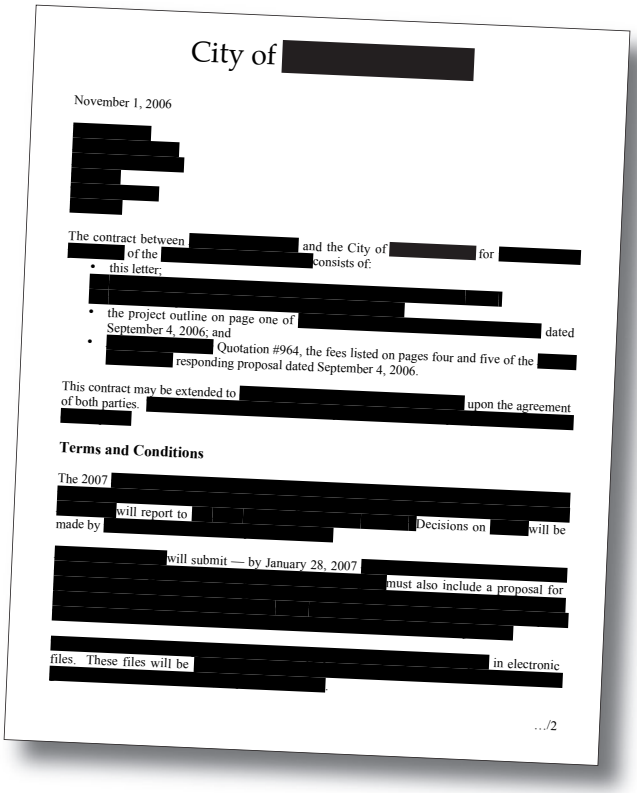
Disclosure of the final contracts entered into by governments goes only part way in ensuring meaningful public scrutiny of public expenditures. The signing of a contract for goods or services is generally the culmination of the procurement process established by a particular government institution. Ensuring the integrity and effectiveness of that procurement process is also an essential element of government accountability for the expenditure of public funds.

In recent years, the issue of transparency and accountability in government procurement has come to the forefront. This was particularly highlighted at the federal level with the release of the report of the Gomery Commission, which inquired into the federal Sponsorship Program and advertising activities. Disputes regarding the awarding of contracts have also arisen on a regular basis at both the municipal and provincial government levels.

Elected officials will readily agree that citizens should get the best value for their dollar. Recent experiences have demonstrated that it is transparency and accountability that ensure that the public procurement process is not only fair, but that successful bids are reasonable and in the best interests of the public.

Many public institutions still resist fully implementing accountability in their public procurement processes. Inquiries from the media or citizens may be met with the instructions to file a freedom of information request. And, the result for the requester may be a disclosure package with significant, if not all, documents exempted under section 17(1) of the *Freedom of Information and Protection of Privacy Act* or section 10(1) of the *Municipal Freedom of Information and Protection of Privacy Act*. These sections protect the disclosure of a trade secret or technical, commercial, or financial information that may be reasonably expected to prejudice the competitive position of a company, disclose information "supplied" in confidence to an institution, and give rise to reasonable expectation of harm by the company. On many occasions, these provisions are applied in an overly broad manner, and are used to prevent the disclosure of information vital to assessing the fairness and effectiveness of the tendering process.

The result is that the public may not be in a position to determine whether the procurement process has been administered fairly, in an unbiased manner and for the taxpayers' benefit. And, even if the contract entered into as a result of the process is made public in some cases, unless information regarding competing bids is also made available, it may be impossible to determine whether the taxpayers have gotten the best deal for their money.



City of [redacted]

November 1, 2006

[redacted]

The contract between [redacted] and the City of [redacted] for [redacted] of the [redacted] consists of:

- this letter;
- [redacted]
- the project outline on page one of [redacted] dated September 4, 2006; and
- [redacted] Quotation #964, the fees listed on pages four and five of the [redacted] responding proposal dated September 4, 2006.

This contract may be extended to [redacted] upon the agreement of both parties. [redacted]

Terms and Conditions

The 2007 [redacted] will report to [redacted] made by [redacted] Decisions on [redacted] will be [redacted] will submit — by January 28, 2007 [redacted] must also include a proposal for [redacted] files. These files will be [redacted] in electronic [redacted]

.../2

WOULD YOU CALL THIS TRANSPARENT GOVERNMENT?

As it currently stands, the Province of Ontario makes use of a private sector, pay-per-use system known as MERX (**www.merx.com**) for its procurement offers. Details of successful bidders on Ontario contracts are not available once a competition is complete; thus, a citizen is often forced to make a freedom of information request to learn of any details of the contract and bid. That citizen's request will then likely be subject to exemptions under Ontario's freedom of information and privacy laws, blocking access to fundamental details in the bid. While the IPC has received a number of appeals on this issue – and has ordered the information released in many cases – not everyone who tried in vain to obtain bidding information from a government organization is fully aware of the appeal process, or follows through with an appeal.

For full accountability and transparency, changes are essential.

Other Canadian provinces can serve as accountability models for Ontario. British Columbia, for example, has instituted an automatic, publicly funded process for publicizing and distributing public procurement competitions and results. In October 2002, the Government of British Columbia transferred all responsibility for public procurement from the Ministry of Management Services to the Office of the Comptroller General, Procurement Governance Office. The result was the creation of the publicly accessible website, BC Bid (**www.bcbid.gov.bc.ca**), where all public competitions and results are posted. As is stated in the Procurement Governance Office's Revised Core Policy Manual, Chapter 6 – Procurement:

> 6.4.2 BC Bid is the Province's online tendering system. Ministries, Crown corporations and public bodies use the system to distribute Opportunity Notices, complete bid documents and bid results for suppliers. BC Bid offers suppliers unrestricted access to government procurement. The disclosure of bid results supports monitoring of the fairness and value of government purchases.

By establishing an institutional program that automatically posts results of public procurement contracts, the Government of British Columbia was able to effectively remove the procurement process, contracts and results from the freedom of information regime, and instead treat them as pure accountability and transparency issues defaulting to de facto public access.

An even bolder example of a public accountability model is the State of New York. The New York State Office of General Services Procurement Services Group requires the posting of not only successful bid information, but the details of all bids submitted. This information is available at the Bid Opening Results page (**http://www.ogs.state.ny.us/purchase/bidresults/bidresults.asp**) of the state's procurement system. Clearly, the State of New York has made a conscious effort to ensure maximum transparency for its citizens vis-à-vis the public procurement process. The information provided also allows companies to submit their most competitive bid in response to future tenders.

As the New York model demonstrates, openness and transparency in the procurement process has benefits beyond accountability for public expenditures. It can provide a more competitive bidding environment for government contracts – which in turn benefits government as a purchaser of programs, goods or services. The extent to which businesses can review a particular tender to analyze why a competitor was successful can only lead to a more competitive bidding process the next time that particular program or service is tendered. To this extent, governments should view transparency in the procurement process as being in their best commercial interests, and by extension, in the best interests of their citizens.

The commercial benefits of an open process were recognized by the final report of the *Doing Business with the Ontario Government Task Force*, released by the Ontario Government in January 2006. The task force was comprised of MPPs from all three parties represented in the Ontario Legislature and was established to find ways to enhance access to government procurement opportunities. The final report included 11 recommendations to reform the public procurement process, including the automatic posting of successful bid details, and mandatory vendor debriefings where unsuccessful vendors could investigate why their bid was rejected. As noted by the task force, "More competitive bidding on government procurement supports efficient, effective government operations." An open and transparent procurement process is a necessary step towards this goal.

Government accountability and transparency is not a novel concept. In fact, many jurisdictions in Canada and the United States have already established popular, functional models for public procurement and bidding. There continues to be resistance, however, within Ontario institutions to reforming and opening the procurement process to public scrutiny.

Recent examples at the federal level of tax dollars being directed to sole-sourced, questionable contracts reinforce the need to re-evaluate the way that government does business, and to ensure that an informed citizenry plays the role of the ultimate check-and-balance in the spending of their own money.

Rather than institutions expending funds, effort and resources on guarding third-party business's financial information in supposedly public contracts, energy should instead be directed to ensuring that public funds flow to the best, most cost-effective bidders.

The biggest challenge will be for institutions and businesses to rethink the way that public procurement is done in Ontario. Not only should the province, as a first step, adopt the British Columbia model of posting winning bids, but like the State of New York, it should go further to disclose all bids, for public comparison. While this may come as a shock to some who are used to the veil of secrecy involved in the old model of public procurement, the new generation of businesses realize that the public has come to expect, and demand, transparency and accountability.

It's time for Ontario to show some leadership in public procurement transparency and accountability.

Commissioner's Recommendations

1. CREATE A CULTURE OF PRIVACY

There is a real need for provincial and municipal government organizations and health information custodians to develop a culture of privacy.

One example which illustrates this point is a truly regrettable situation that occurred at the Ottawa Hospital. A patient admitted to the hospital made a specific request to prohibit her estranged husband and his girlfriend, a nurse at the hospital, from having any information regarding her hospitalization, only to learn later that the nurse had repeatedly been able to access her personal health information. Despite having alerted the hospital to the possibility of harm, the harm occurred nonetheless. While the hospital had policies in place to safeguard health information, they were not followed completely, nor were they sufficient to prevent the privacy breach from occurring.

Unless privacy policies are interwoven into the fabric of a hospital's day-to-day operations or a government organization's daily operations, they will not work. Organizations that fall under Ontario's three privacy *Acts* must not only educate their staff about privacy legislation and the privacy information policies and practices implemented by their organizations, they must work towards ensuring that privacy becomes embedded into their institutional culture – that staff members understand just how serious a privacy breach can be.

I urge all health information custodians and access and privacy staff at government institutions to read this order, HO-002, issued following an investigation into this privacy breach, and to work towards developing a culture of privacy.

2. ONTARIO NEEDS TO MAKE ITS RFP SYSTEM FULLY TRANSPARENT

In my last annual report, I highlighted the need for public accountability for the expenditure of public funds. The rights of citizens to access government-held information is essential in order to hold elected and appointed officials accountable to the people they serve. This fundamental, democratic principle was the basis for my recommendation that all contracts entered into by government institutions for the provision of programs or services be made public on a routine basis.

That is only the first step. As outlined in an article in the *Issues* section of this annual report, disclosure of the final contracts entered into by governments goes only part way in ensuring meaningful public scrutiny of public expenditures. The signing of a contract for goods or services is generally the culmination of the procurement process established by a particular government institution. Ensuring the integrity and effectiveness of that procurement process is also an essential element of government accountability for the expenditure of public funds.

I am recommending that the Ontario government post the winning bid for every contract awarded by a provincial government organization on a government website – and further – to disclose details of all bids. While this may come as a shock to those who are used to the veil of confidentiality involved in the old model of public procurement, Ontarians deserve transparency and accountability.

3. RESPONSIBILITY FOR RECORDS DOESN'T END IF THE HEALTH FACILITY CLOSES

Last fall, a staff member of the College of Physicians and Surgeons of Ontario notified my office that a medical and rehabilitation clinic had closed its operations and left behind boxes of records containing personal health information.

In this case, the records were simply abandoned when the clinic ceased its operations. The custodian's failure to adequately notify individuals that the practice was ceasing its operations and to ensure that all records of personal health information were retained, transferred or disposed of in a secure manner demonstrated a flagrant disregard for the privacy rights of the individuals to whom the records related.

Following a change in practice, inadequate records management policies can not only lead to breaches of privacy, but can also deprive individuals of their right to access their personal health records.

I urge every health information custodian to read and follow the steps laid out in the health order I issued late in 2006, HO-003. Health information custodians must recognize that their obligations to protect personal health information in a secure manner do not cease when a facility shuts down or moves.

Requests by the Public

EARLY EACH YEAR, PROVINCIAL AND MUNICIPAL GOVERNMENT ORGANIZATIONS ARE REQUIRED UNDER THE *ACTS* TO SUBMIT A REPORT TO THE IPC ON THE NUMBER OF REQUESTS FOR INFORMATION OR CORRECTION OF PERSONAL INFORMATION THEY RECEIVED DURING THE PRIOR CALENDAR YEAR, AS WELL AS SUCH OTHER PERTINENT INFORMATION AS TIMELINESS OF RESPONSES, OUTCOMES AND FEES COLLECTED.

There were 36,739 freedom of information (FOI) requests filed across Ontario in 2006, the highest number ever, easily surpassing the previous record of 33,557 requests in 2004.

Much of the increase is due to a major jump in 2006 in the number of requests at the municipal government and police levels. Municipal corporations and police institutions, the largest two categories covered under the *Municipal Freedom of Information and Protection of Privacy Act*, had a 25.4 per cent increase in the number of requests received compared to 2005. For example, the **City of Toronto** and **Toronto Police** received 39 per cent and 22.8 per cent, respectively, more requests in 2006 than 2005.

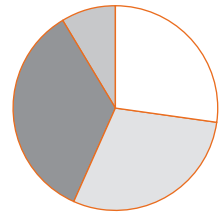
Provincial government organizations received 14,076 FOI requests in 2006, compared with 13,324 in 2005. Of these 3,168 (22.5 per cent) were for personal information and 10,908 (77.5 per cent) were for general records.

Ontario's 19 **universities**, which came under the legislation as of June 10, 2006, received a total of 173 requests. (See the universities chart in the *Response Rate Compliance* chapter, which follows this chapter.)

Municipal government organizations received 22,663 requests in 2006, a 23.6 per cent increase over 2005 (when 18,330 requests were filed). Of these, 8,737 (38.6 per cent) were personal information requests and 13,926 (61.4 per cent) were for general records.

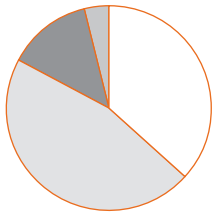
OUTCOME OF REQUESTS – 2006

PROVINCIAL REQUESTS



All Disclosed	27.5%
Disclosed in Part	29.5%
Nothing Disclosed	34.5%
Withdrawn/Abandoned	8.6%

MUNICIPAL REQUESTS



All Disclosed	36.8%
Disclosed in Part	46.2%
Nothing Disclosed	13.3%
Withdrawn/Abandoned	3.8%

36,739

Freedom of information requests filed across Ontario in 2006

The **Ministry of Environment** once again received the largest number of requests under the provincial *Act* (6,005), followed by the ministries of **Community Safety and Correctional Services** (3,323), **Labour** (1,083) and **Community and Social Services** (551). Together, these four ministries received 77.9 per cent of all provincial requests.

Police Services Boards received the most requests under the municipal *Act* – 54 per cent of all requests. Municipal corporations were next with 44.5 per cent, followed by school boards at 0.7 per cent and health boards with 0.3 per cent.

The majority of provincial requests in 2006 (72.1 per cent) were made by businesses, while the majority of municipal requests (66.5 per cent) came from individuals.

The *Acts* contain a number of exemptions that allow, and in some situations actually require, government organizations to refuse to disclose requested information. In 2006, the most frequently cited exemptions for personal information requests were the protection of other individuals' privacy, followed by law enforcement. Privacy protection was the most used exemption for general records requests, followed by law enforcement.

The *Acts* give individuals the right to request correction of their personal information held by government organizations. In 2006, provincial organizations did not receive any requests for corrections. Municipal organizations received 18 correction requests and refused seven. When a correction is refused, the requester can attach a statement of disagreement to the record, outlining why the information is believed to be incorrect. There were two statements of disagreement filed with municipal organizations.

The legislation contains a number of fee provisions. In addition to the $5 application fee, which is mandatory, government organizations can charge certain other prescribed fees for responding to requests. Where the anticipated charge is more than $25, a fee estimate can be given to a requester before search activity begins. Organizations have discretion to waive fees where it seems fair and equitable to do so, after weighing several specific factors listed in the *Acts*.

Provincial organizations reported collecting $68,265.15 in application fees and $459,594.16 in additional fees in 2006. The corresponding numbers for municipal organizations were $109,102.72 and $237,580.84.

Search fees were the most commonly charged category by provincial organizations (63.9 per cent), followed by preparation costs (13.1 per cent) and shipping charges (11.8 per cent). Municipal organizations, in contrast, most frequently charged for reproduction costs (51.7 per cent), followed by search fees (24.4 per cent) and preparation costs (12.8 per cent).

