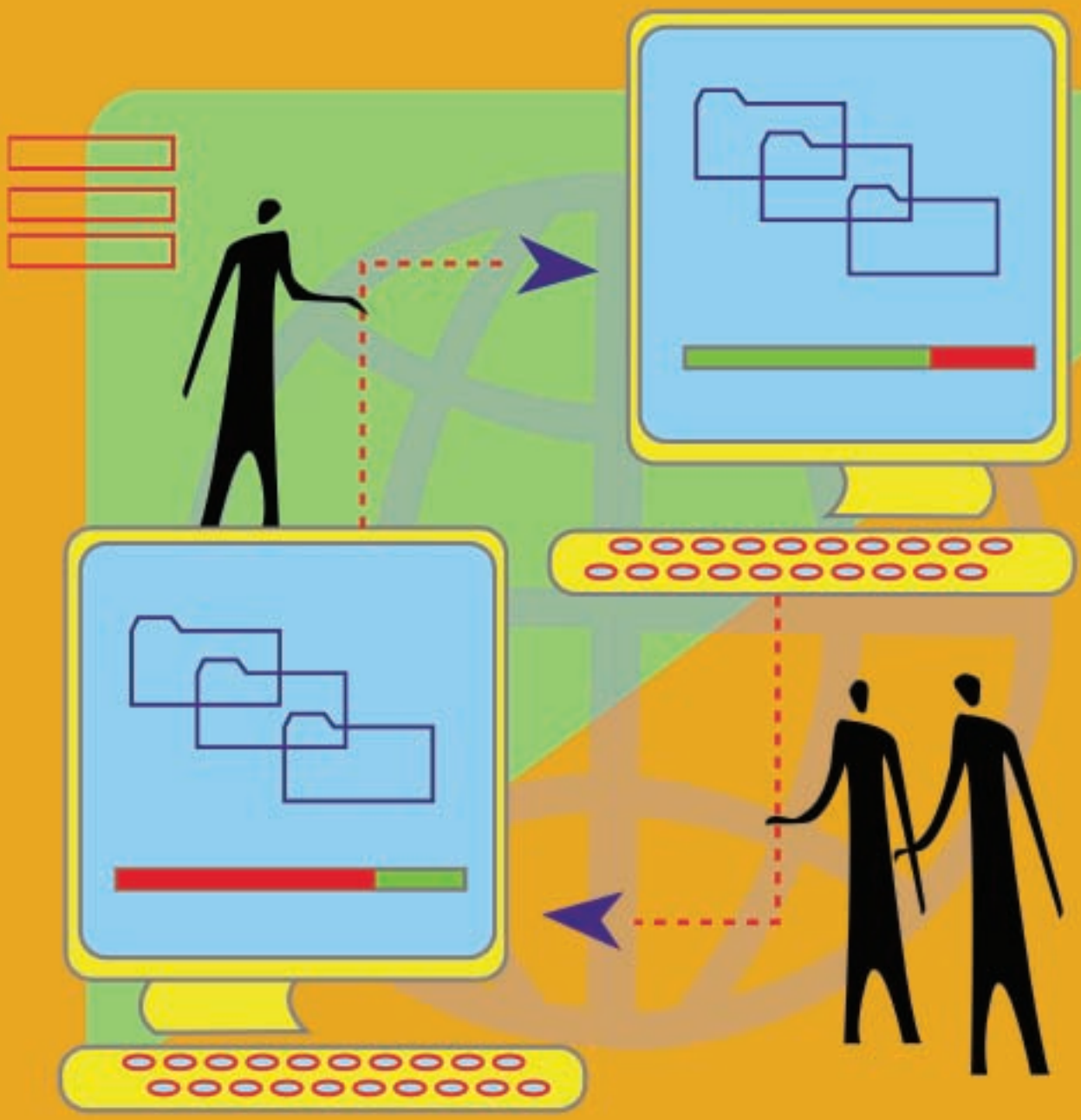


Information & Privacy Commissioner/Ontario

Annual Report 2005

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.

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

June 27, 2006

The Honourable Michael Brown
Speaker of the Legislative Assembly

I have the honour to present the 2005 annual report of the Information and Privacy Commissioner/Ontario to the Legislative Assembly.

This report covers the period from January 1, 2005 to December 31, 2005.

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

role and mandate

Ontario's *Freedom of Information and Protection of Privacy Act*, which came into effect on January 1, 1988, established an Information and Privacy Commissioner (IPC) as an officer of the Legislature to provide an independent review of the decisions and practices of government organizations concerning access and privacy. The Commissioner 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, 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 is the oversight agency. *PHIPA* governs the collection, use and disclosure of personal health information within the health care system.

The Information and Privacy Commissioner plays a crucial role under the three *Acts*. Together, the *Acts* 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 and health information custodians.

The provincial *Act* applies to all provincial ministries and most provincial agencies, boards and commissions, and to universities and colleges of applied arts and technology. The municipal *Act* 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 and control of health information custodians. The *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.

The mandate of the IPC under the *Acts* is to provide an independent review of government decisions and practices concerning access and privacy. 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; and
- 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.

table of contents

commissioner's message

2005 proved to be a year of challenge and inspiration for my office. Helping thousands of health professionals apply the new *Personal Health Information Protection Act (PHIPA)* to day-to-day events and processes was a real challenge. However, seeing how the health sector has embraced and implemented *PHIPA* was extremely gratifying. Unfortunately, our work in another area was less successful, and in fact, very disappointing. Here, I am referring to my inability to convince the government to include much-needed amendments to the *Adoption Information Disclosure Act, 2005*.

ADOPTION INFORMATION DISCLOSURE ACT, 2005

Ann Cavoukian, Ph.D.
Commissioner

My office receives numerous compelling phone calls, letters and e-mails on a number of privacy and access issues every year. But no other subject has ever sparked such an emotional outcry as Bill 183, the *Adoption Information Disclosure Act, 2005*, which was introduced in the Ontario Legislature on March 29, 2005.

The *Act* provides adopted persons and birth parents with a right of access to each other's personally identifying information in adoption-related records. From the day of the bill's introduction, controversy erupted. The most controversial issue was the retroactive application of the bill. While we did not oppose the proposed retroactivity, we sought an amendment that would provide a disclosure veto.

As Commissioner, I am entrusted with a mandate, on behalf of all Ontarians, to comment on proposed legislation that has implications for privacy and access. With regard to Bill 183, I strongly believed (and still do) that retroactively exposing the identities of birth parents and adoptees against their will is wrong, especially in light of promises of confidentiality, with the potential to disrupt the lives of many individuals and families.

In May 2005, I conveyed my concerns to the Standing Committee on Social Policy. As a way to achieve a fair balance between access and privacy rights, I urged then-Community and Social Services Minister Sandra Pupatello to amend the bill to give birth parents and adoptees the right to file a disclosure veto for adoptions that occurred prior to the introduction of the new legislation. These disclosure vetoes would have allowed birth parents and adoptees who did not wish to have their identities revealed to block access to their files. While some of the minor changes we proposed in discussions and through our formal submission were accepted, my disclosure veto proposal was not adopted by the government.

Over a period of eight months, I spoke out against the proposed version of Bill 183. I cannot tell you how deeply moved I was by the calls and letters I received from very frightened and concerned birth parents and adoptees. Some of the callers were, literally, in tears and had trouble speaking. Some expressed feelings of anger and betrayal at the prospect of their sealed files being opened. The amount of faith and hope that these people placed in me and my office motivated me on a profound level not only to perform my duty as Commissioner, but also as an individual who heard the pleas of individuals who looked to my office to prevent their lives from being severely disrupted. They asked me to speak out on their behalf because they could not – for to come forward would mean forfeiting the very privacy they were so desperately seeking to protect.

On November 3, 2005, Bill 183, the *Adoption Information Disclosure Act, 2005,* received Royal Assent and became law – without the protective disclosure veto which I advocated. To say that I was disappointed would be an understatement. I could not offer any protection to the numerous individuals who had called and written, asking that I protect their privacy. I offer my sincere apologies to all of you. The law will come into effect in early 2007.

SUCCESSFUL RESOLUTION OF THE PLAN B ISSUE

Often, my office works with other organizations on issues that affect the privacy and access rights of Ontarians. One very successful collaboration came about after I learned that the Canadian Pharmacists Association was advising its members to collect a woman's name and address, along with very sensitive personal health information – including her customary method of birth control – before dispensing the emergency contraceptive pill known as Plan B, a behind-the-counter drug.

Because of my concern that such privacy invasive questions might become a potential barrier to accessing health care, I requested an emergency meeting with the Ontario College of Pharmacists and the Ontario Pharmacists' Association. Both organizations immediately offered to work with my office.

The two meetings that were held with the College and the Association were extremely productive. A working group was formed to develop new guidelines. In less than two weeks from the day I first became aware of this issue, the Ontario College of Pharmacists issued new guidelines to Ontario pharmacists. The guidelines advise pharmacists to "seek information from the patient only as necessary to clarify the appropriateness of providing Plan B, keeping in mind the need to respect the individual's right to remain anonymous and to decline responding to personally sensitive questions." (See the article, *IPC works with the Ontario College of Pharmacists and the Ontario Pharmacists' Association to replace controversial screening form* in the *Issues* section of this annual report.)

SUCCESS OF THE SHORT NOTICES PROGRAM

One of this office's 2005 achievements that I am most proud of was the development of three sets of short and easy-to-understand notices to the public about their rights under *PHIPA*, with one set for each of: health care providers (*Your Health Information and Your Privacy in Our Office*); hospitals (*Your Health Information and Your Privacy in Our Hospital*); and long-term care facilities (*Your Health Information and Your Privacy in Our Facility*).

A working group set up by the IPC – which included the Ontario Bar Association's Privacy Law and Health Law sections, the Ministry of Health and Long-Term Care, and the Ontario Dental Association – took a "multi-layered" approach to privacy notices. The first layer of our *PHIPA* short notices program is a colourful, user-friendly poster written in plain language (which are now posted in hospitals, in the offices of doctors and other health care providers, and in long-term care facilities across Ontario). The second layer for each of the three categories is a concise and easy-to-read brochure with more information. The third layer, for those seeking additional information, is our website.

To the best of our knowledge, this was one of only two projects around the world focusing on short notices for the health sector. And just how successful has it been? We were swamped with requests for copies of both the posters and brochures. In less than seven months – between the roll out of the program in June and the end of December – we mailed out or gave out more than 325,000 posters and brochures.

An unexpected result of this initiative and the role of my office in developing short notices in Ontario was receiving an international privacy award. The IPC was presented with the *Privacy Innovation Award* at the largest-ever gathering of privacy professionals, during the Hewlett-Packard/International Association of Privacy Professionals *Privacy Innovation Awards.* To have my office recognized by privacy professionals for our innovative work was truly gratifying.

SECURE DESTRUCTION OF PERSONAL INFORMATION

Late in 2005, the personal health information of a significant number of people was literally tossed onto the streets of Toronto as part of a film shoot. The producer was simply looking for scrap paper to make the Toronto streets look like those of New York after the 9/11 terrorist attacks. In a strange twist, personal health records, which were to have been shredded, ended up on Toronto streets, for anyone to pick up. After being taken from a Toronto health clinic, those records went through various hands at two companies before ending up on Toronto's streets.

The order I issued, HO-001, following our investigation, was the first order under *PHIPA*. For a summary of the investigation and order, see the *High Profile Privacy Incidents* section. We have also published a fact sheet, the *Secure Destruction of Personal Information*, which is available on our website, **www.ipc.on.ca**, and devoted an article in the *Issues* section of this annual report, *Secure Destruction of Personal Information Records Requires Real In-depth Planning*, to this important topic.

IDENTITY THEFT REVISITED: SECURITY IS NOT ENOUGH

Incidences of identity theft across North America increased exponentially during 2005. In fact, the problem has become so ubiquitous that a prominent American newspaper named 2005 the worst year for information security breaches ever, with at least 130 reported major breaches and close to 60 million affected persons.

Knowledge and awareness are two key weapons in the fight against identity theft. As part of the IPC's mandate to foster public education, we revisited the topic of identity theft. We published our first paper on identity theft in 1997, flagging this issue as one that would explode in the years to come. A new IPC publication, *Identity Theft Revisited: Security is Not Enough*, was released in September, with two accompanying brochures. While our earlier publications on identity theft focused on issues directly affecting consumers, this paper primarily focuses on the role and responsibility of businesses and organizations in preventing and addressing the problem of identity theft.

If data begins leaking out due to a company's negligence, it is consumers who suffer the most, in the form of financial losses, poor credit ratings, not to mention personal frustration. We placed the responsibility for preventing large-scale identity theft squarely upon businesses.

It is imperative that businesses understand that implementing responsible information practices will not only help to combat identity theft but also build consumer confidence, develop a leadership position, reduce the cost of crisis management, and ultimately protect the corporate brand. Failing to do so will leave companies, and consumers, wide open to identity theft and other risks. I urge businesses in Ontario to be proactive – to develop a "culture of privacy" by establishing accountability, identifying vulnerabilities, developing processes, training staff, and evaluating their data protection practices on a regular basis because privacy is good for business.

American legislators have taken considerable action in passing laws on the heels of California's SB-1386, with the requirement that individuals must be notified if their personal information has been compromised. More recently, California also passed SB-1048, the *Identity Theft Protection Act*, which restricts the sale or display of Social Security Numbers, allows victims of identity theft to file complaints with their local police and to clear their name if their personal information has been used in the commission of a crime. On the business side, the Federal Trade Commission's "Disposal Rule" came into effect in June 2005, stipulating that businesses must take reasonable disposal measures so that personal information is rendered permanently destroyed. Subsequently, much has been written about how to provide focused notice, appropriate to the specific breach.

Ontarians deserve the same type of protection. I spent much of 2005 urging the government to implement a made-in-Ontario, private sector privacy law. One of the elements of that law would be a breach notification requirement, another would be a secure destruction requirement. Stay tuned.

UNIVERSITIES UNDER *FIPPA*

Another 2005 highlight came December 12, when Bill 197, *An Act to Implement Budget Measures*, received Royal Assent. A key provision of that bill places universities under the *Freedom of Information and Protection of Privacy Act* – something I have long advocated. That provision came into effect on June 10, 2006.

One of the foundations underlying freedom of information is the principle that organizations that exist by virtue of public funding should be subject to public scrutiny through FOI laws. Therefore, this is an important step. The government should also bring children's aid societies, hospitals, and other publicly funded organizations under FOI legislation.

TORONTO ORDER – MO-1947

In the spring of 2005, the City of Toronto denied four related freedom of information requests from the CBC, which was seeking records showing the number of lawsuits, dates settled, and the costs, from 1998 through 2004, for the finance department, emergency medical services, Toronto fire services and transportation services. The CBC appealed the city's decision to my office.

After a thorough review, I was not persuaded by the city's claim that disclosure of the information sought by the appellant could reasonably be expected to prejudice the economic interests of the city or be injurious to the financial interests of the city. As a result, I issued an order (MO-1947) requiring the city to provide the CBC with the records related to the civil lawsuits involving the four city departments.

The issues in this appeal relate to fundamental principles of FOI. 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.

(For more information about this appeal, see *Building a Culture of Openness in Government* in the *Issues* section.)

PHIPA-PIPEDA SUBSTANTIAL SIMILARITY RULING

In my 2004 annual report, I stated that I was looking forward to a ruling of substantial similarity – that *PHIPA* was substantially similar to the federal *Personal Information Protection and Electronic Documents Act (PIPEDA)*, which would mean that Ontario health information custodians covered by *PHIPA* would not also be subject to the federal *PIPEDA*. My office worked very hard towards this goal and I am pleased to report that the Governor General in Council issued an Order on November 28, 2005, exempting health information custodians subject to Ontario's *PHIPA* from the application of Part 1 of *PIPEDA*, in respect of the collection, use and disclosure of personal information within Ontario. Excellent news for Ontario.

IPC *PHIPA* TRAINING VIDEO

I have always been a strong proponent of the IPC's public education programs, which is why – in the spring of 2005 – I commissioned the production of an informational training video on *PHIPA*, for the use of Ontario's health care providers.

Entitled, *The Personal Health Information Protection Act: A video guide for training and education*, the video presents four scenarios which demonstrate both the wrong and the right way – under *PHIPA* – for health care staff to deal with personal health information. The first scenario takes place in a pharmacy and deals with acoustic privacy; the second looks at written communication (a referral letter from a surgeon's office to a community care access corporation). The third deals with the theft of a laptop computer containing patient records from a doctor's office, while the fourth scenario deals with an ambulance service trying to collect survey information.

You can obtain a copy of the video through the IPC. (Call 1-800-387-0073 and ask for the Communications Department.)

MY PERSONAL THANKS

I would like to give my sincere thanks to all of the staff in my office. While I thought that 2004 had been one of the most demanding years that my office has ever faced, 2005 proved to be far more challenging. I am genuinely touched by the passion and enthusiasm that my staff has shown. I truly believe that the people of Ontario are very fortunate to have such talented and dedicated people working on their behalf, for open government, and for the protection of their privacy. I truly have the best team! My heartfelt thanks to you, as always.

secure destruction of personal information records requires in-depth planning

On Saturday, October 1, Information and Privacy Commissioner Ann Cavoukian learned via a phone call at her home that personal health records had been strewn across several streets in downtown Toronto as the backdrop for a film shoot. The production company, filming a miniseries that was set in New York right after 9-11, wanted Toronto streets to resemble debris-filled New York streets after the attack on New York's twin towers.

The Commissioner, after personally visiting the site that Saturday because of the potentially devastating impact on patient privacy, ordered an immediate investigation into the incident; an investigation that determined documents containing personal health information had not been securely handled or properly disposed of. This resulted in the Commissioner's first order (HO-001) under the *Personal Health Information Protection Act, 2004* (*PHIPA*).

Ontario's three privacy laws, covering provincial and municipal government organizations and health information custodians – as well as federal legislation covering private sector organizations – require that personal information be disposed of in a secure manner, whether the information is in paper or electronic format.[1] While the incident at the movie set involved personal health information records, it could just as easily have been any other type of personal information, including financial records.