CASES IN WHICH FEES WERE ESTIMATED – 2006

	PROVINCIAL $	MUNICIPAL $
Total Application Fees Collected	**68,265.15**	**109,102.72**
Total Additional Fees Collected	**459,594.16**	**237,580.84**
Total Fees Waived	**30,131.27**	**8,560.81**

AVERAGE COST OF REQUESTS – 2006

	PROVINCIAL REQUESTS $	MUNICIPAL REQUESTS $
Personal Information	**11.55**	**8.64**
General Records	**51.11**	**21.04**

Response Rate Compliance – Only Part of the Story

EACH YEAR, TO HELP FOCUS ATTENTION ON THE IMPORTANCE OF COMPLYING WITH THE RESPONSE REQUIREMENTS OF THE *ACTS*, THE IPC REPORTS COMPLIANCE RATES FOR EACH MINISTRY AND SELECTED OTHER GOVERNMENT ORGANIZATIONS.

These numbers need to be understood in the overall context of the *Acts*. The 30-day compliance rate measures only one aspect of an institution's access to information program. This rate measures an institution's timeliness in responding to formal freedom of information requests. It does not, however, provide a complete view of whether an institution has embraced the philosophy of openness and transparency, which is equally, if not more, important. In other words, a high compliance rate of responding within 30 days does not necessarily mean that an institution is open and transparent in its operations.

The IPC has applauded the Premier for repeatedly stressing the importance of the province's access to information laws. The Premier has established the fundamental principle that, in Ontario, information should be made public unless there is a "clear and compelling reason" not to do so. This principle goes far beyond simply responding to requests in a timely fashion. Although a ministry may respond to a freedom of information request within the timeframe established by the *Acts*, the "quality" of that response may be lacking. The IPC continues to deal with appeals where an institution has improperly withheld information or delayed disclosure, even though its response (its decision regarding what, if anything, would be released) to the requester was provided within the 30-day timeframe.

For example, this office has repeatedly encouraged government institutions not to deny access to a record simply because an exemption may be claimed. There are still too many cases where institutions are resisting the disclosure of information that should be in the public domain through the unnecessary application of exemptions. The fact that a timely response was provided is of little comfort to the requester. In addition, some institutions continue to give an overly broad interpretation to sections 65(6)/52(3) of the *Acts*, which relate to employment and labour relations matters. These provisions are often applied to deny access to basic information that should be routinely disclosed. Again, the fact that such a response was received within the 30-day timeline should not reflect positively on an institution.

There are other ways that institutions, while providing a requester with a timely response, may frustrate the intent of the *Acts*. For example, a fee may be requested that is unjustified, or a fee waiver may be refused where the circumstances would call for such a waiver. As well, even after the IPC has issued an order, institutions may still resist disclosure, even though "clear and compelling" circumstances do not exist. In response to a subsequent request in identical circumstances, an institution may still refuse disclosure, despite an order that speaks otherwise, which then requires a frustrated requester to file an appeal with this office. On occasion, a government institution may bring an application for judicial review of an IPC order, despite the absence of compelling circumstances. This requires a requester to again wait until a lengthy court process is completed, and significant taxpayer dollars have been expended.

Responding to freedom of information requests within the timeframes set by the *Acts* is a laudable goal. However, the ultimate objective of an institution's access to information re-

PROVINCIAL: NUMBER OF REQUESTS COMPLETED IN 2006

(includes organizations where the Minister is the Head)

MINISTRY	REQUESTS RECEIVED	REQUESTS COMPLETED	WITHIN 1-30 DAYS		WITHIN 31-60 DAYS		WITHIN 61-90 DAYS		OVER 90 DAYS	
			No.	%	No.	%	No.	%	No.	%
Agriculture, Food and Rural Affairs	33	35	14	40.0	6	17.1	9	25.7	6	17.1
Attorney General	337	313	267	85.3	16	5.1	10	3.2	20	6.4
Cabinet Office	38	34	32	94.1	0	0.0	1	2.9	1	2.9
Children and Youth Services	37	44	39	88.6	2	4.6	1	2.3	2	4.6
Citizenship and Immigration	4	6	4	66.7	2	33.3	0	0.0	0	0.0
Community and Social Services	551	556	500	89.9	46	8.3	7	1.3	3	0.5
Community Safety and Correctional Services	3,323	3,244	2,634	81.2	482	14.9	63	1.9	65	2.0
Culture	9	12	9	75.0	3	25.0	0	0.0	0	0.0
Democratic Renewal Secretariat	2	2	1	50.0	1	50.0	0	0.0	0	0.0
Economic Development and Trade	14	10	1	10.0	2	20.0	2	20.0	5	50.0
Education	44	42	32	76.2	5	11.9	2	4.8	3	7.1
Energy	30	31	12	38.7	2	6.5	3	9.7	14	45.2
Environment	6,004	5,987	3,609	60.3	1,619	27.0	392	6.6	367	6.1
Finance	156	138	95	68.8	21	15.2	10	7.3	12	8.7
Government Services	221	206	191	92.7	11	5.3	4	1.9	0	0.0
Health and Long-Term Care	189	193	120	62.2	36	18.7	13	6.7	24	12.4
Health Promotion	11	11	7	63.6	3	27.3	0	0.0	1	9.1
Intergovernmental Affairs	7	7	6	85.7	1	14.3	0	0.0	0	0.0
Labour	977	961	896	93.2	32	3.3	14	1.5	19	2.0
Municipal Affairs and Housing	62	66	48	72.7	10	15.2	6	9.1	2	3.0
Natural Resources	106	99	61	61.6	22	22.2	9	9.1	7	7.1
Northern Development and Mines	13	13	5	38.5	7	53.9	0	0.0	1	7.7
Francophone Affairs	1	1	1	100.0	0	0.0	0	0.0	0	0.0
Aboriginal Affairs Secretariat	25	17	10	58.8	7	41.2	0	0.0	0	0.0
Ontario Seniors Secretariat	1	1	0	0.0	1	100.0	0	0.0	0	0.0
Ontario Women's Directorate	1	2	1	50.0	0	0.0	0	0.0	1	50.0
Public Infrastructure Renewal	27	25	21	84.0	1	4.0	2	8.0	1	4.0
Research and Innovation	0	3	3	100.0	0	0.0	0	0.0	0	0.0
Tourism	4	4	3	75.0	0	0.0	1	25.0	0	0.0
Training, Colleges and Universities	65	68	62	91.2	4	5.9	1	1.5	1	1.5
Transportation	251	240	216	90.0	9	3.8	5	2.1	10	4.2

gime should be to provide the fullest disclosure possible to the public. Over the coming year, the IPC will closely scrutinize, not only the timeliness of responses, but also the decisions made by institutions throughout the request and appeal process to determine whether the spirit of openness embodied in the *Acts*, and the Premier's message, are being supported.

As for the actual statistics on the compliance rates, there are two sets of charts illustrating these rates. The first set shows the compliance rate for each institution in meeting the 30-day standard set by the *Acts* for responding to freedom of information requests. The second chart shows compliance rates when Notices of Extension and Notices to Affected Person are included in the compliance calculations. When legitimately required, these notices allow a government organization to be in compliance with the applicable *Act*, despite taking more than 30 days to respond to a request. (Notices of Extension are explained in section 27(1) of the provincial *Act* and section 20(1) of the municipal *Act*. Notices to Affected Person are explained in section 28(1) of the provincial *Act* and section 21(1) of the municipal *Act*.)

PROVINCIAL ORGANIZATIONS

The 30-day compliance rate for provincial ministries dropped by 6.6 per cent in 2006 – to 73.5 per cent – the second drop in the provincial compliance rate since 1998. With the exception of 2004, the compliance rate had risen steadily since the IPC began publishing individual ministry compliance rates. With notices included, however, the 2006 compliance rate was 86.5 per cent, virtually identical to 2005's 86.4.

There were a number of positive stories. The 90 per cent-plus club – more than 90 per cent compliance when notices are considered – grew to 19 from 16. This group includes ministries and Cabinet Office. Newcomers in 2006 were the **Ministry of Children and Youth Services** (95.5 per cent), the **Ministry of Training, Colleges and Universities** (95.6), and the **Ministry of Education** (92.9).

PROVINCIAL

EXTENDED COMPLIANCE INCLUDES NOTICE OF EXTENSION AND NOTICE TO THIRD PARTIES

MINISTRY	30-DAY COMPLIANCE %	EXTENDED COMPLIANCE* %
Agriculture, Food & Rural Affairs	40.0	60.0
Attorney General	85.3	98.7
Cabinet Office	94.1	97.1
Children & Youth Services	88.6	95.5
Citizenship & Immigration	66.7	100.0
Community & Social Services	89.9	92.4
Community Safety & Correctional Services	81.2	97.8
Culture	75.0	100.0
Democratic Renewal Secretariat	50.0	100.0
Economic Development & Trade	10.0	30.0
Education	76.2	92.9
Energy	38.7	38.7
Environment	60.3	76.5
Finance	68.8	93.5
Government Services	92.7	99.0
Health & Long-Term Care	62.2	75.7
Health Promotion	63.6	63.6
Intergovernmental Affairs	85.7	85.7
Labour	93.2	93.2
Municipal Affairs & Housing	72.7	97.0
Natural Resources	61.6	83.8
Northern Development & Mines	38.5	92.3
Office of Francophone Affairs	100.0	100.0
Ontario Secretariat for Aboriginal Affairs	58.8	58.8
Ontario Seniors' Secretariat	0.0	100.0
Ontario Women's Directorate	50.0	50.0
Public Infrastructure Renewal	84.0	96.0
Research and Innovation	100.0	100.0
Tourism	75.0	100.0
Training, Colleges & Universities	91.2	95.6
Transportation	90.0	92.9

** Including sections 27(1) and 28(1) of FIPPA*

Universities

Ontario's 19 universities fell under the *Freedom of Information and Protection of Privacy Act* as of June 10, 2006. The vast majority, compliance wise, are off to a good start. Eleven of the 16 universities that received freedom of information requests in 2006 had a compliance rate, with notices, of 100 per cent.

The three universities with the most completed requests were the University of Toronto (23), York University (22) and Laurentian University (21).

The **University of Toronto** had an 87 per cent 30-day compliance rate; with notices, the compliance rate climbed to 100 per cent. **York University** had a 30-day compliance rate of 54.5 per cent; with notices, 68.2 per cent, while **Laurentian University** compiled an 85.7 per cent 30-day compliance rate, which climbed to 95.2 per cent with notices.

Ryerson University, at 12.5 per cent, and **McMaster University**, at 23.1 per cent, were the only universities with a 30-day compliance rate under 50 per cent. And, with a compliance rate with notices of 25 per cent, Ryerson was the only university with an overall compliance rate under 60 per cent.

The accompanying chart lists the compliance rates for all of Ontario's universities.

UNIVERSITIES

EXTENDED COMPLIANCE INCLUDES NOTICE OF EXTENSION AND NOTICE TO THIRD PARTIES

UNIVERSITY	REQUESTS COMPLETED %	30-DAY COMPLIANCE %	EXTENDED COMPLIANCE* %
Toronto	23	87.0	100.0
York	22	54.5	68.2
Laurentian	21	85.7	95.2
Ryerson	16	12.5	25.0
McMaster	13	23.1	61.5
Queen's	8	87.5	100.0
Western	8	87.5	100.0
Carleton	6	100.0	100.0
Ottawa	6	100.0	100.0
Windsor	4	100.0	100.0
Lakehead	3	66.7	66.7
Trent	3	100.0	100.0
Guelph	2	100.0	100.0
Nipissing	2	100.0	100.0
Brock	1	100.0	100.0
Waterloo	1	100.0	100.0
U of OIT	0	n/a	n/a
Wilfrid Laurier	0	n/a	n/a
OCAD	0	n/a	n/a

TOP EIGHT MUNICIPAL CORPORATIONS

(based on number of requests completed)

			WITHIN 1-30 DAYS		WITHIN 31-60 DAYS		WITHIN 61-90 DAYS		OVER 90 DAYS	
	REQUESTS RECEIVED	REQUESTS COMPLETED	No.	%	No.	%	No.	%	No.	%
POPULATION UNDER 50,000										
City of Clarence-Rockland *(21,624)*	18	18	18	100.0	0	0.0	0	0.0	0	0.0
Township of Dorion *(383)*	0	23	23	100.0	0	0.0	0	0.0	0	0.0
Town of Georgina *(44,000)*	46	46	45	97.8	1	2.2	0	0.0	0	0.0
Town of Gravenhurst *(10,899)*	20	20	18	90.0	1	5.0	1	5.0	0	0.0
The Corporation of Haldimand County *(43,728)*	27	23	14	60.9	6	26.1	3	13.0	0	0.0
Municipality of Highlands East *(2,681)*	14	14	0	0	14	100	0	0	0	0
The Corporation of the Town of Innisfil *(26,979)*	32	32	29	90.6	3	9.4	0	0.0	0	0.0
City of Stratford *(28,617)*	15	15	8	53.3	7	46.7	0	0	0	0
POPULATION BETWEEN 50,000 AND 200,000										
City of Barrie *(130,535)*	87	85	73	85.9	10	11.8	1	1.2	1	1.2
City of Burlington *(148,471)*	88	88	88	100.0	0	0.0	0	0.0	0	0.0
City of Cambridge *(122,000)*	105	105	103	98.1	1	1.0	1	1.0	0	0.0
City of Kitchener *(178,178)*	418	415	414	99.8	1	0.2	0	0.0	0	0.0
Corporation of the Town of Oakville *(144,128)*	608	608	605	99.5	3	0.5	0	0.0	0	0.0
Town of Richmond Hill *(176,830)*	400	400	391	97.8	9	2.3	0	0.0	0	0.0
City of Greater Sudbury *(155,339)*	154	149	124	83.2	21	14.1	4	2.7	0	0.0
City of Thunder Bay *(102,617)*	121	121	121	100.0	0	0.0	0	0.0	0	0.0
POPULATION OVER 200,000										
City of Brampton *(422,600)*	324	324	318	98.2	3	0.9	1	0.3	2	0.6
City of Hamilton *(490,268)*	134	130	129	99.2	1	0.8	0	0.0	0	0.0
City of Mississauga *(700,000)*	477	482	480	99.6	2	0.4	0	0.0	0	0.0
Regional Municipality of Niagara *(399,696)*	68	59	59	100.0	0	0.0	0	0.0	0	0.0
City of Ottawa (870,254)	319	309	270	87.4	28	9.1	6	1.9	5	1.6
Regional Municipality of Peel *(1,180,599)*	131	111	99	89.2	9	8.1	2	1.8	1	0.9
City of Toronto *(2,481,494)*	5152	4832	4162	86.1	562	11.6	66	1.4	42	0.9
Region of York *(786,355)*	92	86	82	95.3	4	4.7	0	0.0	0	0.0

MUNICIPAL ORGANIZATIONS

Municipal government institutions responded to freedom of information requests within the statutory 30-day period at an excellent 86.4 per cent rate in 2006, up from 83.9 per cent in 2005. This was the third year in a row that municipal organizations improved their compliance rate. When notices are considered, the average compliance rate for municipal organizations across Ontario was an impressive 90.7 per cent.

The charts used in this section illustrate individual response rates from the eight **municipalities** that completed the most requests in each of three population categories, as well as the eight **police services** and eight **school boards** that completed the most requests.

Municipalities

Overall, municipal corporations achieved a highly commendable 90.2 per cent 30-day compliance rate, up from 87.6 per cent in 2005.

Among the eight municipalities with a population over 200,000 that completed the most requests in 2006, the **Regional Municipality of Niagara** was the only one with a perfect 100 per cent 30-day compliance score, albeit on only 59 requests. **Mississauga**, which scored 100 per cent in 2005 on 430 requests, nearly equalled that feat in 2006 with a 99.6 per cent rate for 30-day compliance despite handling more requests. Others scoring in the 90th percentile for 30-day compliance in this (the highest) population category were **Hamilton** (99.2 per cent – an increase of more than 15 per cent), **Brampton** (98.2 per cent) and the **Region of York** (95.4 per cent).

The compliance leaders among the municipalities with the most requests in the middle population category (between 50,000-200,000) were **Thunder Bay** and **Burlington**, both achieving 100 per cent 30-day compliance, with 121 and 88 completed requests, respectively. **Kitchener**, with 415 requests, achieved a highly commendable 99.8 per cent 30-day compliance (and, when notices are considered, scored 100 per cent). The **Town of Oakville**, with the most completed requests in this population category, 608, achieved an impressive 99.5 per cent 30-day compliance rate – 99.8 per cent with notices.

Municipalities with populations under 50,000 were led by the **City of Clarence-Rockland** and the **Township of Dorion**, both registering 30-day 100 per cent compliance rates on 18 and 23 completed requests, respectively. Two of last year's leaders, **the towns of Georgina** and **Innisfil**, which had the most requests in this category in 2006 with 46 and 32 respectively, dropped slightly from 2005's perfect 100 per cent 30-day compliance to still very commendable 97.8 per cent and 90.6 per cent, respectively, in 2006.

Police Services

Police services overall increased their 30-day compliance to 83.4 per cent in 2006, up from 80.5 per cent the previous year. **Halton Regional Police Services** was among the leaders with 100 per cent 30-day compliance on 872 completed requests. Halton was joined at the top of the compliance list in 2006 by the neighbouring **Peel Regional Police Services**, which completed all 991 of its requests within 30 days. **Hamilton Police Services** cracked the 90 per cent-plus group with a 91.2 per cent 30-day compliance rate on 1,215 completed requests.

Boards of Education

School boards' overall 30-day compliance dipped slightly to 80.9 per cent in 2006 from 2005's 82.9 per cent. Once again, the **District School Board of Niagara** had by far the most completed requests, 74, and achieved an 87.8 per cent 30-day compliance rate, down slightly from 2005's 92.3 per cent. The only other board to complete more than 10 requests was the **Dufferin-Peel Catholic District School Board**, with 14. It recorded a 57.1 per cent 30-day compliance rate in 2006, up from 50 per cent the previous year. **Hamilton-Wentworth District School Board** and **Ottawa-Carleton District School Board** both achieved 100 per cent 30-day compliance on nine and six completed requests, respectively.

TOP EIGHT MUNICIPAL CORPORATIONS

(based on number of requests completed)

	30-DAY COMPLIANCE %	EXTENDED COMPLIANCE* %
EXTENDED COMPLIANCE INCLUDES NOTICE OF EXTENSION AND NOTICE TO THIRD PARTIES		
POPULATION UNDER 50,000		
City of Clarence-Rockland	100.0	100.0
Township of Dorion	100.0	100.0
Town of Georgina	97.8	100.0
Town of Gravenhurst	90.0	100.0
The Corporation of Haldimand County	60.9	60.9
Municipality of Highlands East	0.0	100.0
The Corporation of the Town of Innisfil	90.6	100.0
City of Stratford	53.3	53.3
POPULATION BETWEEN 50,000 TO 200,000		
City of Barrie	85.9	85.9
City of Burlington	100.0	100.0
City of Cambridge	98.1	98.1
City of Kitchener	99.8	100.0
Corporation of the Town of Oakville	99.5	99.8
Town of Richmond Hill	97.8	100.0
City of Greater Sudbury	83.2	87.9
City of Thunder Bay	100.0	100.0
POPULATION OVER 200,000		
City of Brampton	98.2	98.5
City of Hamilton	99.2	99.2
City of Mississauga	99.6	99.6
Regional Municipality of Niagara	100.0	100.0
City of Ottawa	87.4	93.5
Regional Municipality of Peel	89.2	89.2
City of Toronto	86.1	88.2
Region of York	95.3	95.3

** Including sections 20(1) and 21(1) of MFIPPA*

TOP EIGHT POLICE INSTITUTIONS

(ranked on number of requests completed)

	REQUESTS RECEIVED	REQUESTS COMPLETED	WITHIN 1-30 DAYS		WITHIN 31-60 DAYS		WITHIN 61-90 DAYS		OVER 90 DAYS	
			No.	%	No.	%	No.	%	No.	%
Durham Regional Police Service	885	930	609	65.5	247	26.6	47	5.1	27	2.9
Halton Regional Police Service	895	872	872	100.0	0	0.0	0	0.0	0	0.0
Hamilton Police Service	1240	1215	1108	91.2	101	8.3	3	0.2	3	0.2
London Police Service	544	558	356	63.8	199	35.7	3	0.5	0	0.0
Niagara Regional Police Service	942	922	706	76.6	213	23.1	3	0.3	0	0.0
Peel Regional Police	991	991	991	100.0	0	0.0	0	0.0	0	0.0
Toronto Police Services Board	3085	3074	2524	82.1	406	13.2	95	3.1	49	1.6
Windsor Police Service	557	590	439	74.4	151	25.6	0	0.0	0	0.0

COMPLIANCE INCLUDING NOTICE OF EXTENSION AND NOTICE TO THIRD PARTIES

	30-DAY COMPLIANCE %	EXTENDED COMPLIANCE* %
Durham Regional Police Service	65.5	69.8
Halton Regional Police Service	100.0	100
Hamilton Police Service	91.2	91.2
London Police Service	63.8	98.9
Niagara Regional Police Service	76.6	83.2
Peel Regional Police	100.0	100
Toronto Police Services Board	82.1	85.3
Windsor Police Service	74.4	100

TOP EIGHT SCHOOL BOARDS

(ranked on number of requests completed)

	REQUESTS RECEIVED	REQUESTS COMPLETED	WITHIN 1-30 DAYS		WITHIN 31-60 DAYS		WITHIN 61-90 DAYS		OVER 90 DAYS	
			No.	%	No.	%	No.	%	No.	%
Dufferin-Peel Catholic District School Board	12	14	8	57.1	4	28.6	1	7.1	1	7.1
Hamilton-Wentworth District School Board	9	9	9	100.0	0	0.0	0	0.0	0	0.0
District School Board of Niagara	74	74	65	87.8	8	10.8	1	1.4	0	0.0
Ottawa-Carleton District School Board	6	6	6	100.0	0	0.0	0	0.0	0	0.0
Peel District School Board	7	7	6	85.7	1	14.3	0	0.0	0	0.0
Thames Valley District School Board	6	6	4	66.7	0	0.0	0	0.0	2	33.3
Toronto District School Board	6	6	3	50.0	0	0.0	0	0.0	3	50.0
York Catholic District School Board	8	8	5	62.5	3	37.5	0	0.0	0	0.0

EXTENDED COMPLIANCE INCLUDES NOTICES OF EXTENSION AND NOTICE TO THIRD PARTIES

	30-DAY COMPLIANCE %	EXTENDED COMPLIANCE* %
Dufferin-Peel Catholic District School Board	57.1	100.0
Hamilton-Wentworth District School Board	100.0	100.0
District School Board of Niagara	87.8	87.8
Ottawa-Carleton District School Board	100.0	100.0
Peel District School Board	85.7	85.7
Thames Valley District School Board	66.7	66.7
Toronto District School Board	50.0	83.3
York Catholic District School Board	62.5	100.0

** Including sections 20(1) and 21(1) of MFIPPA*

Access

THE PROVINCIAL AND MUNICIPAL *FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACTS* PROVIDE THAT, SUBJECT TO LIMITED AND SPECIFIC EXEMPTIONS, INFORMATION UNDER THE CONTROL OF PROVINCIAL AND MUNICIPAL GOVERNMENT ORGANIZATIONS SHOULD BE AVAILABLE TO THE PUBLIC.

If you make a written freedom of information request under one of the *Acts* to a provincial or municipal government organization and you are not satisfied with the response, you have a right to appeal that decision to an independent body – the IPC.

Records that do not contain the personal information of the requester are referred to as "general records." General records appeals can be filed concerning a refusal to provide access to general records, the amount of fees sought, the fact that the organization did not respond within the prescribed 30-day period, or other procedural aspects relating to a request. (Appeals relating to requests for access to one's own *personal information* are covered in this annual report in the chapter entitled *Privacy*.)

When an appeal is received, the IPC first attempts to settle it informally. If all issues cannot be resolved within a reasonable period of time, the IPC may conduct an inquiry and issue a binding order, which could include ordering the government organization to release all or part of the requested information.

STATISTICAL OVERVIEW

In 2006, 893 appeals regarding access to general records or personal information were **made to** the IPC, an increase of 7.2 per cent over the 833 appeals **opened** in 2005.

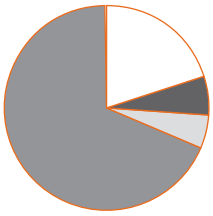
There were 888 appeals **closed** in 2006, an increase of 17 per cent over the 756 appeals **closed** in 2005.

ISSUES IN *GENERAL RECORDS* APPEALS

	PROVINCIAL		MUNICIPAL		TOTAL	
	No.	%	No.	%	No.	%
Exemptions only	107	37.7	138	49.1	**245**	**43.4**
Deemed refusal	39	13.7	21	7.5	**60**	**10.6**
Reasonable search (sole issue)	28	9.9	20	7.1	**48**	**8.5**
Exemptions with other issues	23	8.1	17	6.0	**40**	**7.1**
Third party	17	6.0	14	5.0	**31**	**5.5**
Time extension	19	6.7	8	2.8	**27**	**4.8**
Fee and fee waiver	12	4.2	15	5.3	**27**	**4.8**
Interim decision	17	6.0	8	2.8	**25**	**4.4**
Frivolous/Vexatious	0	0.0	3	1.1	**3**	**0.5**
Failure to disclose	1	0.4	0	0.0	**1**	**0.2**
Other	21	7.4	37	13.2	**58**	**10.2**
TOTAL	**284**	**100.0**	**281**	**100.0**	**565**	**100.0**

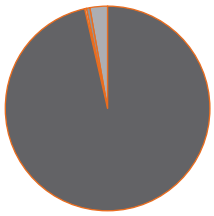
OUTCOME OF *GENERAL RECORDS* APPEALS BY STAGE CLOSED

INTAKE



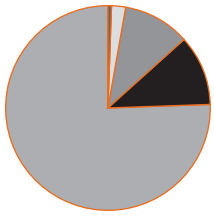
Screened out	20.3%
Mediated in full	6.1%
Abandoned	5.3%
Withdrawn	68.9%
Other	0%
Ordered	0%
TOTAL	**100.0%**

MEDIATION



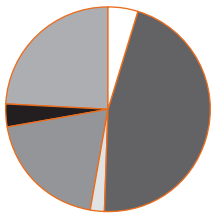
Screened out	0%
Mediated in full	96.5%
Abandoned	0.4%
Withdrawn	0.4%
Other	0%
Ordered	2.7%
TOTAL	**100.0%**

ADJUDICATION



Screened out	0%
Mediated in full	0.6%
Abandoned	2.3%
Withdrawn	10.5%
Other	11.1%
Ordered	75.4%
TOTAL	**100.0%**

TOTAL OUTCOME



Screened out	4.8%
Mediated in full	46.1%
Abandoned	2.1%
Withdrawn	19.6%
Other	3.4%
Ordered	24.2%
TOTAL	**100.0%**

ACCESS TO GENERAL RECORDS

Appeals Opened

Overall, 565 appeals regarding access to **general** records were made to the IPC in 2006, an increase of 16 per cent from the 487 appeals opened in 2005. Of the 2006 appeals, 284 (50.3 per cent) were filed under the provincial *Act* and 281 (49.7 per cent) under the municipal *Act*. (*Percentage figures are rounded off in this report and may not add up to exactly 100.*)

Of the 284 provincial general records appeals received, 206 (72.5 per cent) involved ministries and 78 (27.5 per cent) involved agencies. The **Ministry of Community Safety and Correctional Services** was involved in the largest number of general records appeals (34), followed by the **Ministry of the Environment** (25) and the **Ministry of Health and Long-Term Care** (21).

The agencies with the highest number of general records appeals included the **Ontario Secretariat for Aboriginal Affairs** (10), the **Ontario Lottery and Gaming Corporation** (eight), **Hydro One** (eight), and **Laurentian University** (eight).

Of the 281 municipal general records appeals received, 180 (64.1 per cent) involved municipalities, 71 (25.3 per cent) involved police services, and 13 (4.6 per cent) involved boards of education. Seventeen appeals (six per cent) involved other types of municipal institutions.

In terms of the issues raised, excluding non-jurisdictional cases, 43.4 per cent of general records appeals were related to the exemptions claimed by institutions in refusing to grant access. Another 10.6 per cent of general records appeals were the result of deemed refusals to provide access, in which

TYPES OF APPELLANTS IN APPEALS OPENED

	PROVINCIAL		MUNICIPAL		**TOTAL**	
	No.	%	No.	%	**No.**	**%**
Individual	123	43.5	184	65.5	**307**	**54.3**
Business	76	26.8	72	25.6	**148**	**26.2**
Media	31	10.9	16	5.7	**47**	**8.3**
Academic/Researcher	29	10.2	0	0.0	**29**	**5.1**
Association/Group	13	4.6	8	2.8	**21**	**3.7**
Government	7	2.5	1	0.4	**8**	**1.4**
Politician	3	1.1	0	0.0	**3**	**0.5**
Union	2	0.7	0	0.0	**2**	**0.4**
Total	**284**	**100**	**281**	**100.0**	**565**	**100.0**

the institution did not respond to the request within the time frame required by the *Acts*. In 8.5 per cent of the appeals, the issue was whether the institution had conducted a reasonable search for the records requested. And, 7.1 per cent of general records appeals concerned exemptions with other issues. The remaining appeals (30.4 per cent) were related to fees, time extensions, interim decisions and various other issues.

Most appellants were individual members of the public (54.3 per cent). The remaining appellants were classified under other categories.

Lawyers (95) or agents (12) represented appellants in 18.6 per cent of the general records appeals made in 2006.

In 2006, $10,858 in application fees for general records appeals was paid to the IPC.

Appeals Closed

The IPC **closed** 562 general records appeals during 2006. Of these, 282 (50.2 per cent) concerned provincial institutions, while 280 (just under 50 per cent) concerned municipal institutions.

Of the 562 general records appeals closed, 426 (75.8 per cent) were closed without the issuance of a formal order. Of these, 132 (23.5 per cent) were closed during the intake stage and 259 (46.1 per cent) were closed during the mediation stage. There were 171 (30.4 per cent) general records appeals closed during the adjudication stage.

Overall, there were 136 general records appeals closed by order, 129 at the adjudication stage and seven at the mediation stage.

OUTCOME OF APPEALS CLOSED OTHER THAN BY ORDER

	PROVINCIAL		MUNICIPAL		**TOTAL**	
	No.	%	No.	%	**No.**	**%**
Screened out	14	6.6	12	5.1	**26**	**5.9**
Mediated in full	120	56.9	139	65	**259**	**60.8**
Abandoned	8	3.8	4	1.9	**12**	**2.8**
Withdrawn	63	29.9	47	22	**110**	**25.9**
Other	6	2.8	13	6.1	**19**	**4.5**
Total	**211**	**100.0**	**215**	**100.0**	**426**	**100.0**

OUTCOME OF APPEALS CLOSED BY ORDER

	PROVINCIAL		MUNICIPAL		**TOTAL**	
HEAD'S DECISION	No.	%	No.	%	**No.**	**%**
Not upheld	13	18.3	17	26.2	**30**	**22.1**
Partially upheld	30	42.3	20	30.8	**50**	**36.8**
Upheld	27	38.0	25	38.5	**52**	**38.2**
Other	1	1.4	3	4.6	**4**	**2.9**
Total	**71**	**100.0**	**65**	**100.0**	**136**	**100.0**

High Profile Appeals

SUMMARIES OF FOUR APPEALS THAT THE IPC DEALT WITH IN 2006

MO-2019 – YORK REGIONAL POLICE SERVICES BOARD

The York Regional Police Services Board received a request from a member of the media for access to records about properties identified by the police as housing illegal drug operations, which are sometimes called "grow houses."

The police relied on the exemptions in sections 8(1)(a), (b), and (f), 8(2)(a) (law enforcement) and 14(1) (personal privacy) of the *Municipal Freedom of Information and Protection of Privacy Act* to deny access to the records, which consisted of data in table format for the years 2002 to 2005.

The requester appealed the decision to the IPC. At the close of mediation, the appellant confirmed that he continued to seek access to information about the addresses of grow houses, incident dates, occurrence numbers, criminal charges laid, plants seized, money seized, and the presence of children. The appeal moved to adjudication.

The adjudicator, Assistant Commissioner Brian Beamish, first addressed the law enforcement exemptions in sections 8(1)(a) and (b). He found they did not apply, and agreed with the submission of the appellant that the police had not provided sufficient evidence to establish these exemptions. In his order, the Assistant Commissioner remarked: "The assertion that releasing information … will lead curious citizens to attend the properties in question and to interfere with evidence is not persuasive."

The Assistant Commissioner also found that section 8(1)(f) (right to a fair trial) did not apply because the police had not submitted evidence to establish a "real and substantial risk" of interference with that right based on disclosure of the information.