The Commissioner has cited this privacy breach as an example of the importance of ensuring the secure destruction of personal information in any media, by all types of organizations, whether done in-house or contracted out to a third party (as was the case with the Toronto health records).

After tracing what went wrong in the movie set incident, the IPC has collected and produced best practices for the secure destruction of records containing personal information.

BEST PRACTICES

Records containing personal information must be permanently destroyed or erased in an irreversible manner that ensures that the record cannot be reconstructed in any way. Consider not only the "official" files but any duplicate copies of documents made for in-office use (documents could carry "shred after" dates or "do not copy" warnings).

For paper records, use cross-cut shredding, not simply continuous (single strip) shredding, which can be reconstructed. In fact, it is technically possible (though extremely difficult) to reconstruct even cross-cut shredded documents, so consider going further for highly sensitive records and ensuring that pulverization or incineration of the records takes place. Consider also whether on-site or off-site destruction is more suitable for your organization.

1 *The Personal Health Information Protection Act, 2004* requires health information custodians to protect personal health information in their custody or control and to ensure that records are retained, transferred and disposed of in a secure manner (see sections 12 and 13). Section 2 of Regulation 459 under the *Freedom of Information and Protection of Privacy Act* permits provincial institutions to dispose of personal information in only one of two ways: either by transferring it to the Archives or by destroying it. If the institution destroys the personal information, then the head of the institution must take all reasonable steps to ensure that it is destroyed in such a way that it cannot be reconstructed or retrieved (see section 5 of the Regulation). Municipal institutions under the *Municipal Freedom of Information and Protection of Privacy Act* are encouraged to follow the same rules. Private sector organizations in Ontario are subject to the federal *Personal Information Protection and Electronic Documents Act (PIPEDA)*, including the 10 fair information principles of Schedule 1. For example, clause 4.5.3 of Schedule 1 requires organizations to develop guidelines and implement procedures governing the destruction of personal information, and clause 4.7.5 requires care to be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information.

For electronic and wireless media such as floppy disks, CDs, USB keys, personal digital assistants and hard drives, destruction means either physically damaging the item (rendering it unusable) and discarding it, or, if reuse within the organization is preferred, it means employing wiping utilities provided by various software companies. Keep in mind, however, that electronic wiping may not irreversibly erase every bit of data on a drive.

SELECT YOUR SERVICE PROVIDER CAREFULLY

If you are engaging an external business to destroy records, be selective. Look for a provider accredited by an industrial trade association, such as the National Association for Information Destruction, or willing to commit to upholding its principles, including undergoing independent audits. Check references and insist on a signed contract spelling out the terms of the relationship. The contract should:

- set out the responsibility of the service provider for the secure destruction of the records involved;
- specify how the destruction will be accomplished, under what conditions and by whom;
- require that a certificate of destruction be issued upon completion, including the date, time, location, and method of destruction and the signature of the operator (while a certificate itself cannot prove that destruction has actually occurred, its existence, along with the written service contract, documented reference-checking, accreditation, etc., demonstrates that you have taken reasonable steps to ensure that secure destruction has taken place);
- include a provision that would allow you to witness the destruction, wherever it occurs, and to visit the service provider's facility;
- state that employees must be trained in and understand the importance of secure destruction of personal information;
- require that if any of the work is subcontracted to a third party, the service provider must notify you ahead of time, and have a written contractual agreement with the third party, consistent with the service provider's obligations to you;
- specify a time within which records collected from you will be destroyed, and require secure storage pending such destruction.

In short, take responsibility. Don't assume that once tossed into a garbage can, blue bin, electronic recycle bin, or even a shredder, that documents and the information they carry are gone forever. Be vigilant.

For more information, see the IPC fact sheet, *Secure Destruction of Personal Information*, available on the IPC's website, **http://ipc.on.ca/docs/fact-10-e.pdf**.

building a culture of openness in government

In Ontario, open and transparent government is hinged largely on freedom of information legislation, which has been in effect for almost 20 years. Although there are other laws and mechanisms which provide for public accountability, the right of citizens to access government-held information remains a key instrument for holding elected and appointed officials accountable to the people they serve.

The fundamental principles underlying both the *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act* include the notions that information should be available to the public and that necessary exemptions from the right of access should be limited and specific. In other words, there is a presumption that citizens have a right to access government-held information, and that any exemptions claimed by government should only be applied in narrow circumstances.

During the past two decades, a culture of openness in government, both at the provincial and municipal level, has been slowly evolving. There is no doubt that government today is significantly more open and transparent than it was 20 years ago. However, a protective and risk adverse mindset still prevails in some government bodies. In appeals that come before the IPC, some government organizations apply both discretionary and mandatory exemptions in a broad and liberal manner rather than giving them a limited and specific interpretation.

In July 2005, Commissioner Ann Cavoukian issued an order (MO-1947) that attracted significant media coverage because it highlighted and reminded government organizations of the key principles that are necessary to building a culture of openness in government. The requester, CBC Radio-Canada, filed four access to information requests with the City of Toronto under the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*), seeking access to all records regarding civil lawsuits involving four city departments that the city had settled with third parties from 1998 to 2004. The records sought dealt with information about the number of lawsuits, dates settled and dollar amounts.

The city denied access, citing the exemptions in sections 11(c) and (d) of the *Act*. Section 11(c) allows a government organization to refuse disclosure of a record that contains information whose disclosure could reasonably be expected to prejudice the economic interests of the government organization or its competitive position. Section 11(d) allows a government organization to refuse disclosure of a record that contains information whose disclosure could reasonably be expected to be injurious to the financial interests of the government organization.

CBC Radio-Canada appealed the city's decision to the IPC. In responding to the appeal, the city submitted it was reasonably likely to face financial and economic harms if the information at issue was disclosed. The city took the position that the number of claims made against the city was reasonably likely to increase and, as a result, insurance premiums were reasonably likely to increase or the city might lose its insurance coverage.

At the outset of her order, the Commissioner cited Dagg v. Canada (Minister of Finance) [1997], 2 S.C.R. 403, where Mr. Justice La Forest of the Supreme Court of Canada considered the purpose of the federal *Access to Information Act* (*ATIA*) but also commented on the important role that freedom of information legislation plays more generally in Canada:

> "The overarching purpose of access to information legislation … is to facilitate democracy. It does so in two related ways. It helps to ensure first, that citizens have the information required to participate meaningfully in the democratic process and secondly, that politicians and bureaucrats remain accountable to the citizenry ....
>
> Parliament and the public cannot hope to call the government to account without an adequate knowledge of what is going on; nor can they hope to participate in the decision-making process and contribute their talents to the formation of policy and legislation if that process is hidden from view. Access laws operate on the premise that politically relevant information should be distributed as widely as possible ….
>
> Rights to state-held information are designed to improve the workings of government; to make it more effective, responsive and accountable. Consequently, while the *ATIA* recognizes a broad right of access ... it is important to have regard to the overarching purposes of the *Act* in determining whether an exemption to that general right should be granted."

The Commissioner found that the city had not adduced any fact-based evidence to support its assertion that the release of claims information often sparks widespread public debate and discussion as to when a person may commence an action against the city, which, in turn, often leads to a sudden rise in claims. Given this, it did not logically follow that its insurer would demand increased premiums or that the city would lose its insurance coverage altogether.

The Commissioner concluded that the city had not discharged the burden of proving that the records at issue fall within the exemptions in sections 11(c) or (d) of the *Act*. The evidence adduced by the city amounted to speculation about possible harm, which was insufficient to meet the requirements of sections 11(c) or (d). Consequently, she ordered that the records at issue be disclosed to the appellant.

In support of her decision, the Commissioner emphasized the importance of the disclosure of this type of information:

> "…citizens cannot participate meaningfully in the democratic process and hold politicians and bureaucrats accountable unless they have access to information held by government, subject only to necessary exemptions that are limited and specific. Ultimately, taxpayers are responsible for footing the bill for any lawsuits that the city settles with litigants or loses in the courts. Consequently, taxpayers have a right to know, at a minimum, how many lawsuits or claims have been filed against the city, and how much money the city has paid out in damages or in settling such matters in specific years."

At the end of her order, the Commissioner stated that she was pleased that Toronto Mayor David Miller was committed to open and transparent government and urged him to ensure that there is a shift in the city bureaucracy from a protective mindset to a culture of openness.

> "This culture shift should be based on the principles that information should be available to the public, and that necessary exemptions from the right of access should be limited and specific. Exemptions should not simply be claimed because they are technically available in the *Act*; they should only be claimed if they genuinely apply to the information at issue."

Within hours of the release of Commissioner Cavoukian's order, the city disclosed the records at issue to the appellant. In addition, Mayor Miller stated publicly that he was pleased with the order and told reporters he was continuing to take steps to change the prevailing culture within the city bureaucracy.

Although this order was directed at one institution, the City of Toronto, it contains important messages about the importance of building a culture of openness that should be reviewed by both provincial and municipal institutions in Ontario. A key message is that leadership on openness and transparency must come from the top. Public servants are more apt to disclose information without claiming inapplicable exemptions if they feel that their decisions will be supported by both the politicians and senior executives who lead their ministry, agency, board, commission or local government.

IPC works with the Ontario College of Pharmacists and the Ontario Pharmacists' Association to replace controversial screening form

Within days of a controversy erupting in the media over the screening of women attempting to access the emergency contraceptive pill, commonly known as Plan B, the Ontario College of Pharmacists, after being approached by Commissioner Ann Cavoukian, issued new guidelines for pharmacists operating in the province of Ontario. The new guidelines were issued in record time through a highly successful collaboration between the Ontario College of Pharmacists, the Ontario Pharmacists' Association and the IPC.

On December 2, the *Canadian Medical Association Journal* and the *Toronto Star* both reported that the Canadian Pharmacists Association was advising its members to collect and record a woman's name and address, along with sensitive personal health information, including the date of her last menstrual period, when she last had unprotected sex, and her customary method of birth control, before providing Plan B (levonorgestrel 0.75 mg.).

The Commissioner requested an emergency meeting with the Ontario College of Pharmacists and the Ontario Pharmacists' Association to resolve the privacy issues that this proposed practice raised. Both organizations were readily available to work with the IPC and immediately committed to resolving the controversy as quickly as possible.

The emergency contraceptive pill had recently been removed from Health Canada's list of prescription drugs, enabling pharmacists to provide this drug to individuals without a prescription. Plan B has been designated as a behind-the-counter drug, requiring pharmacist intervention. Although the Ontario College of Pharmacists assured the IPC that, in accordance with their professional standards of practice, pharmacists do not routinely collect personal health information when providing behind-the-counter drugs, voluntary guidelines issued by the Canadian Pharmacists Association recommended that pharmacists routinely collect personal health information, some of it extremely sensitive, prior to providing Plan B. This recommended practice, which was unique to the provision of Plan B, raised alarms among women's organizations and privacy experts who were concerned that the collection of sensitive personal health information could deter some women from accessing the drug.

After two meetings with the Commissioner and the Ontario Pharmacists' Association, the Ontario College of Pharmacists issued a notice December 8 advising pharmacists operating in Ontario not to use the "Screening Form for Emergency Contraceptive Pills" issued by the Canadian Pharmacists Association. Pharmacists were advised not to use this form as its use would result in the routine collection of identifiable health information that would, in virtually all cases, not be necessary for the provision of Plan B. Under the *Personal Health Information Protection Act* (*PHIPA*), pharmacists and other health information custodians are not permitted to collect personal health information if other information will serve the purpose, and are not permitted to collect more personal health information than is reasonably necessary to meet the purpose of the collection. To ensure compliance with the limitations on the collection of personal health information set out in the legislation, Ontario pharmacists were advised to follow the new made-in-Ontario guidelines that would soon be issued by the College.

In working with the Ontario College of Pharmacists and Ontario Pharmacists' Association to develop the new guidelines, the Commissioner acknowledged the important services provided by pharmacists and recognized that the new guidelines would have to fit within both the existing professional standards of practice for pharmacists operating in the province and the requirements of *PHIPA*.

New guidelines for pharmacists operating in Ontario were issued by the Ontario College of Pharmacists on December 15. In the new guidelines, the College advises pharmacists to "seek information from the patient only as necessary to clarify the appropriateness of providing Plan B, keeping in mind the need to respect the individual's right to remain anonymous and to decline responding to personally sensitive questions." Moreover, the guidelines advise that "in the case of Plan B, personally identifiable information should not be recorded except when requested by the patient for reimbursement purposes or in those rare instances where it is deemed important for continuity of care of the patient."

Ontario's new guidelines for pharmacists providing Plan B are available from the Ontario College of Pharmacists (**www.ocpinfo.com**). The Commissioner is grateful to both the Ontario College of Pharmacists and the Ontario Pharmacists' Association for their invaluable support and co-operation.

disclosure of information in emergency or other urgent circumstances

In July 2004, a newspaper in British Columbia reported that a university student, who had suffered from depression, committed suicide one month after being hospitalized for a prior suicide attempt. Neither the hospital nor the university, which had both been aware of the prior suicide attempt, notified the student's mother of that suicide attempt, prior to the student's death. The hospital and university stated that privacy laws, in particular British Columbia's *Freedom of Information and Protection of Privacy Act*, prevented the mother from being notified.

In August 2005, a newspaper in Ontario reported that a daughter, who had been frantically searching for her 86-year-old father, was not informed by a hospital that her father had been admitted following injuries suffered in a car accident. The hospital cited Ontario's *Personal Health Information Protection Act* as the reason for its failure to inform the daughter.

Privacy is often cited as the reason when there is a failure to share information in emergency or other urgent circumstances. It is often used as a shield to minimize disclosure, regardless of how inappropriate that may be.

Given examples such as these, Ontario's Information and Privacy Commissioner felt it important to emphasize that while access and privacy laws underline the importance of protecting the privacy of individuals, they also recognize that in certain circumstances, privacy should not be an impediment to the sharing of vital – and, in some cases, life-saving – information, even in the absence of consent.

The *Freedom of Information and Protection of Privacy Act* (*FIPPA*), the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*) and the *Personal Health Information Protection Act* (*PHIPA*) do not prevent, and in fact permit or even require, the sharing of information, including personal information and personal health information, in emergency or other urgent circumstances. Further, *FIPPA* and *MFIPPA* protect heads of provincial and municipal institutions, and *PHIPA* protects health information custodians, from any liability that may arise from the sharing of such information, provided they acted in good faith.

DISCLOSURES IN THE INTERESTS OF HEALTH AND SAFETY

FIPPA and *MFIPPA* require heads of provincial and municipal institutions to disclose a record as soon as is practicable, subject to the provision of notice to the person(s) to whom the information in the record relates, where feasible, if there are reasonable and probable grounds to believe that the disclosure is in the public interest and that the record reveals a grave environmental, health or safety hazard to the public.

FIPPA and *MFIPPA* also permit heads of provincial and municipal institutions to disclose personal information without consent in compelling circumstances affecting the health or safety of an individual if, upon disclosure, notification is provided to the individual to whom the information relates.

Similarly, *PHIPA* permits health information custodians to disclose personal health information without consent, and even despite an express instruction to the contrary by the individual to whom the personal health information

relates, where there are reasonable grounds to believe the disclosure is necessary to eliminate or reduce a significant risk of serious bodily harm to a person or group of persons.

PHIPA also permits health information custodians to disclose personal health information without consent to certain other health information custodians, whose core function is the provision of health care, if the disclosure is reasonably necessary for the provision of health care and if it is not reasonably possible to obtain consent in a timely manner, unless the individual has expressly instructed the health information custodian not to make the disclosure.

DISCLOSURES TO NEXT OF KIN IN COMPASSIONATE CIRCUMSTANCES

The two public sector *Acts*, *FIPPA* and *MFIPPA*, permit heads of provincial and municipal institutions to disclose personal information without consent in compassionate circumstances in order to facilitate contact with next of kin or a friend where an individual is injured, ill or deceased.

Likewise, *PHIPA* permits a health information custodian to disclose personal health information for the purpose of contacting a relative, friend or potential substitute decision-maker if an individual is injured, incapacitated or ill and unable to give consent personally. *PHIPA* also contains a number of provisions that permit a health information custodian, without consent, to disclose personal health information relating to an individual who is deceased, or is reasonably suspected to be deceased, including:

- for the purpose of identifying the individual;
- for the purpose of informing any person it is reasonable to inform that the individual is deceased or reasonably suspected to be deceased and the circumstances of death; and
- to enable a spouse, partner, sibling or child of the individual to make decisions about their healthcare or that of their children.

DISCLOSURES TO PUBLIC HEALTH AUTHORITIES

The outbreak of Severe Acute Respiratory Syndrome (SARS) in 2003 highlighted the importance of public health authorities having timely access to personal health information.

As stated in the SARS Commission Second Interim Report, entitled, *SARS and Public Health Legislation*, "privacy, an important value, cannot be allowed to stand in the way of necessary reporting that is required by law to protect the public against infectious disease. Privacy legislation was never intended to impede the flow of vital health information mandated by the *Health Protection and Promotion Act*."

PHIPA authorizes health information custodians to disclose personal health information without consent where permitted or required by law. Because the *Health Protection and Promotion Act* requires certain health information custodians, such as hospital administrators, superintendents of psychiatric facilities, laboratory operators and certain health care practitioners, to report reportable, communicable or virulent diseases to a Medical Officer of Health, such disclosures are similarly authorized by *PHIPA*.

In addition, *PHIPA* also permits a health information custodian to disclose personal health information without consent to a Medical Officer of Health or to the Chief Medical Officer of Health for Ontario if the disclosure is made for a purpose of the *Health Protection and Promotion Act*. The purpose of that *Act*, as set out in section 2 of the *Act*, is to provide for the prevention of the spread of disease and the promotion and protection of the health of the people of Ontario.

PHIPA also permits a health information custodian to disclose personal health information without consent to a similar public health authority in another jurisdiction if the disclosure is made for a purpose substantially similar to a purpose of the *Health Protection and Promotion Act*.

The IPC developed an easily accessible fact sheet, *Disclosure of Information Permitted in Emergency or Other Urgent Circumstances*, to provide assistance and clarification regarding these matters. For further information about the sharing of information in emergency or compassionate circumstances, please consult the IPC fact sheet, which is available in the *PHIPA* section of the IPC's website, **www.ipc.on.ca**.

police retention of fingerprints, photos and criminal history records

Police collect, use, retain, and disclose some of the most sensitive personal information. For example, in investigating allegations of criminal wrongdoing, police collect information about the activities and personal lives of complainants, witnesses, and accused persons.

As an investigation proceeds, police may decide to lay criminal charges. This is a preliminary determination; it is not a legal judgment of guilt. An accused person's name and description is filed with a recital of the charges he or she faces. Photographs and fingerprints are taken and filed alongside the charges. Irrespective of whether the individual is innocent or guilty, at this point, he or she is profiled in a highly sensitive police record.

CRIMINAL RECORDS

A police record is not a criminal record, however. Individuals charged with an offence do not have a criminal record; the law presumes each person innocent until proven guilty. In Canada, criminal records are only created after a person has been convicted in a court of law.

An adult convicted of a criminal offence has a criminal record for the rest of his or her life, unless later pardoned. In many circumstances, a pardon allows someone who was convicted of a crime the opportunity to apply for work or volunteer positions without the shadow of a criminal record barring the way.

POLICE RECORDS CHECKS AND NON-CONVICTION DISPOSITIONS

What happens to the highly sensitive police records of those individuals who are charged but never convicted?

Many people assume that when charges are dropped, stayed, withdrawn, or a finding of "not guilty" is made, the name of the accused person is automatically cleared. However, while these and other non-conviction dispositions leave a person without a criminal record, police services in Ontario retain most police records in perpetuity, even where a person is found not guilty by the courts.

Some legally innocent individuals only learn that police maintain a police record on them after they agree to an employer or volunteer organization's request that they submit to a police records check. Police would conduct a search of a federal database containing criminal records as well as of other police databases containing a broad range of police records and files. Both the organization and the individual are informed if there are any records linked to the individual. Only the individual is to be given the details.

While the Ontario Human Rights Code provides some protections from employment discrimination against individuals in possession of a pardon, many legally innocent people faced with having to explain a defunct charge simply withdraw themselves from work competitions. Others attempt to persuade a now skeptical employer or organization that the charges were baseless. Having faced the scrutiny of the justice system and received a non-conviction disposition, they may have assumed that they would continue to enjoy the protection of the right to the presumption of innocence. Instead, many find themselves excluded from vital opportunities essential to a law-abiding citizen's social and economic life.

THE RIGHT TO REQUEST DESTRUCTION OF A POLICE RECORD

In a 2002 case that addressed privacy rights under the *Charter of Rights and Freedoms (R. v. Dore [2002] O.J. No. 2845)*, the Ontario Court of Appeal ruled that legally innocent individuals have a right to request that their *police records* be destroyed or expunged. In doing so, the Court articulated a constitutional principle requiring that, absent compelling and unusual circumstances, police accede to an *expungement* request and destroy the *police records* of legally innocent people.

As is often the case, the challenge is to ensure that legal rights are accessible to those who need and warrant their protections. To date, the courts have encouraged but not required police to provide accused people with information about police policies regarding the use, disclosure, and retention of *police records.* Across Ontario, it does not appear to be routine police practice to do so. Instead, some police officials have suggested that legally innocent people will likely know about their right to request *expungement* of these records or that judges and defence counsel should provide the relevant information.

Many accused, however, do not know their rights. Many do not have legal counsel. And many receive *non-conviction dispositions* from justice system officials other than a judge. This can result in the police having a dual role since police services are also the institution responsible for the collection, use, disclosure, and retention of the sensitive information involved.

It is in this context that the Information and Privacy Commissioner has been working with the policing community to ensure that *expungement* policies and procedures are transparent, accountable and fair. In this endeavour, the Commissioner has been guided by internationally recognized fair information practices, as well as by fundamental privacy principles. Those principles and practices require that policing institutions respect the privacy rights of legally innocent persons by both appropriately limiting the use, disclosure, and retention of their personal information and by notifying them of their rights to access, challenge, and expunge the relevant *police records.*

THE COMMISSIONER'S RECOMMENDATIONS

The Commissioner has developed recommendations on four critical issues:

Issue 1: Notification – Upon arrest, police should notify an accused person in writing of his or her right to seek *expungement* of the individual's *police record* following a *non-conviction disposition.* Once an individual receives a final *non-conviction disposition*, he or she should receive a second written notice regarding the right to seek *expungement.* An adequate notice should include the contact information of the specific office responsible for processing the request and additional information about the *expungement* process. Both of these notice requirements can be built into the regular routine for efficiency.

Issue 2: Fees – No fees should be charged for processing an *expungement* request. Subjecting legally innocent individuals to a fee in order to clear their name compromises the presumption of innocence that is fundamental to our justice system and may constitute an unfair barrier to the exercise of this right in the case of unemployed or low-income individuals.

Issue 3: Criteria – Police should develop objective and fair criteria and timely procedures to handle requests for the destruction of fingerprints, photographs and other police records from individuals who receive a non-conviction disposition. In particular, policies and guidelines should provide that the exceptional decision to refuse a destruction request should only be made where the police have reasonable grounds to believe that the individual has committed, or will commit, a serious offence, such as a "serious personal injury offence" (as defined in section 752 of the *Criminal Code of Canada*). Such an approach would allow police to retain some criminal history records, but

only where objective evidence satisfies appropriately focused criteria. Moreover, the right to apply for the *expungement* of *police records* should not be subject to undue or arbitrary delay. Rather, individuals in receipt of a final *non-conviction disposition* should be entitled to apply immediately and their applications should be processed without undue delay.

Issue 4: Right of Appeal – Individuals should have a right to appeal police refusals to *expunge* to an accessible and independent body. This cannot be left informally to police institutions. This is because police institutions appropriately place considerable emphasis on fighting crime and providing for public safety, so independent balance is difficult to achieve in an appeal. Independent adjudication is required to ensure that privacy rights and the presumption of innocence are accorded adequate weight when evaluating an expungment request. While some individuals may be able to go to court to challenge a police refusal to expunge, in many cases, the cost of going to court will act as an insurmountable barrier.

THE ONGOING WORK OF THE COMMISSIONER

In January 2005, the Commissioner appeared before the Toronto Police Services Board to express her concerns about proposed changes to the police service's *expungement* policies and procedures. The proposal would have required that legally innocent individuals pay a $50 fee to apply to have their *police records* destroyed. (There were no fees charged previously.) The proposal would also have allowed the police to refuse *expungement* requests routinely rather than on an exceptional basis. In effect, police would be empowered to retain the records of all those who received any *non-conviction disposition* in respect of any sexual, firearms, weapons, explosives or violence-related **charges**.

Since that time, the Commissioner and her staff have met with representatives from the Toronto Police Service, the Toronto Police Services Board, the Ontario Association of Chiefs of Police, and RCMP officials from the Canadian Criminal Records Information Services.

Ongoing discussions with the Toronto Police Services Board have led to the Board's decision to declare that those acquitted of an offence will have a right to expungement regardless of the nature of the charge and that no fees will be charged for processing any *expungement* application. The police service and board have struck a working group, which is considering the Commissioner's outstanding concerns.

A fair expungement process must take into account both the legitimate interest of law enforcement and the fundamental rights of legally innocent citizens. The Commissioner is continuing to work with the police towards achieving a fair and balanced solution.

pivotal privacy issues that must be considered as health record systems are developed

Information technology is making clear inroads in the Ontario health care system. Pilot projects are underway to share diagnostic images such as x-rays and ultrasounds online, with the expectation of reducing duplicated tests, wait times, and improving outcomes. Prescription drug claims histories of Ontario recipients of the Ontario Drug Benefit Program and the Trillium Drug Program are available to most hospital emergency departments for reference when a patient enrolled in these programs seeks medical help. Although there are many initiatives such as these that involve partial electronic medical records, a fully interoperable electronic health record that enables a patient's key health history to be available when needed to providers throughout the province remains on the horizon, not quite yet reached.

Individuals who have family doctors will be familiar with the "chart" concept. With each visit to the doctor, information is generated and recorded in the patient's chart. Over time, the information collected can be voluminous. This detailed local clinical information, if recorded in an electronic format, is often known as the *electronic **medical** record* (EMR). While this information may be important to the primary care provider, it may not all be relevant in the context of other encounters with the health care system.

The *electronic **health** record* (EHR), however, is intended to contain only the key, pertinent elements of clinical information from all health care providers used by the patient. Prescription drugs, drug allergies, chronic conditions, results of tests, and past surgeries are good examples. EHRs, available to medical personnel throughout a jurisdiction (hence the term "interoperable"), are intended to improve efficiency, reduce duplication of tests, decrease adverse drug interactions and, overall, improve patient care and outcomes.

In public opinion polls, Canadians have indicated support for the development of EHRs but have signalled concerns about privacy and the security of personal health information in a cyberspace environment.[1] The IPC is working hard to help ensure that in moving toward an interoperable EHR in Ontario, patient privacy and information security remain a high priority.

Since the introduction of the *Personal Health Information Protection Act, 2004* (*PHIPA*), the IPC's mandate has included oversight of the collection, use and disclosure of personal health information within the Ontario health care system. The object is to keep personal health information confidential and secure, while allowing for the effective delivery of health care services. The IPC is charged with overseeing the legislation by responding to or initiating complaints about the information practices of health information custodians as well as by conducting public education programs, providing information and conducting research related to *PHIPA*.

Part of this work includes involving the IPC in a wide variety of consultations with numerous organizations working in Ontario on existing or proposed EHR projects. The IPC strongly believes that it is better, easier – and often less expensive – to build privacy protections into the design of new systems rather than add them after, during a retrofit of existing systems.

1 Ekos, *Pan-Canadian Health Information Privacy and Confidentiality Framework Final Report*. November 2004.

In order to build privacy protections into EHRs (or any electronic exchange of personal health information) from the start, some key questions should be addressed. Questions such as those below arise when fair information practices are applied in the context of the EHR. They are the kinds of questions which the IPC frequently raises with organizations working on EHRs.

- Who will be responsible for the compilation, accuracy and overall security of the EHR system in Ontario? As disparate projects proliferate, this question becomes increasingly urgent.
- How, and by whom, will patients be informed about the existence and functions of the EHR, and about the measures in place to protect their privacy?
- How will **patient consent** be managed, particularly when integrating older systems not designed with consent in mind? These systems may not have been designed to accommodate individuals' preferences with respect to the collection, use and disclosure of their own personal health information.
- Who has access to what information, and for what purposes? How can access be arranged so that only those who need access have it, and even then, only to the information needed? Under what circumstances can information be shared, added to, or deleted?
- What safeguards will be in place to reduce the risk of inappropriate access or use of the information?
- How will patients be able to access their own EHR and request correction of any of the contents?
- How, and by whom, will complaints from patients about information practices surrounding their EHR be handled?

Through the IPC's relationships with various stakeholders, the IPC has been tracking and monitoring EHR developments across the country and, at every opportunity, providing input. For example, the IPC was involved in a national consultation on a privacy and security "architecture" for electronic health records, co-ordinated by Canada Health Infoway. At the provincial level, the IPC has worked with groups co-ordinating electronic information-sharing approaches for laboratory and diagnostic imaging information as well as emergency department access to drug information, to name just a few of the many projects reviewed.

Being uniquely positioned to observe and comment on EHR developments, the IPC has identified a need for strong leadership and accountability in this area. It is important to ensure that public consultation, as well as co-ordination of the various EHR efforts, ultimately occur, along with a continued respect for the privacy of all patients, and the security of their personal health information.

RFID privacy misconceptions: questions answered

The public debate has really just begun about the uses of Radio Frequency Identification (RFID) technologies and their impact on personal privacy. Already, this debate has been skewed by rumours and misinformation. This article reviews some of the common misconceptions.

Radio Frequency Identification (RFID) technology has been around for more than two generations, but the feasibility of commercial uses is just now beginning to emerge. There are virtually unlimited applications in addition to the tracking of inventory in the supply chain management process. These include: validating the authenticity of pharmaceuticals, authorizing access to locked doorways and car ignitions, automating payments on toll roads and at gas stations, and, recording the start, intermediate and finish times of 40,000 marathoners. These are just the first few applications, which signal rapid new developments.

Certain uses of the technology have given rise to questions about its potential impact on privacy, including concerns about possible unintentional consequences.

The IPC has always taken a keen interest in the effects of new technologies on privacy. For more than a decade, the IPC has advocated for more informed public discussion on the topic, the need to "build privacy in" the respective technology involved during the early design stages of development, and for government and private organizations to remain open and accountable for their technological practices. Indeed, technology need not be privacy-invasive; it can be the reverse – privacy-enhancing. The difference is often a matter of better understanding the facts about a given technology and thinking clearly about the problem and possible solutions. In order for this to happen, public debate and discussion must be informed and, by necessity, grounded in facts, not misconceptions.

***Misconception*: Companies that sell RFID-tagged merchandise items will automatically use the technology to spy on, to profile, and to discriminate among their customers**

- Companies that deploy RFID-tagged items will do so primarily to track products for explicit business purposes, such as inventory and supply-chain management.
- The kind of data that is normally on these tags is a numerical string similar to barcodes. Virtually all retail RFID tags are passive tags that contain only tracking information for the product.
- If, at any time, RFID tag information would be associated with an identifiable individual, then its collection, use and disclosure would immediately become subject to the applicable laws and regulations, which prescribe, among other things, strong consumer rights such as notice, access and redress.

***Misconception*: RFID-tagged items carried or owned by individuals will be read by other, unknown entities**

- Although one may read of various doomsday scenarios, from satellite tracking of chips to burglars taking inventories of the assets in homes, the fact is that RFID technology does not have that level of sophistication and capability, nor is it likely to do so for quite some time.
- It is possible that RFID tags could yield their information to anyone who asks, and could be susceptible to "eavesdropping" or "leakage." This is a privacy-invasive possibility that has received a great deal of publicity. However, the likelihood of this occurring is quite low. This scenario assumes

that: (a) RFID readers are ubiquitous and capable of not just reading the tag but making sense of its contents; (b) these readers are networked together; (c) the information collected by these readers is used for nefarious purposes, (d) RFID tags will be left on merchandise rather than removed; and (e) no law, regulation or policy will apply to the collection, use and disclosure of RFID tags data. Yes, these conditions may be theoretically possible, but they are not probable. The risks are very low, and will be more than offset by the benefits offered.

- Personal information is not typically stored on RFID tags. Assuming that someone could read the data on your employee door access card, car key or keychain gas payment card, it's not clear what would be done with it, other than clone it or build a pseudonymous transaction profile, both of which can be defeated using security measures.
- For most RFID tags, especially passive tags, the reader must be within arm's length to read the tag – and this must be done under optimal conditions in order to be successful. Tags that can be read from further away, such as car transponders, typically have their own power-source, enlarging them to the size of chalkboard erasers and increasing per-unit costs substantially. It is true, however, that read ranges can be enhanced by intercepting the data when transmitted to a legitimate reader, but this is a different problem than having one's belongings casually scanned or read.
- There are simple and effective technical solutions to protect privacy, the most obvious one being to kill or disable tags at the point of sale. Other privacy-enhanced solutions involve shielding the tag or encrypting the data with a password.
- The bottom line: There are known privacy and security issues associated with RFID tag data being read by unauthorized readers for unauthorized purposes. In the retail/commercial arena, however, these fears are greatly exaggerated and assume a near-impossible confluence of optimal conditions.

***Misconception*: RFIDs are a low-level privacy issue**

- Actually, it is just the opposite. A wide range of well-known and respected consumer, privacy and civil liberties organizations have been constructively engaged in RFID privacy issues for several years. Groups like the Centre for Democracy and Technology, Electronic Privacy Information Center, Privacy Rights Clearinghouse, the American Civil Liberties Union and the Electronic Frontier Foundation have been active on many fronts, from collecting and publishing public information to testifying before legislative committees.
- Data Protection Commissioners and public regulatory agencies have also been engaged in RFID privacy issues for some time, carrying out public research and education activities, holding public hearings and workshops, working with stakeholders and offering advice, guidance and constructive solutions to common RFID privacy concerns.
- The IPC is also working with the RFID industry, associations and stakeholders to help develop privacy-enhanced solutions and to develop credible governance structures for RFID applications.
- Conclusion: There is considerable interest and engagement in RFID privacy issues taking place across the entire spectrum of society. Different stakeholders will necessarily have different views and positions, but for the most part, they are reacting to a perceived lack of strong and open governance models to ensure that RFID technologies are deployed responsibly and in an accountable manner.

Misconception: **Consumers will acquiesce to RFID roll outs simply because of some form of rewards**

- Reality: Consumers will resist RFID roll outs if they have reason to suspect any misuse and abuse of their personal information. There is nothing inevitable about customer acceptance.
- Published opinion studies and available evidence suggest that the vast majority of consumers are still unaware of, or do not understand, RFID technologies. Their views – and ultimately, consumer and marketplace acceptance of RFIDs – will be shaped in large part by their own evolving knowledge and understanding, by their experiences with it over time, and by the degree of trust they place in the organizations that would have them accept it.
- Companies, for their part, need to be proactive and defuse potential criticisms and fears by adopting and abiding by clear, strong and open information policies and practices.
- Companies need to avoid RFID practices that even appear to be questionable, such as surreptitious trials, unaccountable "uses" or "effects" of RFID data on consumers.
- Companies need to build privacy and security into the design and operation of their RFID information systems, and tell their customers exactly what they have done and what they are doing.

Commissioner's recommendations

In addition to the recommendations included in the *Commissioner's Message* and the *Issues* section, where particular subjects are explored in depth, there is an overarching step that I am recommending every provincial and municipal government organization in Ontario take, and another that I am recommending every health information custodian take.