Under section 8(2)(a), which applies to law enforcement reports, the tables did not qualify as "reports" under the exemption because they "contain nothing more than mere recordings of fact related to the multiple indoor grow operation seizures," said the Assistant Commissioner. A "formal statement of the results of the collation and consideration of information" is required for this exemption to apply.

The Assistant Commissioner then dealt with the mandatory personal privacy exemption in section 14(1), which applies only to "personal information" as defined in section 2(1) of the *Act*. He found that property addresses, occurrence dates, criminal charges, plants seized, money seized, and the presence of children are personal information, but occurrence numbers are not. Accordingly, he ordered disclosure of the occurrence numbers.

Under the personal privacy exemption, he found that neither of the presumptions against disclosure in sections 14(3)(b) and (f) applied, since the personal information was not compiled for the purpose of an investigation *per se*, nor did it describe an individual's finances, as discussed in those sections.

Where no presumption applies, section 14(2) balances privacy interests against rights of access. The Assistant Commissioner found that the inherently sensitive nature of allegations of criminal activity and the potential for unfair damage to the reputation of innocent property owners and individuals charged with criminal offences weighed in favour of privacy protection. But he ultimately found that considerations favouring access outweighed these privacy interests. Under section 14(2)(a), relating to the important principle of public scrutiny, Assistant Commissioner Beamish pointed out that "[i]t is also central to the *Act* that, in appropriate

circumstances, citizens be provided the opportunity for a glimpse inside an institution so that they may better inform themselves as to its activities. In this way, citizens may more meaningfully scrutinize and evaluate these activities." He also found that disclosure would enhance public confidence in the integrity of the institution.

Promotion of public health and safety (section 14(2)(b)) also favoured disclosure. The Assistant Commissioner agreed with the appellant that disclosure could assist prospective home buyers or current owners of former grow houses because of potential electrical hazards and possible issues with mould.

The order concludes that the balance under section 14(2) favours disclosure of the grow house information except where it pertained to children, where privacy interests were paramount. Assistant Commissioner Beamish ordered that the information relating to property addresses, dates, drugs seized, money seized and criminal charges laid, be disclosed.

PO-2511 – ONTARIO RENTAL HOUSING TRIBUNAL

The Ontario Rental Housing Tribunal received a request for access to an order the tribunal had issued in relation to a specified file number. The tribunal granted partial access to the requested order and an accompanying notice of termination relating to the specified proceeding. The tribunal denied access to the tenant's name, unit number and references to the amounts of rent charges paid and owed on the basis of the personal privacy exemption.

The requester (now the appellant) appealed the denial of access to the name, unit number and financial information. He also raised the public interest in disclosure of tribunal decisions, related arguments of a constitutional nature and other claims relating to the *Statutory Powers Procedure Act*.

The IPC order that closed this appeal deals with important issues regarding disclosure of personal information in decisions by tribunals that are institutions under the *Freedom of Information and Protection of Privacy Act* (the *Act*).

Senior Adjudicator John Higgins relied on earlier IPC decisions with respect to the tenant's name and unit number and determined that this information qualified as the personal information of the tenant under the definition of that term in section 2(1) of the *Act*. Under the circumstances, however, he found that if the name and unit number are not disclosed, the financial information does not qualify as "personal information" since it does not relate to an "identifiable individual." Because it is not personal information, the financial information was found not to be exempt under the personal privacy exemption. It was ordered disclosed.

The senior adjudicator went on to consider whether the disclosure of the tenant's name and unit number would be an unjustified invasion of personal privacy under section 21(1) of the *Act* (personal privacy). To that end, he reviewed the presumption in section 21(3)(f) and the factors in sections 21(2)(a) (public scrutiny of the tribunal's activities) and (d) (fair determination of the requester's rights). He found that section 21(3)(f) did not apply to the tenant's name and unit number as that information does not describe the individual's financial situation. As former Assistant Commissioner Tom Mitchinson had done in Order PO-2265, the senior adjudicator also declined to apply 21(2)(a) because the disclosure of the information would not "add to public scrutiny of the tribunal." Similarly, with respect to the application of section 21(2)(d), the senior adjudicator found that the disclosure of the tenant's name and unit number is not relevant to a fair determination of the rights of the requester, as was also the case in Order PO-2265.

Having found that no factors weighing in favour of disclosure were established, the senior adjudicator ruled that the tenant's name and unit number were exempt from disclosure under the mandatory personal privacy exemption in section 21(1).

The senior adjudicator dismissed the appellant's arguments to the effect that there was a public interest in disclosure under section 23. The appellant had argued that the tribunal, like its predecessor the Ontario Court of Justice, operates as a court of record and relies on precedents in making its decisions on landlord and tenant matters. The senior adjudicator found that there was no "strong interest or attention" in the disclosure of the exempt information (the tenant's name and unit number) and therefore no public interest in it. The public interest in disclosure identified by the appellant relates to the release of the tribunal's decisions generally, and in fact, the requested order had been disclosed in this case subject only to minor severances. The public interest did not require disclosure of the severed information.

With respect to the fact that an open hearing had taken place under the *Tenant Protection Act* and the *Statutory Powers Procedure Act*, the senior adjudicator found that the public nature of the hearing does not dictate that there is a public interest in the disclosure of this information in the tribunal's order. He reiterated that "the identified public interest has been met by the disclosure that has taken place, and the further disclosure mandated by this order." (i.e., the particulars of rent paid and owing).

Senior Adjudicator John Higgins added a postscript urging the tribunal to consider addressing the issue of disclosure of personal information in tribunal decisions by "drafting its orders in a manner which removes personal information and identifiers to better facilitate the public's access to its body of case law."

PO-2483 AND PO-2484 – MINISTRY OF THE ATTORNEY GENERAL

The Ministry of the Attorney General received two separate requests for information about the payment of legal fees and other information relating to lawyers' charges for their services. In one of these, a member of the media requested information about the total fees charged by a number of law firms in relation to appearances by ministers of the Crown and then-Premier Mike Harris at the Walkerton Inquiry. In the other, an individual requested information about amounts billed by ministry counsel to the Ministry of Health and Long-Term Care for legal representation on an appeal before the Health Services Appeal and Review Board in relation to government funding of medical testing for a rare form of eye cancer.

The ministry denied the requests, saying that this information was subject to the solicitor-client privilege exemption under the *Freedom of Information and Protection of Privacy Act*. Both requesters filed appeals with the IPC.

IPC Orders PO-2483 (Walkerton Inquiry) and PO-2484 (health board) review the law regarding the application of common law solicitor-client privilege to information about legal billings and fees. The Supreme Court of Canada addressed this issue in *Maranda v. Richer*, [2003] 3 S.C.R. 193. In *Maranda*, legal fee information was sought as part of the Crown's case against an accused individual. *Maranda* creates a rebuttable presumption that the amount of fees charged by lawyers is subject to solicitor-client privilege because it can reveal privileged solicitor-client communications or other privileged information about the solicitor-client relationship.

Senior Adjudicator John Higgins found that the principles enunciated in *Maranda* apply with respect to all types of legal fee and billing information, including information in a statement of account sent to a client, and that it applies whether the matter concerns the criminal law or other types of legal advice. According to *Maranda*, the presumption that information about legal fees and accounts is privileged can be rebutted where its disclosure will not directly or indirectly reveal a privileged communication. The knowledge already in the possession of a requester can have an important bearing on this question; privilege will apply to prevent an "assiduous inquirer" who is aware of background information relating to the circumstances of the retainer from deducing information that is privileged.

In Order PO-2483, the senior adjudicator found that the disclosure of a summary record created during mediation that listed the global "legal costs," including fees and disbursements, billed by several named law firms would not reveal anything about privileged communications between the various lawyers and their clients concerning the Walkerton Inquiry. On this basis, he found that the presumption of privilege had been rebutted. Actual statements of account issued by the law firms, including narrative descriptions of services rendered were found to be privileged except for information in each invoice pertaining only to the name of the law firm (which was already public knowledge), the date of the statement and the combined grand total of the fees and disbursements in each invoice. The latter were found to be neutral information for which the presumption of privilege had been rebutted.

Background information about disbursements, and the detailed accounting records of the law firms regarding the statements of account could not be characterized as "neutral" as they provided details about the activities undertaken by the law firms on behalf of their clients and their disclosure would either directly or indirectly reveal privileged information.

The records that were not subject to common law solicitor-client privilege were also not subject to the additional statutory privileges provided by the exemption because they were not prepared by or for Crown counsel for use in giving legal advice or for use in existing or contemplated litigation. In Order PO-2483, Senior Adjudicator Higgins ordered disclosure of the summary record and the firm name, date and grand total of fees and disbursements in the law firms' invoices.

In Order PO-2484, the same principles were applied to determine whether the ministry's internal invoices to the Ministry of Health and Long-Term Care fall under the solicitor-client privilege exemption. In that case, the requester had pre-existing knowledge that was a factor in determining what would be revealed by disclosure of the fee information, and only the total amount of each invoice was ordered disclosed. Order PO-2484 is the subject of an application for judicial review.

Both of these orders, as well as the first two cited, are available on the IPC's website, ***www.ipc.on.ca****.*

Privacy

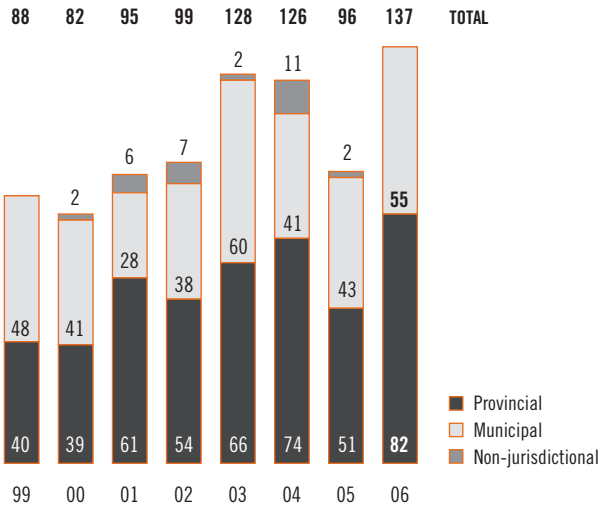
TO PROTECT PEOPLE'S PRIVACY, THE PROVINCIAL AND MUNICIPAL *FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACTS* ESTABLISH RULES THAT GOVERN THE COLLECTION, RETENTION, USE, DISCLOSURE, SECURITY, AND DISPOSAL OF PERSONAL INFORMATION HELD BY GOVERNMENT ORGANIZATIONS.

Anyone who believes that his or her privacy has been compromised because a provincial or municipal government organization failed to comply with one of the *Acts* can file a privacy complaint with the IPC. In the majority of cases, the IPC mediates an informal resolution. The IPC may make formal recommendations to a government organization to amend its practices.

STATISTICAL OVERVIEW

Overall, 170 privacy complaints were **opened** in 2006, a significant increase of 68.3 per cent from 2005, when 101 privacy complaints were opened. Of the 170 privacy complaints, 98 (57.6 per cent) were filed under the provincial *Act* and 72 (42.4 per cent) under the municipal *Act*.

PRIVACY COMPLAINTS *CLOSED* – 1999-2006



Two-thirds of the 170 complaints opened – 113 – were initiated by individuals, while 57 (33.5 per cent) were initiated by the Commissioner. The latter total includes self-reported breaches by institutions. (*Percentage figures are rounded off in this report and may not add up exactly to 100.*)

There were 137 privacy complaints **closed** in 2006. The disclosure of personal information was raised as an issue in 74.5 per cent of complaints. The collection of personal information was an issue in nine per cent of complaints, while security was an issue in 4.8 per cent. The remainder of the privacy complaints under the two public *Acts* involved other issues, including use, retention, notice of collection and consent.

The IPC continues to emphasize informal resolution of all cases, where possible. Accordingly, 125 (91.2 per cent) of the 137 privacy complaints were closed informally without the issuance of a privacy complaint report. Of those 137 complaints, 110 (80.3 per cent) were closed at the intake stage, and 27 (19.7 per cent) at the investigation stage. Twelve privacy complaint reports were issued by the IPC in 2006.

Of the 137 complaints closed, individual members of the public initiated 92 (67.2 per cent) of the complaints and the Commissioner initiated 45 (32.8 per cent). The latter total includes self-reported breaches.

ISSUES* IN PRIVACY COMPLAINTS

	PROVINCIAL		MUNICIPAL		TOTAL	
	No.	%	No.	%	No.	%
Disclosure	65	74.7	43	73.7	**108**	**74.5**
Collection	7	8.0	6	10.5	**13**	**9.0**
Security	3	3.4	4	7.0	**7**	**4.8**
Personal information	4	4.6	0	0.0	**4**	**2.8**
Use	2	2.3	1	1.8	**3**	**2.1**
General privacy issue	3	3.4	0	0.0	**3**	**2.1**
Manner of collection	2	2.3	0	0.0	**2**	**1.4**
Consent	1	1.1	1	1.8	**2**	**1.4**
Accuracy	0	0.0	1	1.8	**1**	**0.7**
Notice of collection	0	0.0	1	1.8	**1**	**0.7**
Retention	0	0.0	1	1.8	**1**	**0.7**
Total	**87**	**100.0**	**58**	**100.0**	**145**	**100.0**

OUTCOME OF ISSUES* IN PRIVACY COMPLAINTS

	PROVINCIAL		MUNICIPAL		TOTAL	
	No.	%	No.	%	No.	%
Resolved –Finding not necessary	69	79.3	41	70.2	**110**	**75.9**
Act does not apply	12	13.8	7	12.3	**19**	**13.1**
Complied in full	6	6.9	7	12.3	**13**	**9.0**
Not complied	0	0.0	3	5.3	**3**	**2.1**
Total	**87**	**100.0**	**58**	**100.0**	**145**	**100.0**

SUMMARY OF PRIVACY COMPLAINTS – 2006

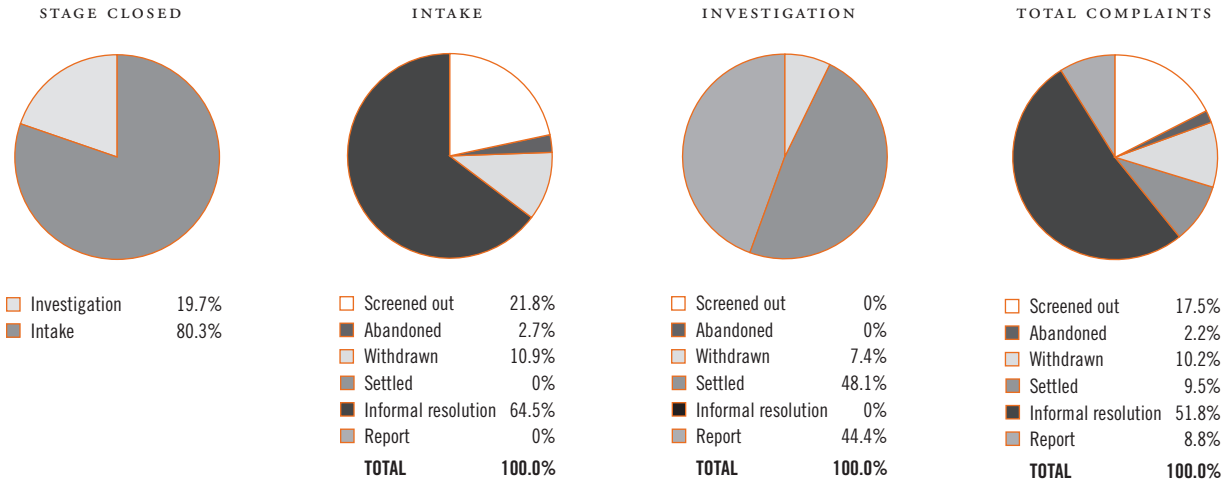
	2005 PRIVACY COMPLAINTS				2006 PRIVACY COMPLAINTS		
	PROVINCIAL	MUNICIPAL	NON-JURISDICTIONAL	TOTAL	PROVINCIAL	MUNICIPAL	TOTAL
Opened	49	50	2	101	98	72	**170**
Closed	51	43	2	96	82	55	**137**

SOURCE OF COMPLAINANTS

	PROVINCIAL		MUNICIPAL		TOTAL	
	No.	%	No.	%	No.	%
Individual	44	53.7	48	87	**92**	**67.2**
Commissioner-initiated	38	46.3	7	13	**45**	**32.8**
Total	**82**	**100.0**	**55**	**100.0**	**137**	**100.0**

** The number of issues does not equal the number of complaints closed, as some complaints may involve more than one issue.*

PRIVACY COMPLAINTS BY RESOLUTION AND STAGE CLOSED



PERSONAL INFORMATION APPEALS

The two public sector *Acts* also provide a right of access to, and correction of, your personal information. If you make a request under one of the *Acts* to a provincial or municipal government organization for your personal information, and you are not satisfied with the response, you can appeal the decision to the IPC.

Personal information appeals may be filed concerning a refusal to provide access to your personal information, a refusal to correct your personal information, the amount of fees charged, the fact that the organization did not respond within the prescribed 30-day period, or other procedural aspects relating to a request. *(Appeals relating to requests for access to* ***general*** *records are covered in the chapter entitled* ***Access****.)*

When an appeal is received, the IPC first attempts to settle it informally. If all the issues cannot be resolved within a reasonable period of time, the IPC may conduct an inquiry and issue a binding order, which could include ordering the government organization to release all or part of the requested information.

Statistical Overview

In 2006, 893 appeals regarding access to general records or personal information were **opened**, an increase of 7.2 per cent compared to the 833 appeals received by the IPC in 2005.

The overall number of appeals **closed** in 2006 was 888, an increase of 17 per cent over the 756 appeals closed in 2005.

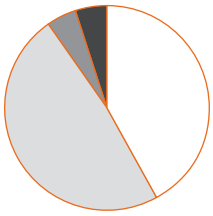
ISSUES* IN PERSONAL INFORMATION APPEALS OPENED

	PROVINCIAL		MUNICIPAL		TOTAL	
	No.	%	No.	%	**No.**	**%**
Exemptions only	86	65.6	124	62.9	**210**	**64.0**
Reasonable search (sole issue)	11	8.4	20	10.2	**31**	**9.5**
Deemed refusal	8	6.1	14	7.1	**22**	**6.7**
Exemptions with other issues	7	5.3	14	7.1	**21**	**6.4**
Other	9	6.9	12	6.1	**21**	**6.4**
Interim decision	3	2.3	1	0.5	**4**	**1.2**
Correction	1	0.8	3	1.5	**4**	**1.2**
Frivolous/Vexatious	0	0.0	4	2.0	**4**	**1.2**
Fee and fee waiver	3	2.3	1	0.5	**4**	**1.2**
Time extension	2	1.5	1	0.5	**3**	**0.9**
Inadequate decision	0	0.0	2	1.0	**2**	**0.6**
Transfer	1	0.8	0	0.0	**1**	**0.3**
Third party	0	0.0	1	0.5	**1**	**0.3**
Total	**131**	**100.0**	**197**	**100.0**	**328**	**100.0**

** The number of issues does not equal the number of complaints closed, as some complaints may involve more than one issue.*

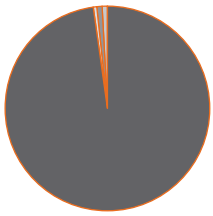
OUTCOME OF APPEALS CLOSED BY STAGE

INTAKE



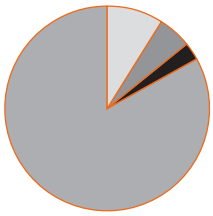
Screened out	42.2%
Mediated in full	0%
Withdrawn	48.2%
Abandoned	4.8%
Other	4.8%
Ordered	0%
TOTAL	**100.0%**

MEDIATION



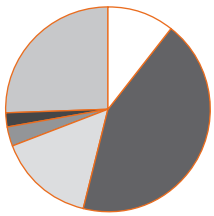
Screened out	0%
Mediated in full	97.9%
Withdrawn	0.7%
Abandoned	0.7%
Other	0%
Ordered	0.7%
TOTAL	**100.0%**

ADJUDICATION



Screened out	0%
Mediated in full	0%
Withdrawn	9.1%
Abandoned	5.1%
Other	3%
Ordered	82.8%
TOTAL	**100.0%**

TOTAL



Screened out	10.7%
Mediated in full	43.3%
Withdrawn	15.3%
Abandoned	3.1%
Other	2.1%
Ordered	25.5%
TOTAL	**100.0%**

ACCESS TO OR CORRECTION OF PERSONAL INFORMATION

Appeals Opened

Overall, 328 appeals regarding access or correction of personal information were **opened** by the IPC in 2006, compared to the 346 appeals received in 2005. Of these appeals, 131 (39.9 per cent) were filed under the provincial *Act* and 197 (60.1 per cent) under the municipal *Act*.

Of the 131 provincial personal information appeals received, 105 (80.2 per cent) involved ministries and 26 (19.8 per cent) involved agencies. The **Ministry of Community Safety and Correctional Services** was involved in the largest number of personal information appeals (81). The **Ministry of Community and Social Services** had the next highest number of personal information appeals (seven).

The agencies with the highest number of personal information appeals included **York University** (six), and **Laurentian University** (four).

Of the 197 municipal personal information appeals received, 144 (73.1 per cent) involved police services, 37 (18.8 per cent) involved municipalities, and nine (4.6 per cent) involved boards of education. Seven appeals (3.6 per cent) involved other types of municipal institutions.

In comparing municipal and provincial appeals, provincial personal information appeals were more likely to involve exemptions only, reasonable search (sole issue) or deemed refusal appeals, while municipal personal information appeals were more likely to involve exemptions only, reasonable search (sole issue) or exemptions with other issues.

Since personal information appeals, by definition, relate to a request for access and/or correction of one's own personal information, all appellants were categorized as individuals. Lawyers (89) or agents (14) represented appellants in 31.4 per cent of the personal information appeals made in 2006.

In 2006, $2,670 in application fees for personal information appeals was paid to the IPC.

Appeals Closed

The IPC closed 326 personal information appeals during 2006 (virtually the same number as 2005, when 327 personal information appeals were closed). While 124 (38 per cent) of these appeals concerned provincial institutions, 202 (62 per cent) concerned municipal institutions.

Of the 326 personal information appeals closed in 2006, 83 (25.5 per cent) were closed during the intake stage, 144 during the mediation stage (42.2 per cent), and 99 (30.4 per cent) during the adjudication stage.

Overall, 25.5 per cent of personal information appeals were closed by issuing an order. The IPC issued 83 final orders for personal information appeals – 33 provincial and 50 municipal. *(In addition, the IPC issued one interim provincial order.)*

In appeals resolved by order, the decision of the head was upheld in 54.2 per cent of the cases. The decision of the head was partly upheld in 36.1 per cent of the cases, while the decision of the head was not upheld in 7.2 per cent of the cases. The remaining 2.4 per cent of the orders issued in 2006 had other outcomes.

OUTCOME OF APPEALS CLOSED OTHER THAN BY ORDER

	PROVINCIAL		MUNICIPAL		TOTAL	
	No.	%	No.	%	**No.**	**%**
Screened out	15	16.5	20	13.2	**35**	**14.4**
Mediated in full	51	56.0	90	59.2	**141**	**58.0**
Withdrawn	18	19.8	32	21.1	**50**	**20.6**
Abandoned	2	2.2	8	5.3	**10**	**4.1**
Other	5	5.5	2	1.3	**7**	**2.9**
Total	**91**	**100.0**	**152**	**100.0**	**243**	**100.0**

OUTCOME OF APPEALS CLOSED BY ORDER

	PROVINCIAL		MUNICIPAL		TOTAL	
HEAD'S DECISION	No.	%	No.	%	**No.**	**%**
Upheld	18	54.5	27	54.0	**45**	**54.2**
Partially upheld	13	39.4	17	34.0	**30**	**36.1**
Not upheld	2	6.1	4	8.0	**6**	**7.2**
Other	0	0.0	2	4.0	**2**	**2.4**
Total	**33**	**100.0**	**50**	**100.0**	**83**	**100.0**

High Profile Privacy Incidents

SUMMARIES OF THREE OF THE PRIVACY INCIDENTS THAT THE IPC DEALT WITH IN 2006

ORDER HO-003 – MARTIN GROVE MEDICAL AND REHAB CENTRE

A privacy investigation late in 2006 led to recommendations dealing with an incident in which personal health records had been left behind when a medical clinic closed.

On September 22, 2006, a staff member of the College of Physicians and Surgeons of Ontario (CPSO) contacted the IPC to advise that a medical and rehabilitation clinic, the Martin Grove Medical and Rehab Centre (the clinic), located in Etobicoke, had closed its operations and left behind records containing personal health information.

The CPSO had been notified by the landlord of the building where the clinic was located that the clinic had abandoned the property prior to the expiration of the lease and had left boxes of health records behind.

The IPC's first priority was to move quickly to ensure that the health records were retrieved. The IPC's Registrar immediately contacted the landlord, who informed the Registrar that he required the immediate removal of the health records due to impending renovations in the building.

Our Registrar personally went to the clinic to retrieve the health records, which were then securely stored at the IPC. The majority of the records consisted of files detailing the provision of physiotherapy and massage therapy services. Other records included invoices for physiotherapy and massage therapy services, physiotherapy sign-in sheets and appointment books, insurance carrier information, a small number of consultation notes and operating room notes relating to patients, and financial records comprised of patient names, physician names and the type of medical service provided by the relevant physician to a particular patient.

The IPC conducted an investigation and interviewed the landlord and the clinic's representative. The representative advised the IPC that the clinic was owned by a numbered company, whose sole director was not part of the day-to-day operations of the clinic. However, the clinic's representative advised the IPC that he and his father were responsible for the clinic's operations. The representative acknowledged that the clinic itself was solely responsible for the records, but was of the understanding that only records created by physicians had to be securely transferred and stored. As a result, health records relating to other practitioners, such as physiotherapists and massage therapists, had been abandoned. The clinic's representative also indicated that he thought that a notice might have been posted at the clinic two weeks prior to its closure, advising patients that the physician would be leaving the clinic, although no such notice could be found.

The clinic's representative, who co-operated with the IPC during the investigation, acknowledged that he was unaware of the *Personal Health Information Protection Act (PHIPA)* and the clinic's obligations under the *Act*.

Following the completion of the investigation, the Commissioner issued her third order (HO-003) under *PHIPA* on December 11, 2006. The Commissioner found that although there were a number of individual health practitioners working at the clinic, the owner of the clinic was the health information custodian, for the purposes of *PHIPA*. The order concluded that the custodian failed to have information practices in place that complied with *PHIPA*, including the lack of a designated contact person and the failure to provide adequate notice to patients that the clinic was

closing. The custodian also failed to take reasonable steps to ensure that the personal health information in its custody and control was protected against theft, loss and unauthorized use or disclosure, as required by *PHIPA*. The custodian also failed to ensure that the personal health information was transferred and stored in a secure manner, and failed to have written contracts in place with its health care practitioners that clearly set out the obligations of the parties regarding records of personal health information.

Based on her findings, the Commissioner ordered the following:

- The custodian was required to ensure the transfer or disposal of the records in the IPC's possession in a secure manner;
- If the records were transferred to a record storage company, the custodian must enter into a written agreement with the record storage company and ensure that the relevant individuals will be provided access to their records; and
- If the custodian operates another group of health care practitioners now or in the future, it must:
  - establish information practices that ensure that records containing personal health information are safeguarded at all times;
  - appoint a staff member to facilitate compliance with *PHIPA*, including the provisions relating to the secure retention, transfer and disposal of personal health information;
  - enter into written contracts with health care practitioners working for the clinic, clearly outlining the obligations of both parties regarding records of personal health information; and
  - in the event of an impending closure, provide a statement to individuals that describes how the records will be stored and how to obtain access to or transfer of those records.

In a postscript to the order, the Commissioner emphasized to all health information custodians that when a custodian ceases operation, the custodian's obligation to retain the records of personal health information in a secure manner does not cease. This includes the obligation to notify patients with sufficient detail so that they can access, or request correction or transfer of, their records.

The Commissioner stressed that having written contracts in place with the custodian's health care practitioners – and policies and procedures that outline the obligations of the parties in the event of changes in practices – will help custodians prevent avoidable situations such as the one reported in order HO-003.

PRIVACY COMPLAINTS MC-050045-1 AND MC-050047-1

The IPC issued a privacy complaint report in 2006 dealing with issues related to the *police reference check* process and *Mental Health Act (MHA)* detainments.

Complaints were received from two individuals raising similar issues. Both complainants had been required to complete a police reference check with the Toronto Police Service (TPS) as part of the application process for a "vulnerable sector position." In this context, the term "vulnerable sector position" refers to a voluntary or paid position where an applicant would be in a position of trust over an individual who is deemed to be vulnerable (such as a child, an elderly person or someone with disabilities).

In both cases, the complainants had previously been the subject of a non-criminal detainment by the Toronto Police under the *MHA*. Under that Act, the police have the power to detain a person where there are reasonable grounds to believe that the individual is acting in a manner where he or she may cause harm to either themself, or to another person. The purpose of such a detainment is to allow the police to take the individual to a location where he or she may be examined by a medical professional.

Years after the detainments, both complainants sought positions working with organizations in the "vulnerable sector." In order to pursue these opportunities, both individuals were required to complete a Toronto Police form entitled, *Police Reference Check Program – Consent to Disclose Personal Information*. Upon receipt of the completed form, the police service conducted a search of its records and, in both cases, identified the individuals' previous detainment under the *MHA*.

As a result of the search, the police sent a letter to the agency that was the subject of each application stating that a police reference check had been conducted and that the applicant had been mailed a summary sheet outlining the information on file with the TPS.

Based on this letter, the agencies in question became aware that the applicant had a record of some type of contact with the TPS. (Where a search does not turn up any contact, the letter sent indicates just that.) In both cases, the applications of the complainants were denied by the agencies in question.

The IPC's privacy complaint report addressed whether the collection and disclosure of personal information by the TPS pertaining to detainments under the *MHA* was in accordance with the provisions of the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).*

With respect to the **collection** of the detainment information, the report concluded that this collection of personal information was permissible as it took place during the course of a law enforcement activity (which is permitted under *MFIPPA*).

With respect to the **disclosure** of the fact that the TPS had some information pertaining to the complainants on file, the report concluded that the disclosure was **not** permissible as the consent form that was used did not clearly state that *MHA* detainments would form a component of the police reference check process. As a result of this finding, the report recommended that the TPS modify its consent form to clearly state that such detainment information may be noted on a police record, and that this may lead to a letter indicating the police service had had contact with the individual being sent to the agency in question.

The report concluded by noting some of the problems that may arise out of the current vulnerable sector screening process, where a letter is sent to the agency in question whenever a *MHA* detainment exists on file. As a result of this process, some individuals with prior *MHA* detainments on file may be effectively excluded from pursuing certain types of employment, as police reference checks are now a customary component of these application processes.

In order to address this problem, the IPC report suggested that the Toronto Police Service include a discretionary risk assessment component to the police reference check process. On a case-by-case basis, the police could determine whether the information on file is indicative of the applicant posing a risk to individuals in the vulnerable sector. Where no risk is seen, the information pertaining to the previous *MHA* detainment need not be reported.

In response to the IPC's report, the TPS wrote to indicate that it would be assessing both its consent form and its policy of disclosing *MHA* information pursuant to police reference checks.

In addition, during the course of the investigation, the IPC was contacted by the Psychiatric Patient Advocate Office (PPAO), which expressed concerns similar to those of the complainants. At the conclusion of the investigation, Commissioner Cavoukian wrote to the PPAO and provided a copy of the report. The Commissioner stated that while she agreed that the current police reference check process may, at times, lead to unfair results, the *MFIPPA* did not contain mechanisms necessary for instructing police services on how to respond to police reference check requests on a case-by-case basis. In her view, specific government legislation may be required to provide police services with proper direction on how to administer their responsibilities to conduct police reference checks.

The *Personal Health Information Protection Act*

THROUGHOUT 2006, THE IPC REFINED ITS POLICIES AND PROCEDURES FOR DEALING WITH ITS NEW MANDATE UNDER THE *PERSONAL HEALTH INFORMATION PROTECTION ACT (PHIPA)*. MUCH OF THE IPC'S WORK FOCUSED ON REVIEWS AND INVESTIGATIONS OF PRACTICES AND PROCEDURES IN THE HEALTH SECTOR TO PROTECT THE PRIVACY AND CONFIDENTIALITY OF PERSONAL HEALTH INFORMATION. THE IPC PRODUCED NEW EDUCATIONAL MATERIAL TO ASSIST THE HEALTH SECTOR IN COMPLYING WITH *PHIPA*, WHICH CAME INTO EFFECT NOVEMBER 1, 2004. THE IPC ALSO REVIEWED AND PROVIDED COMMENTS ON PROPOSED LEGISLATION, POLICY AND PROGRAMS, AS APPROPRIATE.