HOLDING GOVERNMENT ACCOUNTABLE

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 is particularly true for details of government expenditures and the right of the public to scrutinize how tax money is being spent. When government organizations use individuals or companies in the private sector to help develop, produce or provide government programs or services, the public should not lose its right to access this information.

Any government office planning on hiring a consultant, contractor, etc., should make it clear to that future agent that the ***default position*** is that the financial and all other pertinent information related to the contract will be made available to the public, except in rare cases where there are very unusual reasons not to do so.

An example of the type of information I am referring to is cited in the *High Profile Appeals* section of this annual report. The Ministry of Health and Long-Term Care denied an access request for records relating to the e-Physician Project (the ePP), including records maintained by the Smart Systems for Health Agency.

While an appeal to the IPC of that decision was being adjudicated, the requester narrowed the request to a list of consultants hired for the ePP, a description of what they were hired to do, and records relating to their payment. That information was ultimately ordered released by the adjudicator, Brian Beamish, my Assistant Commissioner for Access.

The need for public accountability in the expenditure of public funds is a very important reason why information about such contracts needs to be kept in the public view. All government organizations should make this clear – up front – when seeking outside help.

USE THE *PHIPA* PIA TO IDENTIFY PRIVACY RISKS

Late in 2005, my office developed the *Privacy Impact Assessment Guidelines for the Personal Health Information Protection Act*, a self-assessment tool to assist health information custodians in reviewing the impact that a proposed information system, technology or program may have on the privacy of individuals' personal health information.

Given the increasing use of technology in health care and the constant evolution of that technology, I strongly recommend that every health care institution or professional implementing new technology or upgrading information systems or programs involving personal health information conduct a PIA, to identify and mitigate any possible privacy risks. This is an indispensable tool in the exercise of due diligence. I cannot emphasize enough how strongly I am recommending its use.

requests by the public

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 to personal information they received in the prior calendar year, as well as such other pertinent information as timeliness of responses, outcomes and fees collected.

There were 31,654 freedom of information requests filed across Ontario in 2005, the second highest number ever.

The number of requests filed would have set a record for the fourth straight year except for one very significant development. The Ministry of Health and Long-Term Care received more FOI requests in 2004 than any other government organization in Ontario – 5,199 – but with the enactment of the *Personal Health Information Protection Act (PHIPA)*, the majority of those requests for information are now filed under *PHIPA*. The number of FOI requests filed with that ministry dropped to 212 in 2005, a decline of nearly 5,000.

If the overall total of 3,303 requests filed to government institutions under *PHIPA* are added to the 31,654 FOI requests, the total is 34,957, which would easily exceed the record 33,557 FOI requests filed in 2004.

Provincial organizations received 13,324 FOI requests in 2005, compared with 16,763 in 2004. Of these 2,806 (21.1 per cent) were for personal information and 10,518 (78.9 per cent) were for general records.

Municipal government organizations received 18,330 requests in 2005, an increase of 9.1 per cent over 2004 (when 16,794 requests were filed). Of these, 6,967 (38 per cent) were personal information requests and 11,363 (62 per cent) were for general records.

The Ministry of Environment received the largest number of requests under the provincial *Act* (5,809), followed by the ministries of Community Safety and Correctional Services (3,017), Labour (1,199) and Community and Social Services (598). Together, these four ministries received 79.7 per cent of all provincial requests.

Once again, Police Services Boards received the most requests under the municipal *Act* – 53 per cent of all requests. Municipal corporations were next with 44.1 per cent, followed by school boards at 1.4 per cent and health boards with 0.7 per cent.

Provincial organizations responded to 80.1 per cent of requests within 30 days in 2005, an increase of 11.4 per cent over 2004. This percentage drops marginally to 79.3 per cent when restricted to provincial organizations where a minister is the head. Overall, 94.1 per cent of provincial requests were answered within 60 days (an increase of 5.5 per cent from 2004).

Very significantly, requests that took more than 90 days to complete dropped to 2.5 per cent from 4.9 per cent in 2004.

Municipal government organizations responded to 83.9 per cent of requests within 30 days, up from 75.7 per cent the previous year. Overall, 95.3 per cent of municipal requests were responded to within 60 days, compared to 88.6 per cent the year before.

And, very significantly, the percentage of municipal requests that required more than 90 days to complete dropped by more than two-thirds – to three per cent in 2005 from 9.6 per cent in 2004.

(For a more detailed discussion of compliance rates, see the chapter entitled *Response Compliance*, which follows this chapter.)

The majority of provincial requests in 2005 (73.9 per cent) were made by businesses, while the majority of municipal requests (63.9 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 2005, the most frequently cited exemptions for personal information requests were the protection of other individuals' privacy, followed by law enforcement (sections 49/38 and sections 14/8, respectively, in the provincial and municipal *Acts*). Privacy protection (sections 21/14) was the most used exemption for general records requests, followed by law enforcement (section 14/8).

The *Acts* give individuals the right to request correction of their personal information held by government organizations. In 2005, provincial organizations received five requests for corrections and refused four. Municipal organizations received 154 correction requests and refused five. 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. In 2005, there were seven statements of disagreement filed with municipal organizations; none with provincial organizations.

OUTCOME OF REQUESTS – 2005

	Provincial Requests		Municipal Requests	
All disclosed	3638	27.3%	6777	36.6%
Disclosed in part	3871	29.1%	8080	43.6%
Nothing disclosed	4440	33.3%	2830	15.3%
Withdrawn/abandoned	1376	10.35	826	4.5%

AVERAGE COST OF PROVINCIAL REQUESTS FOR 2005

Personal information	$11.28
General records	$48.89

AVERAGE COST OF MUNICIPAL REQUESTS FOR 2005

Personal information	$ 7.88
General records	$18.95

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 $64,880 in application fees and $418,346.41 in additional fees in 2005. The corresponding numbers for municipal organizations were $78,427.86 and $178,917.34.

Search fees were the most commonly charged category by provincial organizations (61 per cent), followed by reproduction costs (13.6 per cent) and shipping charges (12.3 per cent). Municipal organizations, in contrast, most frequently charged for reproduction costs (42.4 per cent), followed by preparation costs (22.8 per cent) and search fees (22.1 per cent).

CASES IN WHICH FEES WERE ESTIMATED - 2005

	Provincial		Municipal	
Collected in full	5640	81.1%	4017	65.4%
Waived in part	1016	14.6%	106	1.7%
Waived in full	297	4.3%	2,020	32.9%
Total application fees collected (dollars)		$64,880.00		$78,427.34
Total additional fees collected (dollars)		$418,346.41		$178,917.34
Total fees waived (dollars)		$57,250.31		$7,332.57

response rate compliance

To 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.

The IPC is reporting individual compliance rates via two sets of charts. First, as we have done for six years, the compliance rate for each institution is set out in terms of meeting the 30-day response standard set by the *Acts*. A second chart reports on the compliance rate when Notices of Extension (section 27(1) of the provincial *Act*; section 20(1) of the municipal *Act*) and Notices to Affected Person (section 28(1) and section 21(1) respectively) are included in the compliance calculations. The legitimate issuance of either Notice means that a government organization can be in compliance with the *Act*, despite the fact that it takes more than 30 days to respond to a request.

PROVINCIAL ORGANIZATIONS

Overall, provincial ministries had a 30-day compliance rate of 80.1 per cent – the highest provincial compliance rate in 17 years. (The provincial compliance rate was 84.2 per cent, albeit for a much lower number of requests, in 1989, the second year the *Freedom of Information and Protection of Privacy Act* was in effect.)

With the exception of 2004, when one large ministry dragged the provincial average down, the provincial compliance rate has increased every year since 1998 – when the response rate was only 42 per cent – and the IPC advised that it would begin reporting the individual response rates of government organizations the following year.

When Notices are considered, the 2005 provincial compliance rate rises even higher, to an outstanding 86.4 per cent, up from 72.3 per cent for 2004.

There were 16 ministries with compliance rates (including Notices) of over 90 per cent, up one from 2004, even though two of 2004's high-compliance ministries – Consumer and Business Services and Management Board Secretariat – merged into the new Ministry of Government Services (MGS) in 2005. The newly formed MGS achieved an outstanding 96.3 per cent 30-day compliance rate (98.8 per cent with Notices).

The Ministry of the Environment, which completed by far the most requests – 5,757 compared to the 3,060 of the next closest ministry (Community Safety and Correctional Services) – dealt with a 16.6 per cent increase in completed requests while maintaining a high level of compliance: 76.2 per cent, with Notices, compared to 81.6 per cent in 2004.

The Ministry of Community Safety and Correctional Services, despite its caseload, raised both its 30-day compliance rate (to 82.8 per cent from 82.5) and its overall rate with Notices – to an outstanding 99.2 per cent, from 97.6 per cent.

Among other ministries with large numbers of requests completed, the Ministry of Labour achieved an excellent 90.6 per cent compliance rate (90.8 with Notices), while the Ministry of the Attorney General had a 86.8 per cent 30-day rate and an outstanding 97.3 per cent compliance rate with Notices, and the Ministry of Community and Social Services recorded notable compliance rates of 85.1 per cent and 91.6 per cent respectively.

The Ministry of Transportation had an outstanding 30-day compliance rate of 94.9 per cent, which rose even higher – to 96.7 per cent – with Notices.

The Ministry of Natural Resources continues its steady climb, up to 90.8 per cent compliance with Notices, from 86 per cent the previous year and 72 per cent in 2003.

The Ministry of Health and Long-Term Care, which dragged the provincial average down significantly in 2004 with a 40.6 per cent response rate, climbed to 53.4 per cent in 2005 (60.7 per cent with Notices).

MUNICIPAL ORGANIZATIONS

Overall, municipal government institutions responded to 83.9 per cent of requests within the required 30-day time frame, an impressive increase from 2004's 77.6 per cent, and the second consecutive year this number has risen after four years of decline.

In the accompanying charts, the individual response rates from the municipalities that completed the most requests (in each of three population categories) are cited. Also cited, are the police services and school boards that completed the most requests.

Municipalities

Overall, municipal corporations had a 30-day compliance rate of 87.6 per cent, a significant increase from 2004's 79.7 per cent.

Looking first at municipalities with populations of more than 200,000, we note that the City of Mississauga raised its 98.8 per cent 30-day compliance rate of 2004 to a perfect 100 per cent in 2005, while the Regional Municipality of York also showed commendable improvement, achieving a 95.2 per cent 30-day compliance rate, up from 89.5 in 2004. The Town of Markham scored 100 per cent including Notices, on 51 completed requests. The City of Ottawa slipped slightly to 85.4 per cent from 90.1, but when Notices are factored in, increased to an impressive 96 per cent.

But the big gain belongs to the City of Toronto. It achieved an 82.9 per cent 30-day compliance rate on 3,716 completed requests, an impressive improvement on 2004's 65.1 per cent and 2003's 58.7 per cent. (In last year's annual report, we listed the initiatives Toronto was undertaking aimed at improving compliance.) We commend the city's administration for this significant achievement. Cited in the city's 2005 report to the IPC as reasons for the improvement are implementation of policies for routine disclosures of building plans and insurance claims, and the start of efforts to apply routine disclosure to several more city divisions. Development and implementation of a new Access and Privacy Manual has been achieved, along with streamlined processes, reporting systems, escalation procedures, alerts to flag delays and the purchase of a new case management system. It was noted that "the support of the Information and Privacy Commissioner has significantly contributed to the ability of the City Clerk to communicate the importance and responsibility of access and privacy to all city staff."

Turning to mid-size cities: Among the municipal corporations with populations between 50,000 and 200,000, the City of Kitchener, City of Thunder Bay and City of Cambridge all achieved an impressive 100 per cent 30-day compliance rate. The Town of Oakville recorded an excellent 30-day compliance rate of 99.8%, which is even more notable given the big increase in its number of completed requests, from 275 in 2004 to 454 in 2005.

The top eight Ontario municipalities with populations under 50,000 (based on numbers of requests completed) included the Township of McGarry (population 828), with a 100 per cent 30-day compliance rate on the 68 requests completed. The Town of Georgina, Town of Innisfil and City of Belleville also scored perfect marks in this population bracket. When Notices are considered, the Town of Gravenhurst also scored 100 per cent. We commend all of these high-achieving municipalities.

PROVINCIAL: NUMBER OF REQUESTS COMPLETED IN 2005

(includes organizations where the Minister is the Head)

Ministry	Requests Received	Requests Completed	Within 1–30 Days No. of Requests	%	Within 31–60 Days No. of Requests	%	Within 61–90 Days No. of Requests	%	Over 90 Days No. of Requests	%
Agriculture, Food & Rural Affairs	31	27	17	63.0	4	14.8	4	14.8	2	7.4
Attorney General	262	295	256	86.8	22	7.5	7	2.4	10	3.4
Cabinet Office	33	22	21	95.5	0	0.0	0	0.0	1	4.5
Children & Youth Services	60	54	41	75.9	4	7.4	4	7.4	5	9.3
Citizenship & Immigration	8	5	3	60.0	1	20.0	1	20.0	0	0.0
Community Safety & Correctional Services	3017	3060	2534	82.8	466	15.2	34	1.1	26	0.8
Community & Social Services	598	596	507	85.1	69	11.6	7	1.2	13	2.2
Culture	10	8	4	50.0	1	12.5	3	37.5	0	0.0
Democratic Renewal Secretariat	0	0	0		0		0		0	
Economic Development & Trade	16	15	12	80.0	2	13.3	1	6.7	0	0.0
Education	41	43	33	76.7	4	9.3	2	4.7	4	9.3
Energy	29	20	11	55.0	5	25.0	1	5.0	3	15.0
Environment	5807	5757	4315	75.0	985	17.1	304	5.3	153	2.7
Finance	129	126	97	77.0	18	14.3	5	4.0	6	4.8
Government Services	249	240	231	96.3	7	2.9	2	0.8	0	0.0
Health and Long-Term Care	206	234	125	53.4	44	18.8	18	7.7	47	20.1
Health Promotion	0	0	0	0.0	0	0.0	0	0.0	0	0.0
Intergovernmental Affairs	5	5	4	80.0	0	0.0	0	0.0	1	20.0
Labour	1063	1062	962	90.6	57	5.4	16	1.5	27	2.5
Municipal Affairs & Housing	66	62	46	74.2	10	16.1	2	3.2	4	6.5
Natural Resources	129	130	79	60.8	35	26.9	10	7.7	6	4.6
Northern Development and Mines	11	8	4	50.0	2	25.0	1	12.5	1	12.5
Office of Francophone Affairs	4	3	2	66.7	1	33.3	0	0.0	0	
Ontario Secretariat for Aboriginal Affairs	4	1	1	100.0	0	0.0	0	0.0	0	
Ontario Seniors' Secretariat	1	0	0		0		0		0	
Ontario Women's Directorate	1	0	0		0		0		0	
Public Infrastructure Renewal	13	10	10	100.0	0	0.0	0	0.0	0	0.0
Tourism	7	12	3	25.0	6	50.0	3	25.0	0	0.0
Training, Colleges & Universities	67	60	52	86.7	7	11.7	1	1.7	0	0.0
Transportation	223	214	203	94.9	9	4.2	2	0.9	0	0.0

PROVINCIAL: COMPLIANCE INCLUDING NOTICE OF EXTENSION AND NOTICE TO THIRD PARTIES

(includes organizations where the Minister is the Head)

Ministry	30-day compliance %	Compliance including s. 27(1) / 28(1) %
Agriculture, Food & Rural Affairs	63.0	77.8
Attorney General	86.8	97.3
Cabinet Office	95.5	100.0
Children & Youth Services	75.9	85.2
Citizenship & Immigration	60.0	100.0
Community Safety & Correctional Services	82.8	99.2
Community & Social Services	85.1	91.6
Culture	50.0	100.0
Democratic Renewal Secretariat	0.0	0.0
Economic Development & Trade	80.0	93.3
Education	76.7	86.0
Energy	55.0	60.0
Environment	75.0	76.2
Finance	77.0	93.7
Government Services	96.3	98.8
Health & Long-Term Care	53.4	60.7
Health Promotion	0.0	0.0
Intergovernmental Affairs	80.0	80.0
Labour	90.6	90.8
Municipal Affairs & Housing	74.2	83.9
Natural Resources	60.8	90.8
Northern Development & Mines	50.0	100.0
Office of Francophone Affairs	66.7	66.7
Ontario Secretariat for Aboriginal Affairs	100.0	100.0
Ontario Seniors' Secretariat	0.0	0.0
Ontario Women's Directorate	0.0	0.0
Public Infrastructure Renewal	100.0	100.0
Tourism	25.0	100.0
Training, Colleges & Universities	86.7	91.7
Transportation	94.9	96.7

TOP EIGHT MUNICIPAL CORPORATIONS *(population under 50,000) based on number of requests completed*

	Requests Received	Requests Completed	Within 1–30 Days No. of Requests	%	Within 31–60 Days No. of Requests	%	Within 61–90 Days No. of Requests	%	Over 90 Days No. of Requests	%
The Corporation of the City of Belleville (42,300)	13	13	13	100.0	0	0.0	0	0.0	0	0.0
Township of Georgian Bay (1,988)	31	24	11	45.8	13	54.2	0	0.0	0	0.0
Town of Georgina (44,000)	26	26	26	100.0	0	0.0	0	0.0	0	0.0
Town of Gravenhurst (10,899)	26	26	23	88.5	2	7.7	0	0.0	1	3.8
County of Haldimand (43,728)	47	49	34	69.4	12	24.5	3	6.1	0	0.0
Town of Innisfil (26,979)	14	14	14	100.0	0	0.0	0	0.0	0	0.0
Township of McGarry (828)	68	68	68	100.0	0	0.0	0	0.0	0	0.0
Town of New Tecumseh (24,731)	24	20	13	65.0	2	10.0	1	5.0	4	20.0

TOP EIGHT MUNICIPAL CORPORATIONS *(population between 50,000 and 200,000) based on number of requests completed*