With respect to complaints under *PHIPA*, the IPC continued to focus on mediation and alternative dispute resolution. Consequently, only two orders were issued under *PHIPA* in 2006. The orders that were issued highlighted the privacy challenges faced with both paper and electronic systems of health records.

ORDERS

HO-002

A complaint under *PHIPA* was received by the IPC concerning unauthorized access and disclosure of a patient's personal health information during and after her treatment at The Ottawa Hospital.

The IPC's investigation determined that, during and after the complainant's treatment at the hospital, a nurse, who is the girlfriend of the patient's estranged husband, accessed the patient's electronic health records in an unauthorized manner on 10 known occasions. The nurse did not provide health care to the complainant at any time.

In her order, the Commissioner spoke to the need for privacy policies to be interwoven into the fabric of a hospital's day-to-day operations, by ensuring that staff are educated about *PHIPA* and the information policies and practices implemented by the hospital and by ensuring that privacy becomes embedded into the institutional culture. Health information custodians are responsible for ensuring compliance with *PHIPA*. As such, it is necessary for custodians to ensure their employees and agents are fully aware and properly trained with respect to their obligations under *PHIPA* and to create environments in which the need for privacy is understood and forms an integral part of the culture of their institutions.

HO-003

A medical and rehabilitation clinic closed its operations and left behind records containing personal health information. The health information custodian's failure to adequately notify individuals when the practice ceased its operations and to ensure that all records of personal health information were retained, transferred or disposed of in a secure manner demonstrated a flagrant disregard for the privacy rights of the individuals to whom the records related.

Included in the Commissioner's order was a directive to the custodian to retain, transfer or dispose of the records in a secure manner, now and in any future practice, in accordance with *PHIPA*.

She also emphasized the need for all health care practitioners who are part of a group practice or a clinic to have contractual agreements regarding records of personal health information to ensure that sensitive records are not simply abandoned when the practice closes.

SPECIAL INVESTIGATION

PHIPA provides the Commissioner with the authority to conduct investigations into alleged contraventions of the legislation. As such, the Commissioner launched an investigation in response to concerns expressed in an article in *Government Health IT* that In-Q-Tel, the venture capital arm of the Central Intelligence Agency, may gain access to the personal health information of Canadians due to its investment in the software company, Initiate Systems Inc. The Commissioner's investigation was undertaken to determine if personal health information was being collected, used or disclosed in contravention of *PHIPA* through the use of the Initiate™ Software in Ontario.

The Initiate Software is used here and in other provinces to help with the integration of health services, enabling an individual's personal health information to be consistently linked across the health sector to the correct individual. The Initiate Software is used to create an *enterprise master person index (EMPI)* consisting of all individuals who receive health care in the province.

The Commissioner concluded that personal health information is only provided to Initiate Systems under very limited, restricted and controlled conditions. Initiate Systems does not have any remote access to the personal health information contained in the *EMPI* and all services are provided, on-site, at locations within the province. Initiate Systems cannot remove personal health information from these locations or transmit personal health information outside of these locations. No personal health information flows outside Ontario.

Further, Initiate Systems confirmed that there is no mechanism in its investment agreement with In-Q-Tel that would allow In-Q-Tel to access personal health information contained in the *EMPI*. Consequently, the investigation found that In-Q-Tel does not have access to any personal health information contained in the *EMPI*.

REVIEWS OF PRESCRIBED ENTITIES, PRESCRIBED PERSONS

PHIPA permits health information custodians to disclose personal health information, without consent, to certain prescribed entities for the purpose of analysis or compiling statistical information needed to plan and manage the health system. Similarly, health information custodians may disclose personal health information, without consent, to certain prescribed persons that compile or maintain registries of personal health information for the purpose of facilitating or improving the provision of health care.

These organizations are required to have their information practices and procedures approved by the IPC. In 2005, the IPC completed its mandated reviews of four prescribed entities and four prescribed persons that compile or maintain registries of personal health information. The IPC continues to monitor the progress of the prescribed entities and persons in meeting the recommendations that the IPC made during these reviews. Given that these prescribed entities and persons are required to have their information practices approved every three years, their practices will be reviewed by the IPC again in 2008.

The prescribed entities are Cancer Care Ontario, the Canadian Institute for Health Information, the Institute for Clinical Evaluative Sciences, and the Pediatric Oncology Group of Ontario. The prescribed "persons" that maintain registries are the Cardiac Care Network of Ontario (registry of cardiac services), INSCYTE (Cytobase), and the Canadian Stroke Network (Registry of the Canadian Stroke Network). The London Health Sciences Centre (Ontario Joint Replacement Registry) is no longer operating its registry.

In 2006, the Critical Care Information System was added as a registry, with Hamilton Health Sciences Corporation being prescribed as the "person" that compiles or maintains the registry. As required under *PHIPA*, the IPC will be assessing Critical Care Information System's practices and procedures through a comprehensive review of all documented privacy and security policies and a visit to the primary site where personal health information is retained. The final report on the review will be posted on the IPC's website.

REGISTRATION OF ARCHIVES

The Queen's University Archives requested that the Commissioner register its intention to act as a recipient of personal health information in accordance with section 14 of Ontario Regulation 329/04. Section 42(3) of *PHIPA* permits a health information custodian to transfer records of personal health information about an individual to a prescribed person whose functions include the collection and preservation of records of historical or archival importance, if the disclosure is made for the purpose of that function. In order to be prescribed as an archive for personal health information, the person must fulfil a number of obligations set out in section 14 of Ontario Regulation 329/04.

The Queen's University Archives made representations to the IPC in support of its request and, after adopting a number of the IPC's recommendations, was registered as an archive under section 42(3) of *PHIPA*.

REVIEW OF SMART SYSTEMS FOR HEALTH AGENCY

In recognizing the need to ensure the privacy of individuals with respect to their personal health information as the health sector moves to an electronic environment, the Ontario government asked the IPC to review the information practices of the Smart Systems for Health Agency (SSHA). Section 6.1 of Ontario Regulation 329/04 requires SSHA, an electronic goods and services provider to health information custodians, to put in place administrative, technical and physical safeguards, practices and procedures that have been reviewed by the IPC.

SSHA is an agency of the Ministry of Health and Long-Term Care. Its mandate is to work with the health care sector in Ontario to enable health information custodians to share personal health information electronically.

The report on the review of SSHA's privacy and security best practices can be found on the IPC's website.

REVIEW OF CUSTODIANS' PRIVACY AND SECURITY PRACTICES

PHIPA's rules regarding the collection, use or disclosure of personal health information apply to any organization or individual involved in the delivery of health care service, including both private sector and public sector organizations.

Given the wide application of *PHIPA*, the IPC receives many requests from private and public sector organizations for assistance in developing and implementing privacy-protective policies, programs, and technological applications. Most requests for review and comment come from health information custodians and from individuals and organizations that receive personal health information from custodians. The IPC attempts to fulfil as many of these requests as possible.

This type of analysis requires that staff have specialized expertise in the areas of health care, information technology, security, and policy and legal analyses.

PRIVACY INVESTIGATIONS

Although *PHIPA* is the only legislation in Canada to require notification of affected individuals in the event of a privacy breach, the legislation does not require that the Privacy Commissioner be notified. Nonetheless, in a number of cases, custodians have reported breaches of *PHIPA* to the IPC. The IPC has developed a protocol for dealing with self-reported privacy breaches and encourages custodians to continue this practice and applauds their forthright and transparent approach.

The most commonly reported threats to personal health information self-reported by custodians involved the theft of laptop computers or the loss of personal health information when employees have removed records from the workplace.

Adequate physical, administrative, and technical measures must be taken to protect personal health information and staff must be made fully aware and properly trained with respect to their obligations under *PHIPA*.

EDUCATIONAL MATERIALS

A *Breach Notification Assessment Tool* was produced jointly by the IPC and the Office of the Information and Privacy Commissioner of British Columbia to assist organizations in making key decisions about notification after a privacy breach has occurred.

The *Breach Notification Assessment Tool* provides checklists of factors that should be taken into consideration when deciding whether to notify, when and how to notify, what to include in a notification and what other organizations should be contacted.

Also in 2006, the IPC produced a fact sheet – *What to do When Faced with a Privacy Breach: Guidelines for the Health Sector* – that covers a number of specific steps for custodians to take following a privacy breach. A privacy breach occurs whenever a person has contravened, or is about to contravene, a provision of *PHIPA* or its regulations. The *Guidelines* include steps that can be taken to avoid privacy breaches and how to respond, contain, investigate, remediate, and notify affected parties of a privacy breach.

The IPC also produced a fact sheet entitled *Health Information Custodians Working for Non-Health Information Custodians*. Examples of such custodians include: a nurse employed by a school board; a doctor employed by a professional sports team; a registered massage therapist providing health care to clients of a spa; or a nurse employed in-house by a manufacturing firm to provide health care. A custodian may work for a non-custodian as an employee, as an independent contractor, or as a volunteer. The fact sheet discusses the responsibilities of such custodians under *PHIPA*, including the disclosure of personal health information and the retention of personal health information records.

PRESENTATIONS

The Commissioner, the Assistant Commissioner and senior staff made a number of keynote and other presentations in 2006 to health professionals at various conferences.

Presentations to health professionals were also made in Belleville, Owen Sound and Thunder Bay as part of the IPC's *Reaching Out to Ontario* program. The IPC team that visited those cities also set up an information table at the largest area hospital in each city, to hand out IPC publications related to *PHIPA* and to answer questions from health professionals, patients and hospital visitors.

TELEPHONE INQUIRIES

The IPC receives numerous inquiries from health care practitioners and the general public regarding *PHIPA*. Some of the more common inquiries involve a parent's right to obtain personal health information concerning his or her child, obtaining the personal health information records of deceased relatives, and guidance on best practices for custodians of personal health information.

DETERMINATIONS

In conducting reviews, whenever the Commissioner must inspect a record of personal health information without the individual's consent, the Commissioner must first determine that it is reasonably necessary to do so and that the public interest in carrying out the review justifies dispensing with consent in the circumstances. The Commissioner must also provide a written statement, to a person who has custody or control of the record, setting out the determination, with brief written reasons and any restrictions and conditions the Commissioner has specified.

In 2006, the Commissioner made one such determination as part of her investigation leading to Order HO-003 (after records of personal health information were abandoned at the premises of a medical clinic when the clinic closed) and issued one written statement in conjunction with that determination. In this case, the owner of the building where the records of personal health information were left wanted to dispose of the records immediately and was unwilling to wait until the Commissioner concluded her review of the matter. Given the volume and amount of time needed to contact each individual to whom the records of personal health information related, the Commissioner decided that it would not be feasible for the IPC to contact each of these individuals to obtain their consent prior to retrieving the records. Accordingly, the Commissioner concluded that the public interest in carrying out the review justified dispensing with obtaining the individuals' consent in the circumstances.

STATISTICAL REVIEW

Statistics related to requests for access to personal health information or privacy complaints filed under *PHIPA* are collected in two separate ways for the IPC's annual report – internally and externally.

The **internal** collection is from the IPC's own records, showing the number and nature of all privacy complaints filed with the IPC in 2006 under *PHIPA*. These are reported in the following section, *Privacy Complaints*.

External collection is through the reports filed by organizations that report to the IPC about *PHIPA*-related matters. External statistical reporting requirements under *PHIPA* do not provide for a comprehensive picture. While all government organizations covered under the *Freedom of Information and Protection of Privacy Act (FIPPA)* and the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)* are required to file a detailed statistical report to the IPC each year, *PHIPA* covers much more than government organizations. Most of these other health information custodians are not required under *PHIPA* to file an annual report to the IPC. Only government organizations that are also health information custodians or that employ one or more health information custodians (from doctors to nurses to ambulance services) are required to report *PHIPA*-related information annually. A few custodians, such as some hospitals, are reporting voluntarily.

A brief review of access requests filed with health information custodians, based on the available external statistics, is in the section entitled *Personal Information Requests*.

PRIVACY COMPLAINTS

Complaints Filed with the IPC

In 2006, 269 complaints were **opened** under *PHIPA* by the IPC, an increase of 52 per cent from the 177 complaints opened in 2005, which was the first full year that *PHIPA* was in effect.

The IPC **closed** 279 *PHIPA* complaints in 2006, an increase of 158 per cent compared to the 108 complaints closed in 2005.

Of the 269 complaints opened in 2006, 86 (32 per cent) were about access to and/or correction of personal health information, while 66 (24.5 per cent) were about the collection, use and/or disclosure of personal health information. Another 93 (34.6 per cent) were self-reported privacy breaches by health information custodians and the other 24 (8.9 per cent) were Commissioner-initiated complaints. *(Percentage figures in this report are rounded off and may not add up to 100.)*

TYPE OF PHIPA COMPLAINT FILES OPENED AT THE IPC IN 2006

CUSTODIANS, AGENTS AND OTHERS	ACCESS/ CORRECTION	COLLECTION/USE/ DISCLOSURE	SELF-REPORTED BREACH	IPC-INITIATED	TOTAL
Public hospitals	17	10	34	5	**66**
Doctors	25	12	4	5	**46**
Clinics	9	8	5	2	**24**
Community health centres	3	5	8	1	**17**
Ministry of Health & Long-Term Care	4	3	9	0	**16**
Other health professionals	4	1	8	0	**13**
Laboratories	2	0	1	3	**6**
CCA centres	1	2	3	0	**6**
Agents	4	1	0	1	**6**
Psychiatric facilities	4	2	0	0	**6**
Pharmacies & Pharmacists	0	1	1	4	**6**
Social workers	1	2	2	0	**5**
Nursing homes	3	2	0	0	**5**
Psychologists	0	2	2	0	**4**
Recipients	0	4	0	0	**4**
Physiotherapists	0	0	3	0	**3**
Prescribed entities	0	0	2	0	**2**
Other prescribed persons	0	0	2	0	**2**
Long-term care facilities	0	0	0	2	**2**
Ambulance services	1	0	1	0	**2**
Boards of health	0	0	2	0	**2**
Drugless practitioners	1	1	0	0	**2**
Others	7	10	6	1	**24**
Total	**86**	**66**	**93**	**24**	**269**

Sixty-six of the complaints opened (24.5 per cent) involved public hospitals, 46 (17.1 per cent) involved doctors, 24 (8.9 per cent) involved clinics, 17 (6.3 per cent) involved community health centres, while 16 (5.9 per cent) involved the Ministry of Health and Long-Term Care. The remaining 100 (37.2 per cent) complaints involved other health information custodians, such as community care access centres, laboratories, psychiatric facilities, ambulance services, social workers, nursing homes and others.

COMPLAINTS CLOSED

Of the 279 *PHIPA* complaints closed, 88 (31.5 per cent) were about access to and/or correction of personal health information; 71 (25.4 per cent) were about the collection, use and/or disclosure of personal health information; 84 (30.1 per cent) were self-reported privacy breaches by health information custodians; and 36 (12.9 per cent) were Commissioner-initiated complaints relating to collection, use or disclosure issues.

All 88 complaints dealing with access to and/or correction of personal health information were resolved without the IPC having to issue an order. In most cases, the complaints were resolved through informal means, such as clarification at the intake stage, where 46 (52.3 per cent) complaints were resolved, or the more formal mediation stage, where 39 (44.3 per cent) were resolved. Only three (3.4 per cent) of the complaints had to be resolved at the adjudication stage.

Turning to the 71 complaints dealing with the collection, use and disclosure of personal health information that were initiated by individual complainants: 55 (77.5 per cent) were closed during the intake stage, 14 (19.7 per cent) during the mediation stage, and two (2.8 per cent) during the adjudication stage.

Of the 84 complaints closed that were self-reported privacy breaches by health information custodians, 62 (73.8 per cent) were closed during the intake stage, and the other 22 (26.2 per cent) were closed during the mediation stage.

Of the 36 complaints dealing with the collection, use and disclosure of personal health information that were Commissioner-initiated, 22 (61.1 per cent) were closed during the intake stage, 13 (36.1 per cent) were closed during the mediation stage, and one (2.8 per cent) was closed during the adjudication stage.

Of the 88 complaints dealing with access to and/or correction of personal health information, 32 (36.4 per cent) were the result of deemed refusals (where a health information custodian fails to respond to the request within the statutory time frame and is thereby deemed to have refused the request). Twelve (13.6 per cent) of the complaints were about the exemptions applied to deny access to personal health information. Nine (10.2 per cent) were related to the correction of personal health information. In another nine complaints (10.2 per cent), the issue was whether the health information custodian had conducted a reasonable search for records of personal health information. Six complaints (6.8 per cent) were about fees, while two (2.3 per cent) were about custodians extending the time frame to respond to a request for access. The remaining 18 complaints (20.5 per cent) involved other issues.