	Requests Received	Requests Completed	Within 1–30 Days No. of Requests	%	Within 31–60 Days No. of Requests	%	Within 61–90 Days No. of Requests	%	Over 90 Days No. of Requests	%
City of Barrie (100,825)	87	100	84	84.0	13	13.0	3	3.0	0	0.0
City of Cambridge (110,372)	101	99	99	100.0	0	0.0	0	0.0	0	0.0
City of Greater Sudbury (155,339)	105	97	95	97.9	1	1.0	0	0.0	1	1.0
City of Kitchener (178,178)	329	328	328	100.0	0	0.0	0	0.0	0	0.0
Town of Oakville (144,128)	456	454	453	99.8	1	0.2	0	0.0	0	0.0
City of Oshawa (147,030)	79	76	70	92.1	5	6.6	1	1.3	0	0.0
Town of Richmond Hill (124,740)	371	373	372	99.7	1	0.3	0	0.0	0	0.0
City of Thunder Bay (102,617)	122	121	121	100.0	0	0.0	0	0.0	0	0.0

TOP EIGHT MUNICIPAL CORPORATIONS *(population over 200,000) based on number of requests completed*

	Requests Received	Requests Completed	Within 1–30 Days No. of Requests	%	Within 31–60 Days No. of Requests	%	Within 61–90 Days No. of Requests	%	Over 90 Days No. of Requests	%
City of Brampton (422,600)	103	103	90	87.4	8	7.8	1	1.0	4	3.9
City of Hamilton (490,268)	191	185	155	83.8	29	15.7	0	0.0	1	1.2
Town of Markham (202,781)	52	51	25	83.8	26	51.0	0	0.0	0	0.0
City of Mississauga (695,000)	438	430	430	100.0	0	0.0	0	0.0	0	0.0
City of Ottawa (741,105)	354	349	298	85.4	48	13.8	2	0.6	1	0.3
Regional Municipality of Peel (1,175,101)	110	104	85	81.7	0	0.0	0	0.0	19	18.3
City of Toronto (2,125,394)	3706	3,716	3081	82.9	501	13.5	71	1.9	63	1.7
Regional Municipality of York (734,265)	81	84	80	95.2	3	3.6	0	0.0	1	1.2

TOP EIGHT MUNICIPAL CORPORATIONS

Compliance including Notice of Extension and Notice to Third Parties (population under 50,000, based on number of requests completed)

	30-day compliance %	Compliance including s. 27(1) / 28(1) %
City of Belleville	100.0	100.0
Township of Georgian Bay	45.8	66.7
Town of Georgina	100.0	100.0
Town of Gravenhurst	88.5	100.0
County of Haldimand	69.4	83.7
Town of Innisfil	100.0	100.0
Township of McGarry	100.0	100.0
Town of New Tecumseh	65.0	85.0

TOP EIGHT MUNICIPAL CORPORATIONS

(population between 50,000 and 200,000, based on number of requests completed)

	30-day compliance %	Compliance including s. 27(1) / 28(1) %
City of Barrie	84.0	84.0
City of Cambridge	100.0	100.0
City of Greater Sudbury	97.9	97.9
City of Kitchener	100.0	100.0
Town of Oakville	99.8	99.8
City of Oshawa	92.1	92.1
Town of Richmond Hill	99.7	99.7
City of Thunder Bay	100.0	100.0

TOP EIGHT MUNICIPAL CORPORATIONS

(population over 200,000, based on number of requests completed)

	30-day compliance %	Compliance including s. 27(1) / 28(1) %
City of Brampton	87.4	93.2
City of Hamilton	83.8	91.4
Town of Markham	83.8	100.0
City of Mississauga	100.0	100.0
City of Ottawa	85.4	96.0
Regional Municipality of Peel	81.7	81.7
City of Toronto	82.9	83.8
Regional Municipality of York	95.2	95.2

TOP EIGHT POLICE INSTITUTIONS

(ranked on number of requests completed)

	Requests Received	Requests Completed	Within 1–30 Days No. of Requests	%	Within 31–60 Days No. of Requests	%	Within 61–90 Days No. of Requests	%	Over 90 Days No. of Requests	%
Durham Regional Police Service	696	716	406	56.7	231	32.3	44	6.1	35	4.9
Halton Regional Police Service	793	776	776	100.0	0	0.0	0	0.0	0	0.0
Hamilton Police Service	1280	1243	1063	85.5	177	14.2	3	0.2	0	0.0
London Police Service	544	527	353	67.0	169	32.1	3	0.6	2	0.4
Niagara Regional Police Service	914	900	808	89.8	89	9.9	3	0.3	0	0.0
Ottawa Police Service	424	411	411	100.0	0	0.0	0	0.0	0	0.0
Toronto Police Service	2512	2741	1963	71.6	321	11.7	95	3.5	362	13.2
Windsor Police Service	457	470	294	62.6	160	34.0	16	3.4	0	0.0

TOP EIGHT SCHOOL BOARDS

(ranked on number of requests completed)

	Requests Received	Requests Completed	Within 1–30 Days No. of Requests	%	Within 31–60 Days No. of Requests	%	Within 61–90 Days No. of Requests	%	Over 90 Days No. of Requests	%
le Conseil des écoles catholiques de langue française du Centre-Est	8	8	6	75.0	2	25.0	0	0.0	0	0.0
Dufferin-Peel Catholic District School Board	9	12	6	50.0	5	41.7	1	8.3	0	0.0
Halton District School Board	8	8	8	100.0	0	0.0	0	0.0	0	0.0
Hamilton-Wentworth District School Board	8	8	8	100.0	0	0.0	0	0.0	0	0.0
Hastings and Prince Edward District School Board	45	43	38	88.4	2	4.7	3	7.0	0	0.0
District School Board of Niagara	65	65	60	92.3	5	7.7	0	0.0	0	0.0
Peel District School Board	7	7	7	100.0	0	0.0	0	0.0	0	0.0
Toronto District School Board	14	10	5	50.0	3	30.0	0	0.0	2	20.0

TOP EIGHT POLICE INSTITUTIONS

Compliance including Notice of Extension and Notice to Third Parties (ranked on number of requests completed)

	30-day compliance %	Compliance including s. 27(1) / 28(1) %
Durham Regional Police Service	56.7	58.7
Halton Regional Police Service	100.0	100.0
Hamilton Police Service	85.5	85.5
London Police Service	67.0	99.1
Niagara Regional Police Service	89.8	97.3
Ottawa Police Service	100.0	100.0
Toronto Police Service	71.6	74.3
Windsor Police Service	62.6	62.6

TOP SCHOOL BOARDS

Compliance including Notice of Extension and Notice to Third Parties (ranked on number of requests completed)

	30-day compliance %	Compliance including s. 27(1) / 28(1) %
le Conseil des écoles catholiques de langue française du Centre-Est	75.0	87.5
Dufferin-Peel Catholic District School Board	50.0	50.0
Halton District School Board	100.0	100.0
Hamilton-Wentworth District School Board	100.0	100.0
Hastings and Prince Edward District School Board	88.4	88.4
District School Board of Niagara	92.3	92.3
Peel District School Board	100.0	100.0
Toronto District School Board	50.0	100.0

Police Services

Overall, police services achieved a notable 30-day compliance rate of 80.5 per cent, helped by a very remarkable turnaround by the Toronto Police Service, which had pulled the overall police services compliance average down significantly in recent years.

Toronto Police Service (which completed more than twice as many requests as the next closest police service) achieved a 30-day compliance rate of 71.6 per cent, more than doubling its 2004 compliance rate of 32 per cent. When Notices are considered, Toronto scored 74.3 per cent. We congratulate the Toronto Police Service for this achievement. It appears that steps undertaken over the last year, noted in our report, have borne fruit, and we are hopeful these results can be maintained. The only blemish on this stellar record is the 362 requests, 13.2 per cent of the total, that were completed in over 90 days, and we are hopeful that this number will be reduced in 2006.

Once again, Halton Regional Police Service posted a 100 per cent 30-day compliance rate, and was joined in this select company by the Ottawa Police Service. Hamilton Police Service, which posted a lofty 92.5 per cent 30-day compliance rate in 2004, slipped slightly to 85.5 per cent in 2005, on a slight increase in requests. Durham Regional Police Service, which dropped significantly in 2004 to 51.1 per cent 30-day compliance from 78.3 per cent in 2003, climbed slightly to 56.7 per cent (58.7 with Notices) in 2005.

School Boards

It has been several years – not since the 2002 *Annual Report* – since we last reported on school board compliance (each year, our municipal report includes municipalities, police services and the third largest category – based on the number of requests – of institution, which in 2005 was school boards). Overall, school boards achieved a 30-day compliance rate of 82.9 per cent in 2005.

The District School Board of Niagara achieved a 92.3 per cent 30-day compliance rate on the 65 requests it completed over the course of the year, by far the highest number of requests received by any school board. Hastings and Prince Edward District School Board achieved a 30-day compliance rate of 88.4 per cent (43 completed requests). The Toronto District School Board, one of only two other school boards in the province to receive 10 or more requests, scored 50 per cent for 30-day compliance, but when Notices are considered, achieved 100 per cent. The other board with double-digit requests completed, Dufferin-Peel Catholic District School Board, achieved 50 per cent compliance within 30 days, and the same mark when Notices are included.

access

The *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 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 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 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 2005, 833 appeals regarding access to general records and personal information were made to the IPC, a slight increase from 2004, when 827 were received. The number of appeals closed in 2005 was 756.

ACCESS TO GENERAL RECORDS

Appeals Opened

Overall, 487 appeals regarding access to general records were made to the IPC in 2005. Of these, 204 were filed under the provincial *Act* and 283 under the municipal *Act*. (Percentage figures are rounded off in this report and may not add up to exactly 100.)

Of the 204 provincial general records appeals received, 160 involved ministries and 44 involved agencies. The Ministry of Health and Long-Term Care was involved in the largest number of general records appeals (25), followed by the Ministry of Community Safety and Correctional Services (24), and the ministries of Natural Resources (17), the Attorney General (16), Environment (15) and Finance (11). The agencies with the highest number of general records appeals included the Ontario Lottery and Gaming Corporation (seven), Hydro One (five), Ontario Power Generation (four), Ontario Realty Corporation (four) and the Criminal Injuries Compensation Board (three).

Of the 283 municipal general records appeals received, 174 (61.5 per cent) involved municipalities, 75 (26.5 per cent) involved the police, and 11 (3.9 per cent) involved boards of education. An additional 23 (8.1 per cent) appeals involved other types of municipal institutions.

In terms of the issues raised, 54 per cent of appeals were related to the exemptions claimed by institutions in refusing to grant access. An additional 7.4 per cent concerned exemptions with other issues. As well, 8.8 per cent of appeals were the result of deemed refusals to provide access, in which the institution did not respond to the request within the time frame required by the *Acts*. In 6.4 per cent of appeals, the issue was whether the institution had conducted a reasonable search for the records requested. And 4.3 per cent were third party appeals. The remaining appeals were related to fees, time extensions and other issues.

Among provincial institutions, the Ministry of Health and Long-Term Care had the most deemed refusals (four). No other provincial institution had more than two deemed refusal appeals. With respect to municipal institutions, the City of Toronto had the largest number of deemed refusals (10). No other municipal institution had more than one deemed refusal appeal.

Most appellants were individual members of the public (49.3 per cent). A substantial portion (32.2 per cent) of appellants came from the business community. (If a company were to appeal a denial of access to a competitor's bid for a government contract, for example, the appellant would be categorized as a business.) Other appellants were categorized as associations (8.2 per cent), media (six per cent), and government (2.1 per cent). (With respect to the category of government, if a municipality were to appeal a decision of a provincial government institution, the appellant would be categorized as government.) The remaining appellants were classified under other categories.

Lawyers (95) and agents (28) represented appellants in 25 per cent of general records appeals in 2005.

In 2005, $9,975 in application fees for general records appeals was paid to the IPC.

Appeals Closed

The IPC closed 429 general records appeals during 2005. Of these, 188 (43.8 per cent) concerned provincial institutions and 241 (56.2 per cent) concerned municipal institutions.

Nearly three-quarters (71.6 per cent) of general records appeals were closed without the issuance of a formal order. Of the appeals closed by means other than an order, 8.1 per cent were screened out, 56.4 per cent were mediated in full, 32.6 per cent were withdrawn, 2.6 per cent were abandoned, and 0.3 per cent were dismissed without an inquiry. Of the 144 general records appeals that were not mediated in full and went on to adjudication, 70 appeals (48.6 per cent) were mediated in part during the mediation stage.

The proportion of appeals that were screened out, withdrawn or abandoned was slightly higher for the municipal sector, while the proportion of appeals that were mediated in full was somewhat higher for the provincial sector.

Of the 429 general records appeals closed in 2005, 24.7 per cent were closed during the intake stage, 41.7 per cent during the mediation stage, and 33.6 per cent during the adjudication stage.

Of the appeals closed during the intake stage, 68.9 per cent were withdrawn, 23.6 per cent were screened out, 4.7 per cent were closed by issuing a formal order, and 2.8 per cent were abandoned. Of the appeals closed during the mediation stage, 96.1 per cent were mediated in full, 1.7 per cent were closed by issuing a formal order, 1.7 per cent were withdrawn, and 0.6 per cent were abandoned. Of the appeals closed during the adjudication stage, 79.2 per cent were closed by issuing a formal order, 16.7 per cent were withdrawn, 2.8 per cent were abandoned, 0.7 per cent were mediated in full and 0.7 per cent were dismissed without an inquiry.

In 2005, 28.4 per cent of general records appeals were closed by issuing an order. The IPC issued a total of 114 final orders pertaining to general records – 52 provincial and 62 municipal orders. [1] In addition, the IPC issued eight interim orders – one provincial and seven municipal. [2]

Of the general records appeals resolved by order, the decision of the head was upheld in 33.6 per cent and partly upheld in 37.7 per cent of cases. The head's decision was not upheld in about 22.1 per cent of the appeals closed by order. As well, 6.6 per cent of the orders issued in 2005 had other outcomes.

In comparing the outcome of provincial and municipal orders, it is notable that the decision of the head is somewhat more likely to be fully upheld in municipal orders, and somewhat more likely to be partly upheld or not upheld in provincial orders.

1 The number of appeals closed by order exceeds the number of orders, since one order may close more than one appeal.

2 Overall, the IPC issued a total of 178 final orders – 114 pertaining to access to general records and 64 pertaining to access to personal information. Also, the IPC issued 14 interim orders – eight pertaining to access to general records (which this chapter covers) and six pertaining to access to personal information.

ISSUES IN GENERAL RECORDS APPEALS

Head's Decision	Provincial	%	Municipal	%	Total	%
Exemptions	96	47.1%	167	59.0%	263	54.0%
Exemptions with other Issues	13	6.4%	23	8.1%	36	7.4%
Deemed Refusal	18	8.8%	25	8.8%	43	8.8%
Reasonable Search	11	5.4%	20	7.1%	31	6.4%
Interim Decision	13	6.4%	7	2.5%	20	4.1%
Third Party	12	5.9%	9	3.2%	21	4.3%
Fees (including fee waiver)	6	2.9%	9	3.2%	15	3.1%
Time extension	6	2.9%	2	0.7%	8	1.6%
Frivolous/vexatious request	1	0.5%	1	0.4%	2	0.4%
Transfer	1	0.5%	0	0.0%	1	0.2%
Failure to Disclose	1	0.5%	1	0.4%	2	0.4%
Inadequate Decision	0	0.0%	1	0.4%	1	0.2%
Correction	0	0.0%	1	0.4%	1	0.2%
Other	26	12.7%	17	6.0%	43	8.8%
Total	**204**	**100.0%**	**283**	**100.0%**	**487**	**100.0%**

TYPES OF APPELLANTS

	Provincial	%	Municipal	%	Total	%
Academic/Researcher	3	1.5%	0	0.0%	3	0.6%
Business	78	38.2%	79	27.9%	157	32.2%
Government	6	2.9%	4	1.4%	10	2.1%
Individual	86	42.2%	154	54.4%	240	49.3%
Media	10	4.9%	19	6.7%	29	6.0%
Association/Group	14	6.9%	26	9.2%	40	8.2%
Politician	5	2.5%	0	0.0%	5	1.0%
Union	2	1.0%	1	0.4%	3	0.6%
Total	**204**	**100.0%**	**283**	**100.0%**	**487**	**100.0%**

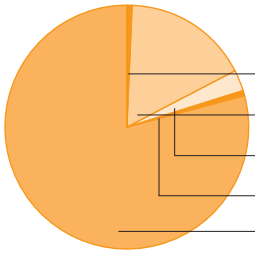
OUTCOME OF APPEALS CLOSED OTHER THAN BY ORDER

	Provincial	%	Municipal	%	Total	%
Screened out	10	7.6%	15	8.6%	25	8.1%
Mediated in full	79	59.8%	94	53.7%	173	56.4%
Withdrawn	41	31.1%	59	33.7%	100	32.6%
Abandoned	2	1.5%	6	3.4%	8	2.6%
No inquiry	0	0.0%	1	0.6%	1	0.3%
Total	**132**	**100.0%**	**175**	**100.0%**	**307**	**100.0%**

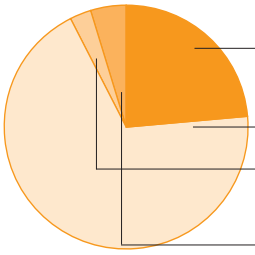
OUTCOME OF APPEALS CLOSED BY ORDER

Head's Decision	Provincial	%	Municipal	%	Total	%
Upheld	17	30.4%	24	36.4%	41	33.6%
Partly upheld	23	41.1%	23	34.8%	46	37.7%
Not upheld	14	25.0%	13	19.7%	27	22.1%
Other	2	3.6%	6	9.1%	8	6.6%
Total	**56**	**100.0%**	**66**	**100.0%**	**122**	**100.0%**

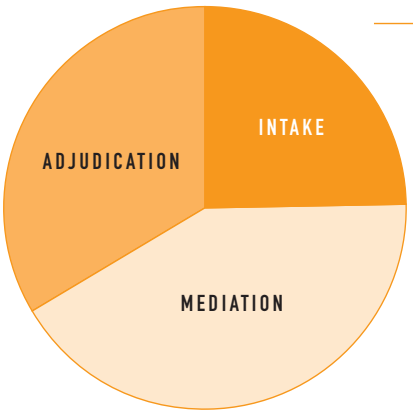
OUTCOME OF APPEALS BY STAGE CLOSED

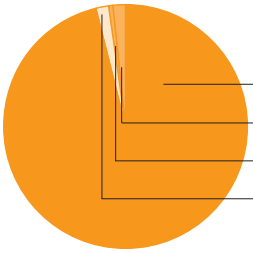


Screened out 0 (0.0%)
Mediated in full 1 (0.7%)
Withdrawn 24 (16.7%)
Abandoned 4 (2.8%)
No inquiry 1 (0.7%)
Ordered 114 (79.2%)
Total 144 (100.0%)



Screened out 25 (23.6%)
Mediated in full 0 (0.0%)
Withdrawn 73 (68.9%)
Abandoned 3 (2.8%)
No inquiry 0 (0.0%)
Ordered 5 (4.7%)
Total 106 (100.0%)





Screened out 0 (0.0%)
Mediated in full 172 (96.1%)
Withdrawn 3 (1.7%)
Abandoned 1 (0.6%)
No inquiry 0 (0.0%)
Ordered 3 (1.7%)
Total 179 (100.0%)

TOTAL

Screened out 25 (5.8%)
Mediated in full 173 (40.3%)
Withdrawn 100 (23.3%)
Abandoned 8 (1.9%)
No inquiry 1 (0.2%)
Ordered 122 (28.4%)
Total 429 (100.0%)

high profile appeals

ORDER MO-2011 – CITY OF OTTAWA

The City of Ottawa received an access request for records dealing with the city's emergency plans. The records sought by the requester included two versions of a "vulnerability analysis report." The city disclosed a number of records in response to the request, but denied access to others. The city disclosed more records during the processing of the requester's appeal to the IPC. The records remaining to be dealt with consisted of one long version of a vulnerability analysis report (VAR), as well as a condensed version, and two pages withheld from other records.

The city relied on the exemptions in sections 7(1) (advice or recommendations), 8(1)(e), (i) and (l) (law enforcement), 11(f) and (g) (economic and other interests of the city) and 13 (danger to safety or health) of the *Municipal Freedom of Information and Protection of Privacy Act*. The city also relied on the discretionary exemption in section 2.1(4) of the *Emergency Management Act* as an alternative basis for denying access.

The IPC adjudicator upheld the application of the advice or recommendations exemption in section 7(1) to those portions of the VAR described as section 4, consisting of staff and consultant recommendations to the senior management team of the city with respect to certain aspects of emergency planning.

MO-197, an order issued in July 2005 by Commissioner Ann Cavoukian that attracted significant attention, is reviewed in the *Issues* section of this annual report in an article entitled, *Building a Culture of Openness in Government.*

The adjudicator then addressed the law enforcement exemptions cited by the city. He acknowledged that, "[B]ecause it is impossible to anticipate the myriad ways in which individuals with criminal intent can cause certain types of emergencies and take advantage of others, it is necessary to be cautious about what information is disclosed in the context of emergency planning processes." However, the adjudicator noted that this consideration does not "relieve an institution claiming these exemptions from its onus to establish a reasonable basis for believing that endangerment will result from disclosure." He added that the exemption applies to "information that can be reasonably expected to either facilitate creation of the risks or hazards, facilitate the commission of crimes after an emergency has occurred, or impede the ability of law enforcement and other officials to respond to the emergency."

The adjudicator differentiated between innocuous or obvious information that is readily available to the public and information whose disclosure may serve to facilitate the harms contemplated by sections 8(1)(e), (i) and (l). He made specific findings with respect to various portions of the records themselves, finding that in some cases, the exemptions apply while in others, they do not. In particular, he found that information such as the ranking of hazards, specific facilities at risk, the specific manner in which a human-created event may be expected to happen, and weaknesses in the response capacity of public agencies, for example, could reasonably be expected to facilitate the harms contemplated by sections 8(1)(e), (i) and (l) in some cases.

With respect to the application of sections 11(f) and (g), which are intended to protect from premature disclosure certain types of plans relating to the management of personnel or the administration of an institution, the adjudicator found the information in the records represents only the "documentation of a step taken in the process of developing a plan" and that they are not plans or proposed plans for the purposes of sections 11(f) and (g). The adjudicator did determine that one page from a duty officer briefing relates to the undisclosed plan for the man-

agement of personnel of the city and that this portion of the records is exempt under section 11(f). Otherwise, these exemptions did not apply.

The adjudicator also considered whether the exemption in section 2.1(4) of the *Emergency Management Act* applied to the parts of the records he had not previously found exempt. This exemption has a harms-based component and requires (among other things) that disclosure could reasonably be expected to prejudice the defence of Canada or its allies, or hinder efforts to combat espionage, sabotage or terrorism. The adjudicator found that the city did not provide a reasonable basis for its belief that this exemption would apply to the information he had not previously found exempt.

In the order, some information was ordered disclosed, but the adjudicator upheld the city's decision not to disclose information that could reasonably be expected to impact law enforcement or planning activities, as well as the advice or recommendations, recognized in the claimed exemptions.

ORDER MO-1989 – TORONTO POLICE SERVICES BOARD

The Toronto Police Services Board received two access requests from a member of the media for access to two police databases. The requests were further to a series of articles by the requester about the issue of racial profiling. The requester was not seeking access to any information that could potentially be used to identify individuals. The requester wanted the police to replace "unique identifiers" (which could identify individuals) with "randomly generated, unique numbers" using one unique number for each individual. The intent was to allow entries about the same individual to be linked, to the extent possible, without identifying any individual.

In response to these requests, the police indicated that, in their view, each request would require them to create a record since the information sought by the requester does not represent recorded information, as required by section 2 of the *Municipal Freedom of Information and Protection of Privacy Act.* As a result, the police advised the requester that the information sought under the requests does not exist.

The requester appealed the decisions to the IPC. As mediation was not possible, the appeals were moved to the adjudication stage of the process.

The adjudicator reiterated the long-standing principle that institutions are not, in most instances, required to create a record in response to a request. The appellant argued that different considerations apply to electronic records which are "capable of being produced from a machine readable record." The adjudicator agreed that the definition of "record" includes only recorded information. He found that although the databases were not designed to record unique identifiers, these identifiers exist in the current databases and, notwithstanding a possible accuracy rate of only 65 to 70 per cent, they are capable of being produced from a machine readable record.

He also considered whether replacing the existing identifiers with unique numbers would amount to creating a record as the police had argued. Applying the principles in Order MO-1381, he found that replacing the unique identifiers in the databases with unique numbers does not amount to creating a record. The information remains the same, though it is now in a "modified, anonymized format." He also found that the information is not changed when the unique identifiers are replaced with randomly generated numbers; instead, it only serves to anonymize the information. The adjudicator ordered the police to issue access decisions to the requester.

[This order is subject to an application from the police for judicial review.]

ORDER PO-2435 – MINISTRY OF HEALTH AND LONG-TERM CARE

The Ministry of Health and Long-Term Care received an access request from a journalist for records relating to the e-Physician Project (the ePP), including records maintained by the Smart Systems for Health Agency (the SSHA). Specifically, the requester sought access to records which included "requests for proposals," contracts, invoices, timesheets, reports and memoranda related to consultants hired for the project.

The requester then narrowed the request to include only a list of consultants hired for the ePP, a description of what they were hired to do and records relating to their payment. After resolution of an issue regarding fees, the ministry denied access to portions of the records under the third party information exemption in section 17(1) and the invasion of privacy exemption in section 21(1) of the *Freedom of Information and Protection of Privacy Act* (the *Act*).

The third party information exemption in section 17(1) requires that each of three requirements be satisfied in order for the section to apply. The information must be "commercial" or "financial," or a number of other categories, must have been "supplied in confidence" to the ministry, and there must be a reasonable expectation that disclosure would lead to one or more "harms" identified in the section, including damage to a third party's competitive position, or undue gain or loss.

Assistant Commissioner Brian Beamish found that the records contain information that qualifies as commercial and financial information for the purposes of that exemption. He then addressed whether the service level agreements entered into between the ministry and its consultants include information that was "supplied" to the ministry by the consultants. He referred to *Boeing v. Ontario (Ministry of Economic Development and Trade)*, [2005] O.J. No. 2851 (Divisional Court.), which upheld a decision, based on a number of recent access to information cases in both Ontario and British Columbia, that the terms of executed contracts are generally not "supplied" even where they were agreed to with little discussion by the government body or agency.

Although not required to do so since the second of the three requirements was not met, the Assistant Commissioner also addressed the "harms" element of the section 17(1) exemption. He found that neither the ministry nor the third parties provided the kind of "detailed and convincing" evidence required to demonstrate a reasonable expectation of prejudice to competitive position, or undue loss or gain, resulting from disclosure. Assistant Commissioner Beamish reminded the parties who opposed disclosure that they "should *not* assume that such harms are self-evident or can be substantiated by self-serving submissions that essentially repeat the words of the *Act*."

The Assistant Commissioner emphasized that transparency and government accountability are the key purposes of access to information legislation. He referred to a number of previous decisions, including Commissioner Ann Cavoukian's Order MO-1947 (City of Toronto), and explained that "the need for public accountability in the expenditure of public funds is an important reason behind the need for 'detailed and convincing' evidence to support the harms outlined in section 17(1)." He added that, "[W]ithout access to the financial details contained in contracts related to the ePP, there would be no meaningful way to subject the operations of the project to effective public scrutiny. Further, there would be insufficient information to assess the effectiveness of the project and whether taxpayer money was being appropriately spent and accounted for."

The section 21(1) exemption was addressed through a finding that, whether or not the information qualified as "personal information" as defined in section 2(1) of the *Act*, the exception to the personal privacy exemption found in section 21(4)(b) mandated the disclosure of the information. This section states that disclosure is not an unjustified invasion of personal privacy if it "discloses financial or other details of a contract for personal services between an individual and an institution." The ministry and SSHA were ordered to disclose all responsive records to the appellant.

privacy

To help 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 attempts to mediate a solution. The IPC may make formal recommendations to a government organization to amend its practices.

STATISTICAL OVERVIEW

Overall, 101 privacy complaint files were **opened** in 2005 under the two public sector *Acts*. (See the *PHIPA* section, which follows this section, for a report on the number of privacy complaints filed under the *Personal Health Information Protection Act*.) Of the complaints filed under the public sector *Acts*, 49 complaints (48.5 per cent) were filed under the provincial *Act* and 50 (49.5 per cent) under the municipal *Act*. In addition, two non-jurisdictional complaints were filed in 2005. The previous year, 128 complaint files were opened.

Of the complaints opened in 2005, 73 (72.3 per cent) were initiated by individuals and 28 (27.7 per cent) were initiated by the Commissioner. (Percentage figures are rounded off in this report and may not add up exactly to 100).

Ninety-six privacy complaints were **closed** in 2005. The complaints that were resolved involved 98 issues. The disclosure of personal information was the most frequent issue, raised in 74.5 per cent of complaints. The collection of personal information was an issue in 14.3 per cent, general privacy was an issue in 4.1 per cent and security was an issue in 3.1 per cent of complaints. The remainder involved other issues including use, retention, notice of collection and consent.

Roughly seven out of every eight issues – 86.7 per cent – raised in the privacy complaints were disposed of without the need for a formal finding. For the issues requiring a finding, institutions were found to have complied with the *Acts* in 61.5 per cent of complaints, and to have not complied in 38.5 per cent.

While processing privacy complaints, the IPC continues to emphasize informal resolution. Consistent with this approach, 84 of the 96 privacy complaints closed in 2005 – 87.5 per cent – were closed without the issuance of a formal privacy complaint report. Seventy-seven complaints (80.2 per cent of complaints) were closed during the intake stage. Of these, 18.2 per cent were screened out, 15.6 per cent were withdrawn, and 66.2 per cent were resolved informally. The remaining 19.8 per cent of complaints proceeded to the investigation stage. Of the complaints closed during this stage, 10.5 per cent were withdrawn, 26.3 per cent were settled, and 63.2 per cent were closed by issuing a report. Twelve privacy complaint reports were issued in 2005. These reports contained three recommendations to government organizations.

Of the 96 complaints closed in 2005, individual members of the public initiated 67.7 per cent of the complaints and the Commissioner initiated 32.3 per cent.

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 can 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 2005, 833 appeals regarding access to general records and personal information were made to the IPC, a slight increase over the number received in 2004 (827). The overall number of appeals closed in 2005 was 756.

ACCESS AND CORRECTION OF PERSONAL INFORMATION

Appeals Opened

The IPC received 346 appeals regarding access or correction of personal information in 2005. Of these, 131 (37.9 per cent) were filed under the provincial *Act* and 213 (61.6 per cent) under the municipal *Act*. Two non-jurisdictional personal information appeals were made in 2005. (Percentage figures are rounded off in this report and may not add up exactly to 100).

Of the 131 provincial personal information appeals received, 111 (84.7 per cent) involved ministries and 20 (15.3 per cent) involved agencies. The Ministry of Community Safety and Correctional Services was involved in the largest number of personal information appeals (69). The Ministry of Community and Social Services (13) and the Ministry of the Attorney General (10) had the next highest number of personal information appeals, followed by the ministries of Health and Long-Term Care (five) and Transportation (three). The agencies with the highest number of personal information appeals included the Ontario Human Rights Commission (five), Centennial College of Applied Arts and Technology (two), Hydro One (two) and the Ontario Lottery and Gaming Corporation (two).

Of the 213 municipal personal information appeals received, 151 (70.9 per cent) involved police services, 42 (19.7 per cent) involved municipalities, and 10 (4.7 per cent) involved boards of education. Ten appeals (4.7 per cent) involved other types of municipal institutions.

The majority of personal information appeals – 62.5 per cent – were related to the exemptions claimed by institutions in refusing to grant access. An additional 8.4 per cent concerned exemptions with other issues. And 5.5 per cent of personal information appeals were the result of deemed refusals to provide access, in which the institution did not respond to the request within the time frame required by the *Acts*. In 7.6 per cent of appeals, the issue was whether the institution had conducted a reasonable search for the records requested, and in 2.3 per cent, the issue was whether the request had been frivolous or vexatious. The remaining appeals were related to fees, time extensions, interim decisions, and various other issues.

In comparing municipal and provincial appeals, provincial personal information appeals were more likely to involve exemptions, deemed refusals, or reasonableness of search, while municipal personal information appeals were more likely to involve exemptions with other issues, fees or determination as to whether the request had been frivolous or vexatious.

No provincial institution had more than two deemed refusals. Of the municipal institutions, the City of Brantford had the highest number of deemed refusal appeals (five). No other municipal institution had more than two.

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 (94) or agents (13) represented appellants in 30.9 per cent of the personal information appeals made in 2005.

In 2005, $2,624 in application fees for personal information appeals was paid to the IPC.

Appeals Closed

The IPC closed 327 personal information appeals during 2005. Of these, 127 (38.8 per cent) involved provincial institutions, while 198 (60.6 per cent) concerned municipal institutions. The IPC also closed two non-jurisdictional personal information appeals during 2005.

Just over three-quarters (76.1 per cent) of personal information appeals were closed without the issuance of a formal order. Of the appeals closed by means other than an order, 16.6 per cent were screened out, 55.5 per cent were mediated in full, 21.1 per cent were withdrawn, 6.5 per cent were abandoned, and 0.4 per cent were dismissed without an inquiry. Of the 91 personal information appeals that went on to adjudication, 39 (42.9 per cent) were mediated in part during the mediation stage.

Of the 327 personal information appeals closed in 2005, 29.7 per cent were closed during the intake stage, 42.5 per cent during the mediation stage, and 27.8 per cent during the adjudication stage.

Of the appeals closed during the intake stage, 46.4 per cent were withdrawn, 43.3 per cent were screened out, 8.2 per cent were abandoned, and 2.1 per cent were closed by issuing a formal order. Of the appeals closed during the mediation stage, 97.1 per cent were mediated in full, 0.7 per cent were withdrawn, and 2.2 per cent were abandoned. Of the appeals closed during the adjudication stage, 83.5 per cent were closed by issuing a formal order, 6.6 per cent were withdrawn, 6.6 per cent were abandoned, 2.2 per cent were mediated in full, while 1.1 per cent were dismissed without an inquiry.

In 2005, 23.9 per cent of personal information appeals were closed by issuing an order. The IPC issued a total of 64 final orders for personal information appeals – 27 provincial and 37 municipal orders.[1] In addition, the IPC issued six interim orders – two provincial and four municipal.

In appeals resolved by an order, the decision of the head was upheld in 56.4 per cent and partly upheld in 29.5 per cent of cases. The head's decision was not upheld in about nine per cent of the personal information appeals closed by order. As well, 5.1 per cent of the orders issued in 2005 had other outcomes. In comparing the outcomes of provincial and municipal orders, the decision of the head was almost equally likely to be upheld or partly upheld for both provincial and municipal orders. The head's decision was somewhat more likely not to be upheld in municipal orders; other outcomes were somewhat more likely to occur in provincial orders.