Of the other 191 complaints resolved in 2006, the disclosure of personal health information was the most frequent issue, arising in 143 complaints (74.9 per cent). Security of personal health information was an issue in 40 (20.9 per cent). The collection of personal health information was raised as an issue in nine (4.7 percent) and the consent for the collection, use and/or disclosure of personal health information was raised in six (3.1 per cent). The remaining issues raised included notice of collection, accuracy of personal health information, privacy in general, retention, and use and disposal of personal health information.

PERSONAL INFORMATION REQUESTS

There were 1,973 requests under *PHIPA* for access to, or correction of, personal health information reported to the IPC as being completed during 2006 by government institutions governed by *FIPPA* and *MFIPPA*.

The **Ministry of Health and Long-Term Care** completed 1,722 of these. The ministry was able to complete 1,690 (98.1 per cent) within the statutory 30-day time period, and provided full access to the requested information for 1,657 (96.2 per cent) of the requests.

The ministry charged fees for 115 of the 1,722 requests. A total of $1,843.43 was collected, an average of $16.03 per request. In 21 cases, provisions of *PHIPA* were applied to limit the amount of access provided to the personal health information. Section 52(1)(e) (where there is a risk of harm, or identification of an individual) was the most frequently applied provision to refuse access. It was applied on 11 occasions.

In three cases, the requested information was not accessed following a fee estimate by the ministry.

The remaining 251 requests that were reported to the IPC were made primarily to homes for the aged and nursing homes, ambulance services, boards of health/medical officers of health, and health care practitioners.

The offices of boards of health and medical officers of health reported 149 requests and completed 96 per cent of them within 30 days. **Halton's health unit**, which had the most requests (40), achieved 100 per cent 30-day compliance.

This group of health information custodians charged fees for 69 of the 149 requests, with an average fee of $37.07. Full access to the personal health information requested was provided in 136 (91.3 per cent) cases.

Ambulance services completed 32 requests, with **Halton** (nine) and **Toronto** (eight) receiving the most requests. Overall, the ambulance services reported a 96.9 per cent 30-day compliance rate. Fees were charged for 16 requests, for an average fee of $60.72. Full access to the records requested was provided for 90.6 per cent of the requests.

Homes for the aged and nursing homes reported receiving 32 requests, more than half of them (17) in Toronto. The **Toronto facilities** achieved 70.6 per cent 30-day compliance. The other homes for the aged and nursing homes that reported to the IPC achieved 100 per cent compliance with the 30-day time period. Overall, this category of health information custodians achieved an 84.4 per cent rate of compliance with the 30-day time period. Fees were charged for nine requests, for an average fee of $76.56 per request. Full access to the personal health information sought was provided in 28 of the 32 instances, or 87.5 per cent.

Judicial Reviews

IN 2006, THE ONTARIO COURTS ISSUED IMPORTANT DECISIONS AFFIRMING THE INFORMATION AND PRIVACY COMMISSIONER'S (IPC) STATUTORY AUTHORITY AND PROCESSES FOR INVESTIGATING PRIVACY COMPLAINTS UNDER THE *FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT (FIPPA)* AND THE *MUNICIPAL FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT (MFIPPA)*, AS WELL AS THE IPC'S INTERPRETATION AND APPLICATION OF CORE EXEMPTIONS UNDER THESE STATUTES. THE SUPREME COURT OF CANADA ALSO ESTABLISHED NEW GUIDELINES GOVERNING THE ONTARIO COURTS' PROCESSES ON JUDICIAL REVIEW OF THE IPC'S DECISIONS.

(1) In two landmark decisions released in late 2006, the Divisional Court for the first time affirmed that the Commissioner has the authority as part of her "legislative" functions to investigate and report on privacy complaints brought by members of the public against government institutions, despite the absence of an explicit grant of power under either *FIPPA* or *MFIPPA*. At the same time, the Court held that the Commissioner's privacy rulings are protected by "Parliamentary privilege" and are not subject to judicial review by the courts, because they fall within her general oversight and reporting mandate as an Officer of the Legislature.

Unlike the powers given to the Commissioner under Ontario's *Personal Health Information Protection Act* and to the commissioners under many public sector privacy statutes in other jurisdictions in Canada, Ontario's *FIPPA* and *MFIPPA* do not give the IPC express "tribunal" powers to investigate complaints and make decisions concerning alleged breaches of the personal privacy protections in these statutes. In previous annual reports, and in other submissions to the Legislative Assembly, the IPC has recommended that Ontario's public sector privacy laws be amended to set out explicitly the IPC's powers, duties and processes in conducting investigations into complaints of privacy breaches by government and other public institutions.

In its two rulings, the Court found that the IPC's function of investigating and reporting on privacy complaints is a discretionary one, grounded in the Commissioner's authority to receive representations from the public concerning the operation of *FIPPA* and *MFIPPA* and her duty to report annually to the Legislative Assembly concerning the effectiveness of these statutes in protecting personal privacy. The IPC's annual reports to the Legislature must include an assessment of the extent to which institutions are complying with the statutes, as well as recommendations with respect to the practices of particular institutions. The Court summarized its conclusions as follows:

> .... [T]he Commissioner is acting within the legislative sphere in collecting information about privacy issues that she obtains from accepting, investigating and reporting on the complaints she receives from the public... [T]he scope and supervision of the activities of the Commissioner in gathering information to fulfil her duty as an Officer of the Legislature to report to it on the operation of these Acts is a matter for the House and not for the courts.

The Court went on to hold that, even if it did have the authority to review the IPC's privacy rulings, her decisions not

to investigate the two complaints brought under *MFIPPA* in these cases were correct and reasonable, and arrived at in a fair and unbiased fashion.

In a third related decision, the Divisional Court held that the IPC was correct in deciding that the municipal institution in question did not have custody or control of the interview notes of an independent investigator which it retained to report on allegations of impropriety in the bidding process on a municipal project. Accordingly, the investigator's records were not subject to *MFIPPA* or accessible pursuant to a request for access made under that statute.

(2) In another ruling, the Divisional Court upheld the IPC's decision ordering the Ministry of the Attorney General (MAG) to disclose to a media requester financial reporting records provided to it by an Ontario First Nations organization (the "OFN") set up to receive revenues derived from the operation of Casino Rama and distribute these to its First Nations band members. The OFN was required to file these records with MAG in order to demonstrate that the revenues it received from the casino operations were properly accounted for and equitably distributed to member bands for social, economic and cultural development. MAG and the OFN both claimed the records were exempt under the "third party" exemption for commercial information at section 17 of *FIPPA*.

The OFN was not involved in the day-to-day operations of the casino, which was managed by the Ontario Lottery and Gaming Corporation. The IPC found that the commercial source of revenue from the casino operations did not transform the essential nature of the First Nations' financial auditing information into "commercial" information. The IPC also found that the OFN was not itself engaged in competitive commercial activity and that it had not provided the level of "detailed and convincing evidence" necessary to establish a reasonable expectation of harm to any commercial or competitive interests, including the revenue generating capacity of the casino. Accordingly, the IPC concluded that the records did not satisfy the test for exemption from disclosure under section 17. In upholding the IPC's decision on a standard of reasonableness, the Court affirmed the principle of public accountability in the distribution and expenditure of funds generated from public sources.

(3) In 2006, the Supreme Court of Canada issued its first judgment in an appeal from a decision of the Ontario Court of Appeal on a procedural issue arising in an application for judicial review of an IPC decision. The case involved a journalist's request for access to records relating to allegations of sexual abuse of offenders by employees of the then-Ministry of Correctional Services. In the decision subject to judicial review, the IPC upheld the ministry's decision denying access on the basis that the great majority of requested records were exempt from disclosure under the solicitor-client privilege exemption at section 19 of *FIPPA*. However, the IPC found that some of these records were not exempt and ordered them disclosed to the requester. The ministry then brought an application for judicial review seeking to protect all of the records from disclosure.

In the course of these proceedings, the requester secured an order of a judge of the Divisional Court permitting her counsel to have access to all the disputed records on a confidential basis for the purpose of making informed arguments to the Court. This decision was upheld by a three judge panel of the Divisional Court and by the Ontario Court of Appeal on the basis that the Court has the discretion to afford procedural fairness to a party by granting limited access to counsel bound by a confidentiality undertaking. The Supreme Court of Canada overturned the Ontario Courts' decisions, holding that solicitor-client privilege should not be interfered with except in a case of "absolute necessity" which was not present here. The Supreme Court went on to hold that the Ontario Courts were not bound by the provisions of *FIPPA* requiring the IPC to maintain strict confidentiality over any records at issue, and that the Ontario Courts had the authority to grant counsel confidential access in other cases where disputed records are not subject to a claim of solicitor-client privilege.

(4) In another case heard this past year, the Divisional Court upheld two IPC decisions finding that records relating to a requester's prosecution for fraud in 1982 were exempt from disclosure under *FIPPA* and *MFIPPA*. After the charges against the requester were dismissed, he sought access to records held by the Ministry of the Attorney General and a municipal police force for use in his action for malicious prosecution against the investigating RCMP officer. On appeal from the ministry and police decisions denying access, the IPC found that the bulk of the records consisting of witness statements and police occurrence reports were exempt under section 21 of *FIPPA* and section 14 of *MFIPPA* as personal information compiled in an investigation into a possible violation of law, the disclosure of which was presumed to constitute an unjustified invasion of the privacy of others. The IPC also found that one of the records was exempt as "advice" under section 13(1) of *FIPPA* and another record was exempt as a law enforcement report under section 8(2) of *MFIPPA*.

In holding that the IPC's decisions were reasonable, the Court affirmed the principle that the statutory presumption of privacy invasion cannot be rebutted. The Court also affirmed the IPC's view that the Crown's obligation to make full disclosure in a criminal prosecution did apply in an access to information context. Finally, the Court agreed with the IPC that a requester's private interest in gaining access to information for prosecuting a civil action did not constitute a "public interest" in disclosure that could override the application of the exemptions.

(5) In a case involving a request for records relating to the "Mega Studio Project" in the Toronto Port Lands, a majority of the Divisional Court ruled that the City of Toronto Economic Development Corporation (TEDCO) is not covered by *MFIPPA*. The requester, a film studio company, made requests to the City of Toronto and to TEDCO. Both denied access on the basis that *MFIPPA* does not apply to TEDCO. On appeal, the IPC found that TEDCO is a corporation wholly owned by the city, and that the city appoints all of TEDCO's directors, who are its "controlling minds." On this basis, the IPC concluded that TEDCO is a part of the city under section 2(3) of *MFIPPA*. TEDCO applied for judicial review of the IPC's decision.

The majority of the Divisional Court held that the IPC erred in interpreting the word "officers" in section 2(3) of *MFIPPA* to include the directors of TEDCO. Rather, the majority stated that the IPC should have adopted the narrower meaning of officers contained in Ontario's *Business Corporations Act*. The majority also stated there was no evidence that TEDCO's directors are its "controlling minds." A dissenting judge found that the IPC correctly ruled that the term "officer" in section 2(3) may include the directors of TEDCO and that there was evidence that TEDCO's directors are its "controlling minds." This judge also stated that the IPC's decision was consistent with the purpose of *MFIPPA*, given that TEDCO carries out important public functions, and the city is the sole shareholder of TEDCO.

The requester and the IPC have applied to the Ontario Court of Appeal for leave to appeal the Divisional Court's decision.

(6) In the continuation of two cases first heard in 2004, and summarized in the IPC's 2005 annual report, the Supreme Court of Canada refused to grant the Ministry of Transportation and the Ministry of Northern Development and Mines leave to appeal from two decisions of the Ontario Court of Appeal. In those decisions, the Court of Appeal had affirmed the IPC's interpretation and application of the "advice to government" exemption at section 13 of *FIPPA*. In reaching this decision, the Court stated that, if the ministries' interpretation were adopted, "…the public's right to information would be severely diminished because much communication within government would fall within the broad meaning of advice." These decisions have great significance for preserving and promoting open government and accountability.

2006 JUDICIAL REVIEW STATISTICS

NEW JUDICIAL REVIEW APPLICATIONS RECEIVED IN 2006

Launched by:	
Institutions[1]	3
Requesters[2]	2
Affected parties[3]	3
Total	**8**

OUTSTANDING JUDICIAL REVIEWS AS OF DECEMBER 31, 2006

Launched by:	
Institutions	5
Requesters	3
Institution and other party	6
Affected parties	8
Total	**22**

JUDICIAL REVIEWS CLOSED/HEARD IN 2006

Abandoned (Order reconsidered)[4]	1
Abandoned (Order stands)[5]	1
Heard but not closed (appeal pending)[6]	1
Matter remitted back to IPC	–
IPC Order/Decision upheld[7]	12
IPC Order not upheld (appeal pending)[8]	1
IPC Order upheld in part[9]	1
Appeal on procedural motion allowed[10]	1
Dismissed for delay (Order stands)[11]	2
Dismissed for delay (non-jurisdictional)[12]	1
Total	**21**

1 PO-2455, PO-2456, PO-2484
2 PO-2455, MO-1929
3 PO-2491, PO-2496, PO-2497
4 MO-1935
5 MO-1742
6 PO-1779
7 P-1579, P-1582, PO-1993 (2 JR Applications), PO-2028, PO-2084 (Leave applications to the S.C.C. in PO-1993, PO-2028 and PO-2084 heard together), PO-2328, M-1124, MO-1844 (Leave application to C.A. and S.C.C. dismissed), MO-1892, Decision in Privacy Complaints MC-030029-1 & MC-030029-2, Decision in Privacy Complaints MC-030028-1 & MC-030043-1
8 MO-1966
9 PO-1664
10 PO-1905 (S.C.C. - decisions in lower courts quashed)
11 MO-1923-R, PO-2418
12 MA-040360-1

Outreach Program

One of the key responsibilities of the IPC is to help increase public awareness of access and privacy issues and individuals' rights under Ontario's access and privacy laws. The IPC has a multi-layered outreach program to accomplish this goal.

The IPC's corporate outreach program is based on five key elements:

- the public speaking program, led by Commissioner Cavoukian;
- the school program, *What Students Need to Know about Freedom of Information and Protection of Privacy* – under which every student in Ontario will ultimately study access and privacy;
- the publications program;
- the media relations program; and
- the IPC's extensive website.

The first four of those elements are all interwoven into the IPC's *Reaching Out to Ontario (ROTO)* program. Under *ROTO*, an IPC team visits three or four Ontario cities or regions each year for a series of presentations, seminars and meetings (public speaking, distributing IPC publications, meeting with school board curriculum staff regarding the free IPC teachers' kits, and meeting with area media). In 2006, IPC teams visited Belleville, Owen Sound and Thunder Bay. A presentation to area health professionals on the *Personal Health Information Protection Act (PHIPA)* was a key part of all three educational initiatives, as was an information table the IPC set up at a leading hospital in each city.

Speeches and Presentations

Commissioner Cavoukian gave 32 keynote presentations at major conferences and workshops in 2006 – to a diverse group of organizations in the public, private and academic sectors.

Among the presentations given were those to: the International Association of Privacy Professionals, the European Biometrics Forum, Ontario's first Right to Know Week event, the International Association of Business Communicators, the Women of Influence series, the National Association for Information Destruction Canada, the Ontario Bar Association, the International Fraud Investigators' Conference organized by the Toronto police, the Ontario Occupational Health Nurses Association, an Insight conference on health information privacy and security – and the Ethics at Ryerson Speakers Series and Bishop Strachan School, both of which were part of the Commissioner's public information campaign aimed at getting university, college and high school students to think about the potential implications, short term and long term, before posting personal information on a social networking website.

Other segments of the IPC's speakers' program include:

- presentations by the IPC's two Assistant Commissioners and senior staff to various organizations; and
- a media program, under which presentations are made to editorial boards or newsroom staff on the role of the IPC and access and privacy issues. The IPC's Communications Co-ordinator also addresses university and college journalism and electronic media classes.

IPC Publications

The IPC released 15 publications and videos on access or privacy topics in 2006. These include three videos released for training or educational purposes: *The Personal Health Information Protection Act – A Video Guide for Training and Education; A Word About RFIDs and Your Privacy…in the Retail Sector,* and *Get together, win together: Mediation at the IPC.*

Among the papers released was the ground-breaking *7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity in the Digital Age* (a white paper and a brochure described in detail elsewhere in this annual report). Other 2006 publications that address evolving issues included *Privacy Guidelines for RFID Information Systems,* and *Reduce Your Roaming Risks: A Portable Privacy Primer*.