1 The number of appeals closed by order exceeds the number of orders, since one order may close more than one appeal.

SUMMARY OF PRIVACY COMPLAINTS - 2005

	2004 PRIVACY COMPLAINTS				2005 PRIVACY COMPLAINTS			
	Provincial	Municipal	Non-jurisdictional	Total	Provincial	Municipal	Non-jurisdictional	Total
Opened	76	41	11	128	49	50	2	101
Closed	74	41	11	126	51	43	2	96

NUMBER OF PRIVACY COMPLAINTS CLOSED 1999-2005

	Provincial	Municipal	Non-jurisdictional	Total
1999	40	48	0	88
2000	39	41	2	82
2001	61	28	6	95
2002	54	38	7	99
2003	66	60	2	128
2004	74	41	11	126
2005	51	43	2	96

PRIVACY COMPLAINTS BY TYPE OF RESOLUTION

	Provincial	%	Municipal	%	Non-jurisdictional	%	Total	%
Screened out	6	11.8%	6	14.0%	2	100.0%	14	14.6%
Abandoned	0	0.0%	0	0.0%	0	0.0%	0	0.0%
Withdrawn	4	7.8%	10	23.3%	0	0.0%	14	14.6%
Settled	3	5.9%	2	4.7%	0	0.0%	5	5.2%
Informal resolution	32	62.7%	19	44.2%	0	0.0%	51	53.1%
Report	6	11.8%	6	14.0%	0	0.0%	12	12.5%
Total	**51**	**100.0%**	**43**	**100.0%**	**2**	**100.0%**	**96**	**100.0%**

SOURCE OF COMPLAINANTS

	Provincial	%	Municipal	%	Non-jurisdictional	%	Total	%
Individual	26	51.0%	37	86.0%	2	100.0%	65	67.7%
IPC Commissioner-initiated	25	49.0%	6	14.0%	0	0.0%	31	32.3%
Total	**51**	**100.0%**	**43**	**100.0%**	**2**	**100.0%**	**96**	**100.0%**

PRIVACY COMPLAINTS BY TYPE OF RESOLUTION AND STAGE CLOSED

	Intake	%	Investigation	%	Total	%
Screened out	14	18.2%	0	0.0%	14	14.6%
Abandoned	0	0.0%	0	0.0%	0	0.0%
Withdrawn	12	15.6%	2	10.5%	14	14.6%
Settled	0	0.0%	5	26.3%	5	5.2%
Informal resolution	51	66.2%	0	0.0%	51	53.1%
Report	0	0.0%	12	63.2%	12	12.5%
Total	**77**	**100.0%**	**19**	**100.0%**	**96**	**100.0%**

ISSUES* IN PRIVACY COMPLAINTS

	Provincial	%	Municipal	%	Non-jurisdictional	%	Total	%
Disclosure	38	73.1%	35	79.5%	0	0.0%	73	74.5%
Collection	6	11.5%	8	18.2%	0	0.0%	14	14.3%
Use	0	0.0%	1	2.3%	0	0.0%	1	1.0%
Security	3	5.8%	0	0.0%	0	0.0%	3	3.1%
Retention	1	1.9%	0	0.0%	0	0.0%	1	1.0%
Disposal	0	0.0%	0	0.0%	0	0.0%	0	0.0%
Access	0	0.0%	0	0.0%	0	0.0%	0	0.0%
Personal information	0	0.0%	0	0.0%	0	0.0%	0	0.0%
Notice of collection	1	1.9%	0	0.0%	0	0.0%	1	1.0%
General privacy	2	3.8%	0	0.0%	2	100.0%	4	4.1%
Consent	1	1.9%	0	0.0%	0	0.0%	1	1.0%
Total	**52**	**100.0%**	**44**	**100.0%**	**2**	**100.0%**	**98**	**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 ISSUES* IN PRIVACY COMPLAINTS

	Provincial	%	Municipal	%	Non-jurisdictional	%	Total	%
Did not comply with the *Act*	2	3.8%	3	6.8%	0	0.0%	5	5.1%
Complied with the *Act*	4	7.7%	4	9.1%	0	0.0%	8	8.2%
Act does not apply	6	11.5%	6	13.6%	2	100.0%	14	14.3%
Resolved – Finding not necessary	40	76.9%	31	70.5%	0	0.0%	71	72.4%
Complied in part	0	0.0%	0	0.0%	0	0.0%	0	0.0%
Total	**52**	**100.0%**	**44**	**100.0%**	**2**	**100.0%**	**98**	**100.0%**

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

ISSUES IN PERSONAL INFORMATION APPEALS

	Provincial	%	Municipal	%	Total	%
Exemptions	86	65.6%	129	60.6%	215	62.5%
Exemptions with other issues	5	3.8%	24	11.3%	29	8.4%
Deemed refusal	8	6.1%	11	5.2%	19	5.5%
Reasonable search	13	9.9%	13	6.1%	26	7.6%
Fees (including fee waiver)	1	0.8%	4	1.9%	5	1.5%
Time extension	1	0.8%	1	0.5%	2	0.6%
Interim decision	1	0.8%	1	0.5%	2	0.6%
Frivolous/vexatious request	0	0.0%	8	3.8%	8	2.3%
Correction	2	1.5%	3	1.4%	5	1.5%
Third party	1	0.8%	1	0.5%	2	0.6%
Inadequate decision	0	0.0%	1	0.5%	1	0.3%
Other	13	9.9%	17	8.0%	30	8.7%
Total	**131**	**100.0%**	**213**	**100.0%**	**344**	**100.0%**

(Two non-jurisdictional appeals were not included in this chart).

OUTCOME OF APPEALS BY STAGE CLOSED

	Intake	%	Mediation	%	Adjudication	%	Total	%
Screened out	42	43.3%	0	0.0%	0	0.0%	42	12.8%
Mediated in full	0	0.0%	135	97.1%	2	2.2%	137	41.9%
Withdrawn	45	46.4%	1	0.7%	6	6.6%	52	15.9%
Abandoned	8	8.2%	3	2.2%	6	6.6%	17	5.2%
No inquiry	0	0.0%	0	0.0%	1	1.1%	1	0.3%
Ordered	2	2.1%	0	0.0%	76	83.5%	78	23.9%
Total	**97**	**100.0%**	**139**	**100.0%**	**91**	**100.0%**	**327**	**100.0%**

OUTCOME OF APPEALS CLOSED OTHER THAN BY ORDER

	Provincial	%	Municipal	%	Total	%
Screened out	14	14.0%	27	18.4%	41	16.6%
Mediated in full	57	57.0%	80	54.4%	137	55.5%
Withdrawn	21	21.0%	31	21.1%	52	21.1%
Abandoned	8	8.0%	8	5.4%	16	6.5%
No inquiry	0	0.0%	1	0.7%	1	0.4%
Total	**100**	**100.0%**	**147**	**100.0%**	**247**[1]	**100.0%**

[1] *In addition, two non-jurisdictional files were closed other than by order. One was screened out and the other abandoned, both at the intake stage.*

OUTCOME OF APPEALS CLOSED BY ORDER

Head's Decision	Provincial	%	Municipal	%	Total	%
Upheld	15	55.6%	29	56.9%	44	56.4%
Partly upheld	8	29.6%	15	29.4%	23	29.5%
Not upheld	1	3.7%	6	11.8%	7	9.0%
Other	3	11.1%	1	2.0%	4	5.1%
Total	**27**	**100.0%**	**51**	**100.0%**	**78**	**100.0%**

high profile privacy incidents

HO-001 – FIRST *PHIPA* ORDER

On Saturday, October 1, 2005, Information and Privacy Commissioner Ann Cavoukian was contacted by a newspaper reporter who advised her that sensitive patient health records had been scattered across the streets of downtown Toronto. The location was being used for a film shoot about the September 11, 2001 terrorist attack on New York City's World Trade Centre.

The seriousness of the incident, and the potential devastating impact on patient privacy, led the Commissioner to personally visit the scene.

The Commissioner had a number of discussions with senior staff over that weekend, then, on Monday, October 3, the Commissioner implemented the IPC's "privacy breach protocol," and commenced an investigation pursuant to the *Personal Health Information Protection Act (PHIPA)*. The Commissioner met with key staff members to review the known facts, develop an action plan and assign responsibilities to carry it out.

The first priority was to move quickly to ensure that the breach was contained and the health records retrieved. Two investigation teams were assigned to attend relevant sites to recover any personal health information and to start the process of determining how this incident could have occurred. Initially, the two teams retrieved records from a number of sources, including the reporter, the recycling company that provided the records to the film shoot and a member of the public who had contacted the IPC.

IPC investigators spoke to the film's producer, who informed the investigators that, on the day in question, the production company used what it believed was scrap paper for special effects purposes during the filming on city streets. A special effects company had obtained the paper from a recycling company. On the Saturday, after the film crew learned that the paper had included patient health records, it quickly began retrieving it. The recycling company that had provided the paper was contacted and asked to come to the set to assist in retrieving the paper from the streets. The recycling company immediately returned to the site and removed the records.

Further investigation by IPC staff determined that the health records, most of them dating back to 1992, originated with a Toronto X-ray and ultrasound clinic (*Toronto clinic*). Boxes containing the records had been removed, without notice, from a locked storage area by the *Toronto clinic's* landlord and placed near the building's common parking area. A *Toronto clinic* staff member, realizing that the records were not secure, drove them to a Richmond Hill clinic owned by the same corporation. From there, the boxes were picked up by the *paper disposal company* that provided shredding services for both clinics. Because of a misunderstanding on the part of an employee of the *paper disposal company*, some of the boxes were mistakenly believed to be intended for recycling, not shredding. These boxes were then passed on to the recycling company, which subsequently sold the records to the special effects company for use on the film set.

Throughout the investigation, staff of all parties involved were extremely co-operative with IPC investigators and worked closely with the IPC to contain the damage from the original incident, to investigate the facts and to prevent a similar incident from occurring in the future. The IPC also worked closely with the Toronto clinic to develop a plan to notify affected patients. Given the age of the records and the potential that patient addresses had been rendered inaccurate, it was determined that the best approach would be to post a notice at the Toronto clinic. The notice set out exactly what happened and the chain of events leading to the loss of the records.

Following the completion of the investigation, the Commissioner issued her first order (HO-001) under *PHIPA on October 31, 2005*. The order concluded that the *Toronto clinic* had 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 clinic also failed to ensure that the personal health information was disposed of in a secure manner and that its agent, the *paper disposal company*, handled the records responsibly.

In her order, the Commissioner emphasized the critical need for the secure disposal of records containing personal health information. Industry standards indicate that secure disposal means permanently destroying the records by irreversible shredding or pulverizing, thus making them *unreadable* and *non-reconstructable*. Recycling can never equate secure disposal. Any health information custodian who is relying on a third party to dispose of records must have a written agreement in place setting out the obligation for secure disposal and requiring the third party to provide written confirmation once the secure disposal has occurred.

Based on her findings, the Commissioner ordered the following:

- The *Toronto clinic* was ordered to review its information practices to ensure that personal health records are securely stored and protected against theft, loss and unauthorized use or disclosure;
- The *clinic* was ordered to put into place a written contract with any agent it retains to dispose of health records. The agreement must set out the obligation for secure disposal and require the agent to provide written attestation once secure disposal has been concluded;
- The *paper disposal company* was ordered to put into place a written contract with any health information custodian for whom it provides shredding services – including the obligation for it to shred securely and irreversibly and to provide an attestation of destruction; and
- The *paper disposal company* was also ordered to ensure that any handling of health records by a third party on its behalf be documented in a written contact that binds the third party to the requirements and obligations of *PHIPA*.

Order HO-001 provides detailed guidance to all health professionals and their agents in Ontario with respect to the Commissioner's expectations for the secure disposal of health records. Based on Order HO-001, the IPC developed a fact sheet entitled, *Secure Destruction of Personal Information,* to provide further assistance to anyone responsible for the destruction of personal and confidential information. (That fact sheet is available on the IPC's website, **www.ipc.on.ca**.)

UPDATE ON IPC SPECIAL REPORT

On December 14, 2004, the Commissioner tabled a Special Report to the Legislative Assembly of Ontario on the disclosure of personal information by the Shared Services Bureau (the SSB) of Management Board Secretariat (now the Ministry of Government Services, MGS) and the Ministry of Finance (the ministry). The report detailed her investigation of the mailing of more than 27,000 cheques under the Ontario Child Care Supplement for Working Families Program that included – on the cheque stubs – the name, address and Social Insurance Number of another recipient, as well as each recipient's own personal information. The Commissioner's 2004 Annual Report detailed the highlights of the investigation and the recommendations she made in the special report.

In her report, the Commissioner made the following recommendations:

- that MGS initiate a comprehensive and independent end-to-end audit of SSB's functions, operations and privacy practices involving the handling of personal information and that this audit report should be made available to the public;

- that the ministry and MGS discontinue the practice of using the Social Insurance Number (SIN) and create a purpose-specific unique identifier for each of their clients to replace the use of the SIN; and
- as an additional security and quality assurance measure, and pending the outcome of the independent audit, MGS ensure that a trial run printing of several cheques on the production printer be conducted and the cheques manually examined by someone from the program area involved, before each monthly printing of the cheques and stubs is commenced.

The IPC is pleased to report that the ministry and MGS have fully complied with all of these recommendations and applaud them for this excellent work.

In February 2005, MGS presented the terms of reference for the end-to-end audit of SSB's operations to the IPC and confirmed that the SSB had retained Deloitte and Touche LLP (Deloitte) to conduct a comprehensive review of all SSB functions involving the protection of personal information. The objective of the review was "to report on the design and existence of controls in place at SSB to protect personal information, with a view to fostering a culture of privacy protection, commensurate with current and evolving Canadian standards." The end goal was also to help MGS and SSB develop a more effective privacy culture that was both compliant and sustainable.

In March 2005, MGS advised that the SIN was no longer printed on Ministry of Finance cheques and stubs for the Ontario Child Care Supplement recipients. MGS has since reported that the SIN is also no longer used in the ministry's tax systems to access program information for other social assistance programs. MGS advised further that the SIN is no longer used on employee health and dental claims and that it has been replaced with the workplace identification number. New forms have been created to reflect this change.

In June 2005, the ministry and MGS met with the Commissioner to report on further progress. Deloitte had gathered information on all SSB practices, procedures, operations and activities for handing personal information. This involved more than 60 interviews with the SSB executive management team, directors, senior management, OSS staff and other MGS executives. All SSB business processes involving personal information were reviewed and all SSB holdings of personal information were identified and updated in the public *Directory of Records*.

The Ontario Shared Services Privacy Standard or *FIPPA* Plus was developed and endorsed as the standard against which the SSB privacy practices were reviewed and gaps or areas of deficiency identified. The privacy standard was then used to conduct the review of management responsibility for privacy, requirements pertaining to notice, collection, limiting use and disclosure, accuracy, disposition, security, transparency, access and correction within SSB. The privacy standard was also used to develop tools, policies and practices to fill the gaps identified through the review.

All privacy incidents identified in the Commissioner's special report and subsequent incidents were reviewed to ensure that all necessary actions and remedies had been completed.

By June, more than 85 per cent of the OSS staff had received training on privacy, handling and classifying personal or sensitive information, and the development of privacy impact assessments and threat risk assessments. Between March and June 2005, 56 training sessions were held around the entire province.

In August 2005, MGS delivered a copy of the audit completed by Deloitte to the IPC. The audit report concludes that, as a result of the review, the SSB "has addressed privacy in a positive and proactive manner and developed privacy-specific standards based on the requirements of provincial legislation and fair information practices that recognize the rights and obligations of both individuals and the government in dealing with personal information."

Subsequently, MGS confirmed that all work to eliminate use of the SIN as a personal identifier was completed in December 2005, in compliance with the recommendation made in the Commissioner's special report. MGS and the Ministry of Finance are highly commended for their remedial work in this critical area.

implementation of the *Personal Health Information Protection Act*

Throughout 2005, much of the work of the IPC continued to be focused around the implementation of Ontario's new *Personal Health Information Protection Act (PHIPA)*, which came into effect November 1, 2004.

Resources for health information custodians that were added during 2005 included a privacy impact assessment tool, a range of fact sheets, and three sets of "short notice" brochures and posters (about patients' privacy rights) for hospitals, health care providers' offices, and long-term care facilities. The IPC also completed the reviews of eight organizations that were required to have their information practices and procedures approved by the IPC prior to November 1, 2005. In November, a conference to celebrate the successes of the health community in implementing *PHIPA* and to discuss best practices was hosted by the IPC.

PIA TOOL

A privacy impact assessment (PIA) is a self-assessment tool designed to help organizations assess the impact of a proposed information system, technology or program on privacy. The goal of any PIA is to assess the risks to privacy and to develop strategies for mitigating those risks. Although PIAs are not required under *PHIPA*, they are rapidly becoming a best practice for protecting privacy in the health sector. Accordingly, the IPC developed a PIA self-assessment tool specifically designed to help health information custodians comply with the requirements of *PHIPA* whenever they are considering changing or implementing information systems, technology, programs or services. The value of the PIA self-assessment tool is reflected in its high degree of popularity among health information custodians.

FACT SHEETS

The IPC issues fact sheets in response to important issues that have been raised in relation to *PHIPA* (by the IPC, health information custodians or patients). For example, although *PHIPA* requires health information custodians to ensure that records of personal health information are disposed of in a secure manner, the legislation provides no guidance on how this may be done. The lack of clarity around appropriate disposal procedures contributed to at least one high profile privacy breach in 2005 in which records of personal health information were used as props by a movie production company. This serious breach resulted in both the first order issued by the Commissioner under *PHIPA* and the issuing of a fact sheet on *Secure Destruction of Personal Information.*

Another prominent issue for health information custodians was the implementation of the "lock-box" provisions of *PHIPA*, which came into full force in November 2005. Lock-box is a term that is used to refer to those provisions of the legislation that allow individuals to withdraw their implied consent for the collection, use and disclosure of personal health information for the purpose of providing health care, and allow individuals to expressly instruct custodians not to use or disclose their personal health information for the purpose of providing health care, in those circumstances where custodians are permitted to do so without consent. Implementation of these requirements is particularly challenging for organizations that rely on legacy systems of personal health information that were not designed to accommodate individuals' preferences. While assisting health information custodians in addressing lock-box issues, it became apparent that there was a lack of clarity around what the lock-box is, and what the legislative requirements are in relation to the lock-box. The *Lock-box Fact Sheet* was issued to address this need.