Schools Program

The IPC's popular schools program, *What Students Need to Know About Freedom of Information and Protection of Privacy*, has free teachers' kits tailored to the Grade 5 social studies curriculum (where students first study government) and the mandatory Grade 10 civics course (where access and privacy, following submissions by the IPC, are part of the curriculum). A third guide provides resources for Grade 11 and 12 history and law teachers. In addition, IPC staff members make presentations to a number of Grade 5 classes every school year.

The teachers' guides, developed by the IPC with the aid of curriculum professionals and classroom teachers – and brochures that describe the guides – are available on the IPC's website in the *Resources/Education Materials* section.

Since the IPC's schools' program was launched in the 1999-2000 school year with the release of the guide for Grade 5 teachers, more than 32,000 copies of the guides have either been sent to teachers or downloaded from the IPC's website.

Media Relations

As media reports are one of the ways that Ontarians learn about access and privacy issues, the IPC has a proactive media relations program to help raise the media's awareness of access and privacy issues. Among the elements of this program are meetings with editorial boards, presentations to newsrooms and media students, and the distribution of news releases, IPC publications and other material.

IPC PUBLICATIONS

The IPC has an extensive publishing program aimed at fostering increased awareness and understanding of various access and privacy-related issues. The papers and videos released in 2006, in chronological order, included:

TITLE	FORMAT
▪ *Health Information Custodians Working for Non-Health Information Custodians*	FACT SHEET
▪ *A Word About RFIDs and your Privacy in the Retail Sector*	VIDEO
▪ *Get together, win together: Mediation at the IPC*	VIDEO
▪ The spring 2006 edition of the newsletter, *IPC Perspectives*	
▪ *The Personal Health Information Protection Act – A Video Guide for Training and Education*	VIDEO
▪ *What to do When Faced With a Privacy Breach: Guidelines for the Health Sector*	
▪ *Privacy Guidelines for RFID Information Systems*	
▪ *Practical Tips for Implementing RFID Privacy Guidelines*	
▪ The Commissioner's 2005 annual report	
▪ *If you wanted to know … How to access your personal information held by a municipal organization*	
▪ *Reduce Your Roaming Risks: A Portable Privacy Primer*	
▪ *When Online Gets Out of Line: Privacy – Make an Informed Online Choice*	
▪ *7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity in the Digital Age*	WHITE PAPER AND BROCHURE
▪ *Breach Notification Assessment Tool*	

IPC publications are available on the IPC's website, ***www.ipc.on.ca****, or by calling the Communications Department at 416-326-3333 or 1-800-387-0073 to request copies of specific publications.*

IPC staff also answer media inquiries relating to freedom of information, protection of privacy, and the *Personal Health Information Protection Act*.

The Commissioner gave 91 media interviews in 2006, to media organizations from all across Canada and beyond. Overall, the IPC assisted more than 170 journalists who requested interviews or background information or who had general inquiries about access and privacy, including the process for filing freedom of information requests. The Commissioner issued 10 news releases in 2006.

Website Resources

In late October 2006, the IPC rolled out its newly redesigned website, delivering improved access for visitors via a more user-friendly interface with the IPC's extensive and growing collection of online resources, including more than 5,000 orders and investigation reports, and hundreds of publications.

The most popular online resource in 2006 was *Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology*. Two other RFID papers were in the top four: *Privacy Guidelines for RFID Information Systems* (released in June 2006) and *Guidelines for Using RFID Tags in Ontario Public Libraries*. The second most popular online resource in 2006 was the *Commissioner's PHIPA Highlights #2*.

Four out of the top 10 most visited online resources were health-related documents. The perennially popular *A Guide to the Personal Health Information Protection Act*, 2005's most referenced paper, ranked fifth in 2006.

On a per-month basis, however, the *7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity in the Digital Age* (White Paper), drew the most attention. Released in October, it had more hits than the next five most popular papers combined that month. Overall, it finished in sixth place for the year, despite being available for less than three months.

Other popular online resources in 2006, based on the number of visits, included the IPC's *2005 Annual Report, Health Order 001 Executive Summary, Health Order 001,* and *Health Order 002 Executive Summary.*

Monitoring Legislation, Programs, and Information Practices

PART OF THE MANDATE OF THE IPC UNDER THE *ACTS* IS TO OFFER COMMENT ON THE PRIVACY PROTECTION AND ACCESS IMPLICATIONS OF PROPOSED GOVERNMENT LEGISLATIVE SCHEMES OR PROGRAMS, AND EXISTING OR PROPOSED INFORMATION PRACTICES OF HEALTH INFORMATION CUSTODIANS. THE FOLLOWING LIST PROVIDES A SAMPLING OF THE WORK DONE BY THE IPC IN THIS AREA DURING 2006.

PROVINCIAL CONSULTATIONS

Ministry of Community Safety and Correctional Services:
Bill 56, *Emergency Management Statute Law Amendment Act, 2006*

Ministry of Community and Social Services:
Regulations to the *Adoption Information Disclosure Act, 2005*

Ministry of Energy:
Bill 21, the *Energy Conservation Responsibility Act, 2006*

Ministry of Government Services:
Bill 152, the *Consumer Protection and Service Modernization Act, 2006*

Ministry of Health and Long-Term Care:
Bill 171, the *Health System Improvements Act, 2006*

Ministry of Labour:
Bill 69, the *Regulatory Modernization Act, 2006*

Ministry of Municipal Affairs and Housing:
Bill 130, the *Municipal Statute Law Amendment Act, 2006*

MUNICIPAL CONSULTATIONS

City of Windsor: Video surveillance

Toronto Police Service: Video surveillance
Toronto Transit Commission: Video surveillance

In addition to the consultations listed below, the IPC worked with numerous non-government health information custodians on matters related to the *Personal Health Information Protection Act, 2004*, including the health professions associations and regulatory colleges, prescribed registries and entities under the *Act*, individual hospitals and many more.

HEALTH INFORMATION CUSTODIANS CONSULTATIONS

Ministry of Health and Long-Term Care:
PHIPA regulations
Ontario Laboratory Information System

Smart Systems for Health Agency:
Review of information practices in accordance with a regulation under *PHIPA*

INDIRECT COLLECTIONS

Ministry of Transportation:
Driver record database management

SUBMISSIONS AND SPECIAL REPORTS

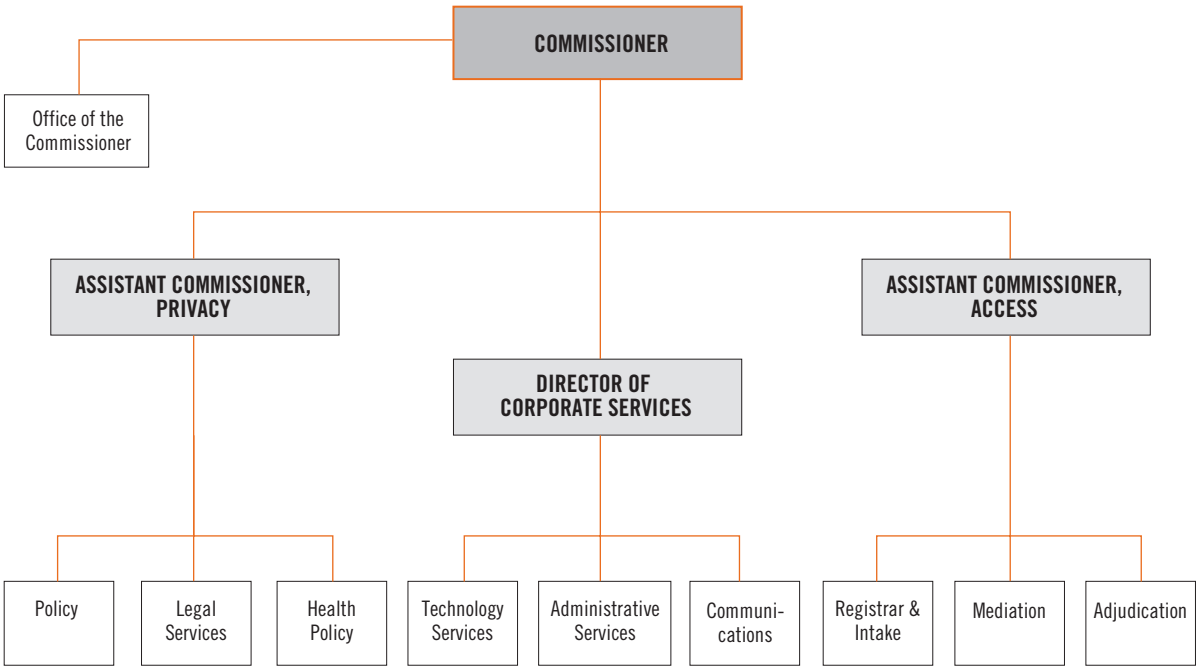
A letter from Commissioner Ann Cavoukian to the Honourable Maxime Bernier, Federal Minister of Industry, and the Honourable Bev Oda, Federal Minister of Canadian Heritage, regarding the privacy implications of digital rights management technology and copyright reform;

A letter from Commissioner Ann Cavoukian to Alok Mukherjee, Chair of the Toronto Police Services Board, regarding upholding the right to expunge non-conviction records;

A letter from Assistant Commissioner (Access) Brian Beamish to Shafiq Qaadri, MPP, Chair, Standing Committee on Social Policy, regarding Bill 152, Consumer Protection and Service Modernization Act, 2006 amendments to Freedom of Information and Protection of Privacy Legislation.

A letter from Assistant Commissioner (Privacy) Ken Anderson to Ernie Parsons, MPP, Chair, Standing Committee on Social Policy, regarding Bill 140, Long-Term Care Homes Act, 2006.

ORGANIZATIONAL CHART



FINANCIAL STATEMENT

The financial administration of the IPC is audited on an annual basis by the Office of the Auditor General of Ontario.

	2006-2007 ESTIMATES $	2005-2006 ESTIMATES $	2005-2006 ACTUAL $
Salaries and wages	8,239,000	7,904,000	7,176,818
Employee benefits	1,771,500	1,699,400	1,265,615
Transportation and communications	323,700	255,400	317,130
Services	1,523,800	1,492,000	2,055,929
Supplies and equipment	274,800	374,900	334,382
Total	**12,132,800**	**11,725,700**	**11,149,874**

Note: The IPC's fiscal year begins April 1 and ends March 31.

PUBLIC SECTOR SALARY DISCLOSURE

As required by the *Public Sector Salary Disclosure Act*, 1996, the following chart shows which IPC employees received more than $100,000 in salary and benefits for the calendar year ending December 31, 2006.

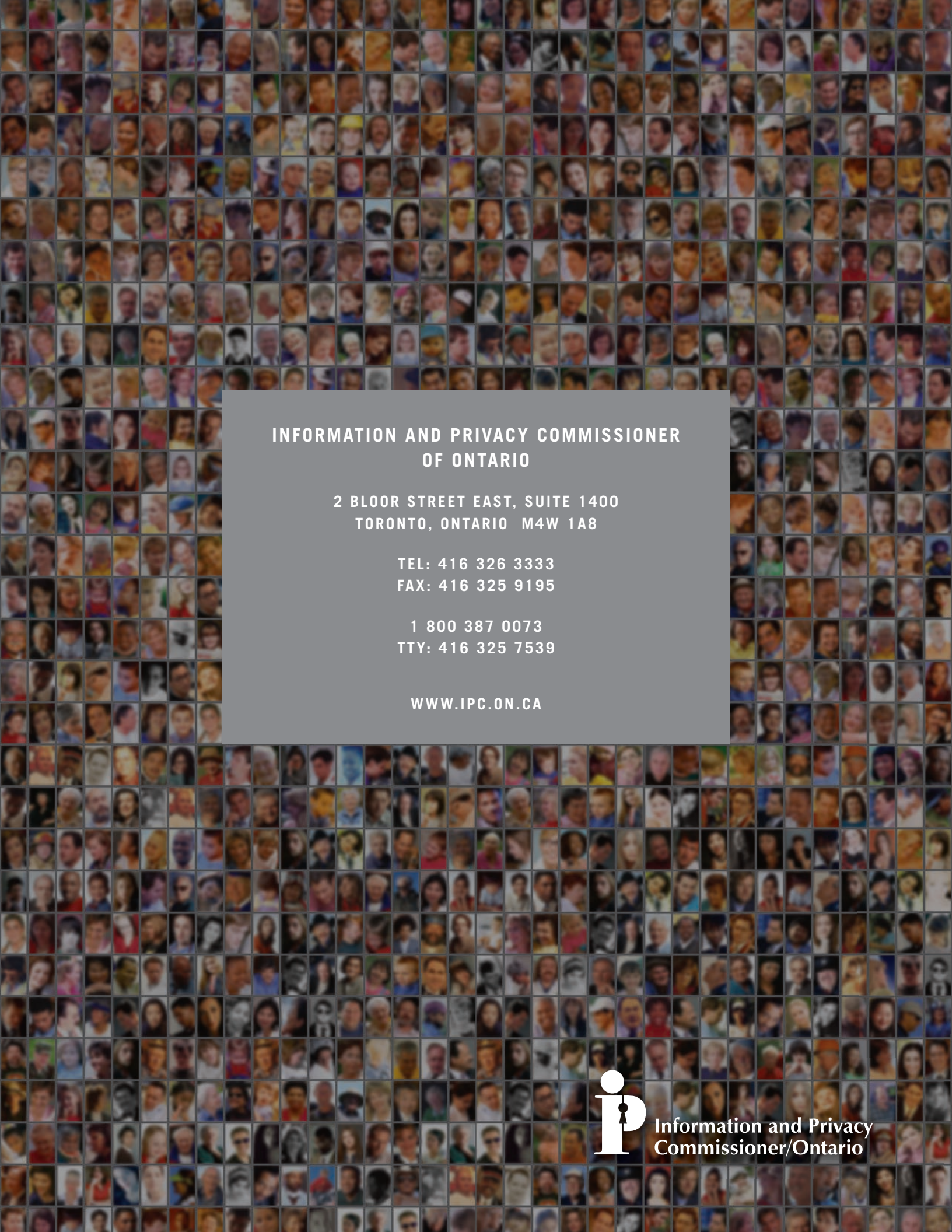
APPENDIX 1

NAME	POSITION	EARNINGS $	TAXABLE BENEFITS $
CAVOUKIAN, Ann	Commissioner	192,103.93	332.35
ANDERSON, Ken	Assistant Commissioner, Privacy	203,121.96	315.10
BEAMISH, Brian	Assistant Commissioner, Access	203,013.69	315.10
BINSTOCK, Robert	Registrar	105,012.74	186.10
CHALLIS, William	General Counsel	192,000.18	313.82
DI RE, Manuela	Health Law Legal Counsel	121,737.88	202.85
FAUGHNAN, Steven	Adjudicator	108,802.24	187.05
GEISBERGER, Janet	Director, Corporate Services	114,695.04	199.68
GOLDSTEIN, Judith	Legal Counsel	177,564.31	288.00
GOODIS, David	Legal Counsel	186,413.45	289.37
GRANT, Debra	Senior Health Specialist	111,934.29	177.21
HALE, Donald	Team Leader, Adjudication	113,369.77	196.87
HIGGINS, John	Manager, Adjudication	186,421.41	289.37
LIANG, Sherry	Legal Counsel	117,212.58	204.61
McCAMMON, Stephen	Legal Counsel	128,328.05	109.93
MORROW, Bernard	Adjudicator	108,802.24	187.05
O'DONOGHUE, Mary	Manager, Legal Services	196,691.77	309.72
SENOFF, Shirley	Legal Counsel	122,381.64	203.02
SWAIGEN, John	Legal Counsel	179,190.72	289.37

STATEMENT OF DISCLOSURE

All images of individual persons depicted in this publication have been purchased from a vendor in compliance with copyright laws.

DESIGN: nectar design + communications **www.nectardesign.ca** PRINTED IN CANADA



INFORMATION AND PRIVACY COMMISSIONER
OF ONTARIO

2 BLOOR STREET EAST, SUITE 1400
TORONTO, ONTARIO M4W 1A8

TEL: 416 326 3333
FAX: 416 325 9195

1 800 387 0073
TTY: 416 325 7539

WWW.IPC.ON.CA

Information and Privacy
Commissioner/Ontario