To ensure the new health privacy legislation was not perceived to be a potential barrier to the disclosure of personal health information in emergency situations, the IPC issued a fact sheet on the *Disclosure of Information Permitted in Emergency or other Urgent Circumstances*. The impetus for the fact sheet came from several high profile cases in which failures to disclose critical information in a timely manner, largely due to misperceptions about restrictions imposed by privacy legislation, may have contributed to harm or the death of an individual. To help prevent these types of tragedies from occurring in the future, the fact sheet was issued to raise awareness about the provisions of *PHIPA* and other access and privacy legislation in Ontario that would permit the flow of personal information in a range of urgent circumstances and to encourage health information custodians and others to exercise their discretion to disclose personal information in appropriate circumstances. (See the article, *Disclosure of information in emergency or other urgent circumstances*, in the *Issues* section of this annual report.)

SHORT NOTICES

Transparency about information practices is one of the fundamental principles of privacy protection. Accordingly, whenever new privacy legislation is introduced, organizations that fall within the scope of the legislation are often required to begin providing notice about their practices and procedures for collecting, using and disclosing personal information.

In the past, the introduction of new privacy legislation often resulted in individuals being bombarded with long, legalistic privacy notices that were specifically designed to fulfil an organization's perceived legal obligations. However, these privacy notices tended to be incomprehensible to members of the public, were often ignored, and generally served no useful purpose in terms of enhancing transparency about an organization's information practices. To ensure that this did not happen with the introduction of *PHIPA*, the IPC established a working group to develop short, comprehensible, layered notices that would be appropriate for certain health information custodians to provide to their patients.

Short notice posters that provide essential information, backed up by privacy brochures containing more detailed information about the collection, use and disclosure of personal health information, were developed for health care providers, hospitals, and long-term care facilities. The success of this project is reflected in the high demand for these from health information custodians. More than 325,000 brochures and posters were distributed by the IPC in 2005.

REVIEWS

By October 31, 2005, the IPC completed its mandated reviews of four prescribed entities and four prescribed persons that compile or maintain registries of personal health information. *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.

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 (Information System for Cytology), the London Health Sciences Centre (Ontario Joint Replacement Registry), and the Canadian Stroke Network (Canadian Stroke Registry).

One of the conditions for disclosures to prescribed entities and prescribed persons that compile or maintain registries is that, prior to November 1, 2005, these organizations were required to have their information practices and procedures approved by the IPC. The IPC assessed these 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. All of the organizations that were reviewed were successful in having their information practices and procedures approved by the IPC. Final reports on each of the reviews and approvals are posted on the IPC's website.

PHIPA SUMMIT

On November 3, 2005, the IPC sponsored the *PHIPA Summit, PHIPA: A Balancing Act*, to celebrate the successes of the health community in implementing *PHIPA* and to discuss best practices. About 300 health information custodians from across Ontario attended this Toronto conference. The *Summit* provided an opportunity for the health care provider community to share their own experiences with *PHIPA* over the first year, to learn best practices and to participate in spirited debate and discussion with field leaders. One of the feature sessions of the conference was a panel discussion on privacy and electronic health records chaired by Commissioner Ann Cavoukian. The *PHIPA Summit* was declared a resounding success by those in attendance.

DETERMINATIONS

In conducting reviews, whenever the Commissioner must inspect a record of, require evidence of, or inquire into personal health information without the consent of the person to whom it relates, the Commissioner must first determine that it is reasonably necessary to do so to carry out the review and that the public interest in carrying out the review justifies dispensing with obtaining the individual's 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 2005, the Commissioner made one such determination (after records of personal health information were strewn across Toronto streets as a backdrop for a film shoot) and issued two written statements in conjunction with that determination. In that case, it was not possible to obtain the individuals' consent since the identities of the individuals whose privacy had been breached could not be determined unless the Commissioner first reviewed the records. The review was necessary to determine if the records contained personal health information and an unauthorized disclosure had been made, and to prevent further disclosure of the personal health information. The Commissioner also concluded that it was in the interests of the individuals whose health records were affected that these records be secured by the Commissioner's office as quickly as possible. 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, reflecting the number and nature of all privacy complaints filed with the IPC in 2005 under *PHIPA*. These are reported in the *Complaints Filed with IPC* section, which follows.

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* and the *Municipal Freedom of Information and Protection of Privacy Act* are required to file a detailed statistical report to the IPC, *PHIPA* covers the full health care sector rather than just government organizations. Most 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 government organizations that employ health information custodians (a school board, for example, with a school nurse). Hospitals are not required to file, but 48 public hospitals voluntarily submitted a statistical report.

A brief review of access requests filed with health information custodians, based on the limited statistics available, is included in this article (under *Personal Information Requests*).

COMPLAINTS FILED WITH THE IPC

In 2005, 177 complaints were opened under *PHIPA*. Of these, 75 (42.4 per cent) were about access to and/or correction of personal health information and 49 (27.8 per cent) were about the collection, use and/or disclosure of personal health information. Thirty-five (19.8 per cent) were self-reported privacy breaches by health information custodians and the other 18 (10.1 per cent) were Commissioner-initiated complaints. (Percentage figures in this report are rounded off and may not add up to 100.)

Of these 177 complaints, 47 (26.6 per cent) involved public hospitals, 29 (16.4 per cent) involved doctors, 14 (7.9 per cent) involved clinics, 12 (6.8 per cent) involved the Ministry of Health and Long-Term Care, 10 (5.6 per cent) involved community care access centres, eight (4.5 per cent) involved psychiatric facilities, eight (4.5 per cent) involved independent health facilities, and seven (4.0 per cent) involved laboratories. The remaining complaints involved various other health information custodians and non-health information custodians, such as agents.

During 2005, 108 *PHIPA* complaints were closed. Of these, 59 (54.6 per cent) were about access to and/or correction of personal health information; 26 (24.1 per cent) were about the collection, use and/or disclosure of personal health information; 19 (17.6 per cent) were self-reported privacy breaches by health information custodians; and four (3.7 per cent) were Commissioner-initiated complaints relating to collection, use or disclosure issues.

Of the 59 complaints closed about access to and/or correction of personal health information, 25 (42.4 per cent) were the result of deemed refusals (where a health information custodian fails to respond to a request within the statutory time frame and is thereby deemed to have refused the request); eight (13.6 per cent) were about whether a health information custodian had conducted a reasonable search for records of personal health information; seven (11.9 per cent) were about fees; three (5.1 per cent) were about the exemptions applied to deny access to personal health information; three (5.1 per cent) were about the exemptions applied to deny access along with other issues; two (3.4 per cent) were about the correction of personal health information; and two (3.4 per cent) were about custodians extending the time frame to respond to a request for access. Nine (15.3 per cent) involved other issues.

All 59 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 or more formal mediation. In one case, the IPC determined that an inquiry was not necessary as the health information custodian had taken all reasonable steps to respond to the complaint.

TYPE OF *PHIPA* COMPLAINT FILES OPENED IN 2005 AT THE IPC

Custodians, Agents and Others	Access/Correction	Collection, Use and/or Disclosure	Self-reported Breach	IPC-Initiated	Total
Total	75 (42.4%)	49 (27.7%)	35 (19.8%)	18 (10.1%)	177 (100%)
Public hospitals	13	17	13	4	**47 (26.6%)**
Doctors	22	6	0	1	**29 (16.4%)**
Clinics	6	4	1	3	**14 (7.9%)**
Ministry of Health	7	1	4	0	**12 (6.8%)**
CCACs	1	1	4	4	**10 (5.6%)**
Psychiatric facilities	5	3	0	0	**8 (4.5%)**
Independent facilities	7	1	0	0	**8 (4.5%)**
Laboratories	0	4	2	1	**7 (4.0%)**
Others, (including Agents)	14	12	11	5	**42 (23.7%)**

In the 49 other complaints resolved in 2005, the disclosure of personal health information was the most frequent issue, arising in 33 (67.3 per cent) complaints. Security of personal health information was an issue in seven (14.3 per cent). Consent for the collection, use and/or disclosure of personal health information was an issue in four (8.2 per cent). The collection of personal health information was an issue in three (6.1 per cent). Other issues that were raised included fundraising, privacy in general, disposal of personal health information, information practices, use of personal health information, and the conditions placed on the collection, use and disclosure of personal health information (i.e., lock-box issues).

As in the case of access to and/or correction complaints, the overwhelming majority of collection, use or disclosure complaints were resolved informally or through mediation. Of the 49 complaints closed in this category, the IPC issued an order in only one case (see the *High Profile Privacy Incidents* chapter in this annual report for details).

As mentioned previously, health information custodians self-reported a significant number of privacy breaches to the IPC. Although *PHIPA* does not require custodians to report privacy breaches to the IPC, the IPC was very pleased with this development. In these cases, the IPC was able to assist the health information custodians in meeting their obligations under *PHIPA* (for example, the requirement that patients be notified when their personal health information is stolen, lost or accessed by unauthorized persons). The IPC applauds health information custodians for their willingness to come forward and report breaches of *PHIPA* (these breaches most usually are unintentional or the result of theft). This underscores the positive working relationship that has developed between the IPC and health care professionals.

PERSONAL INFORMATION REQUESTS

Government institutions that submitted reports to the IPC reported 3,303 requests under *PHIPA* for access to, or correction of, personal health information were completed during 2005. The majority of these, 2,839, were completed by the Ministry of Health and Long-Term Care.

The ministry noted that with the advent of *PHIPA*, a large proportion of its access requests shifted to the new legislative regime; these requests for personal health information were previously filed under the *Freedom of Information and Protection of Privacy Act*.

The ministry reported completing 98 per cent of its 2,839 requests within the 30-day time period. As well, full access to the personal information sought was provided for 98 per cent of requests. The ministry did not charge fees for these access requests. (The ministry also reported completing 21,306 requests from third parties – with the consent of the individuals whose personal health information was involved – for disclosure of personal health information.)

Excluding the ministry, there were 464 requests under *PHIPA* completed by government institutions. Of these, 242 were completed by boards of health, 109 by health care practitioners, and 90 by ambulance services. Twenty-two were completed by homes or joint homes (designated as such under the *Homes for the Aged and Rest Homes Act*).

Of the 242 requests completed by boards of health, 231, or 95.5 per cent, were completed within 30 days, and of the remaining 11, nine of them within 60 days. Of the completed requests, 209, or 86.4 per cent, resulted in full access being provided. The provision of *PHIPA* used most often as the reason for full or partial denial of access was section 51(d) – prescribed personal health information – which permits a custodian to deny access to certain prescribed information. (Individuals may complain to the IPC when access is denied.) Fees were collected in 30 instances – a total of $299.60 was collected. There were no corrections requested.

Health care practitioners completed 109 requests, all but one of them within the statutory 30-day period, including 14 expedited requests that were completed within the requested time period. Full access was provided for all 109 requests. Eleven requests were subject to fees, totaling $490.

Of the 90 access requests completed by ambulance services, 89 (98.9 per cent) were within 30 days, with the remaining request being completed within 60 days. For 85 of the requests, or 94.4 per cent, full access was provided. Fees were charged for 18 requests (20 per cent) and $992.50 was collected.

Under *PHIPA*, health information custodians that are not institutions covered under one of the public sector access and privacy *Acts*, nor part of such an institution, are not required to report statistical information to the IPC. However, 48 of Ontario's **public hospitals** voluntarily filed statistical reports, which the IPC appreciates a great deal, as this has provided us with additional data that we are using to help gain insight into how the public used *PHIPA* in its first full year.

judicial reviews

In 2005, the Ontario Courts issued several decisions affirming the IPC's interpretation and application of the exemptions and procedural obligations under the *Freedom of Information and Protection of Privacy Act (FIPPA)* and the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*, and an important ruling on the IPC's role on judicial review.

ONTARIO COURT OF APPEAL DECISIONS

(1) The Court of Appeal issued two important rulings affirming the IPC's interpretation and application of the "advice to government" exemption (section 13) of *FIPPA*. These decisions have great significance for preserving and promoting open government and public accountability.

Both cases involved the disclosure of background information used by government agencies to make decisions concerning the expenditure of public funds. One case involved evaluation scores assigned by Ministry of Transportation staff to contractors bidding on highway construction projects. The other case involved evaluation reports prepared by Ministry of Northern Development and Mines staff which were used in making decisions to fund projects promoting tourism and development in Northern Ontario. In both cases, the IPC found that the relevant portions of the records were not exempt as "advice to government" under section 13 of the *Act* because their disclosure would neither reveal nor permit accurate inferences to be drawn concerning "a suggested course of action."

In dismissing their appeals from decisions of the Divisional Court, the Court of Appeal rejected the ministries' overly broad interpretation of "advice" as meaning simple "information or analyses conveyed with a view to influencing a decision." The Court stated that "the meaning of advice urged by the ministry would not be consonant with [the purpose of the statute]. The public's right to information would be severely diminished because much communication within government would fall within the broad meaning of advice, and s. 13(1) would not be a limited and specific exemption." The Court also held that the IPC was reasonable in finding that the specific information at issue in both cases was not exempt based on its own interpretation.

Finally, the Court of Appeal affirmed that the standard of review for the IPC's decisions on questions of statutory interpretation remains the deferential standard of "reasonableness." Among other factors cited by the Court was its view that these questions lie "at the core" of the IPC's expertise in striking a delicate balance between access and privacy rights. These rulings thus ensure that the Court will continue to defer to the IPC's expertise in interpreting and applying the exemptions from the right of access.

It should be noted that both ministries have sought leave to appeal these decisions to the Supreme Court of Canada.

(2) In another important case, the Court of Appeal dismissed an appeal from a Divisional Court decision upholding two IPC rulings on the exemptions for solicitor-client privilege at section 19 of *FIPPA* and personal privacy at section 21. The IPC found that neither exemption could be claimed by the Ministry of the Attorney General to withhold the amounts of legal fees it paid to lawyers representing two individuals in high profile cases involving serious criminal charges. Both Courts agreed that these exemptions did not apply and that records showing the amounts paid must be disclosed. The Court of Appeal stated that there is a presumption that the amount of legal fees paid is subject to privilege, but that this presumption can be rebutted where the amount would not reveal,

directly or indirectly, any communication protected by the privilege. The Court agreed with the IPC that disclosure of the amounts would not, in fact, reveal any protected communications in this case. The Court also agreed with the IPC that the amounts paid did not constitute "social service or welfare benefits" paid to the individual clients nor did they reveal any information about the "finances" of the clients or the lawyers who represented them. Since disclosure in this case would result in virtually no interference with anyone's privacy interests, the IPC was reasonable in holding that the amounts were not exempt under section 21.

(3) In a third case heard by the Court of Appeal, the IPC's right to actively participate in judicial reviews of its decisions was again upheld. The Children's Lawyer for Ontario (CLO) applied for judicial review of the IPC's decision that it could not rely on "Crown counsel privilege" at section 19 or the "advice to government" exemption at section 13 to withhold records from its own client, who was a minor represented by the CLO in child protection and other proceedings. In the course of the judicial review, the CLO challenged the IPC's right to file written arguments or make oral submissions, claiming this would compromise the IPC's impartiality in future cases. The Divisional Court upheld the IPC's decision and dismissed the CLO's motion to deny the IPC standing before the Court. The CLO appealed the Court's ruling on the standing issue, but not its ruling on the exemptions.

The Court of Appeal held that the IPC's participation in this case ensured a fully informed adjudication of the issues, especially given the lack of participation by the requester in the judicial review proceedings. It stated that the IPC's expertise and public interest role, together with the nature of the issues raised under the statute, "suggest that the impartiality consideration was not a significant brake on full standing for the Commissioner." Not only did the Court permit the IPC full standing, it found that the IPC's counsel could properly raise a new argument in support of the decision which was not explicitly set out in the IPC's original reasons. The Court's decision has attracted considerable interest for its clarification of the standing of tribunals in applications for judicial review of their own decisions.

DIVISIONAL COURT DECISIONS

(4) In a case involving the Ontario government's purchase and sale of an aerospace company, de Havilland Inc., the Divisional Court upheld the IPC's approach to contracts under the third party information exemption. The Ministry of Economic Development and Trade had denied access to three requested contracts, in part on the basis of section 17 of *FIPPA*. On appeal, the IPC stated that information in a contract will not normally qualify for exemption under section 17 because the exemption requires that the information be "supplied" to the government, as opposed to negotiated between the government and an outside party. The IPC ruled that, in the circumstances of this case, there was insufficient evidence to establish that the information in the contracts was supplied rather than negotiated. Two affected parties applied for judicial review of the IPC's decision.

The Divisional Court endorsed the IPC's general approach to contracts. Further, the Court held that the IPC acted reasonably in finding that, in the circumstances, the contracts did not qualify for exemption under section 17 because they had been negotiated rather than supplied. One of the affected parties applied to the Ontario Court of Appeal for leave to appeal the Divisional Court's decision. The Court of Appeal dismissed the leave application.

(5) In the continuation of a case first heard in 2002, the Divisional Court upheld the IPC's decision that certain records relating to security for the Premier should not be disclosed. The requester had sought access to information relating to the Ontario Provincial Police security detail that accompanied the Premier on trips to the United States. The Ministry of the Solicitor General denied access to the information, in part on the basis of the "danger to life or physical safety" exemption in section 14(1)(e) of *FIPPA*. On appeal, the IPC found that certain information revealing summary expense information was not exempt and should be disclosed. However, the IPC held that

the remaining information should not be disclosed, on the basis that disclosing the size of the Premier's security detail could reasonably be expected to endanger the life or physical safety of government officials. The requester applied for judicial review to the Divisional Court.

The Divisional Court held that the IPC acted reasonably in finding that the exemption applied, even though the records related to a predecessor of the current Premier. The requester applied to the Ontario Court of Appeal for leave to appeal the Divisional Court's decision. The Court of Appeal dismissed the leave application.

(6) In one case involving a procedural issue, the Divisional Court upheld the IPC's ruling that the City of Toronto had conducted a reasonable search for records responsive to a request. The requester had sought access to records relating to alleged dog attacks. The city conducted a search and advised the requester that it had no responsive records. Later, the city conducted an additional search and located a number of records. On appeal, the IPC ruled that the city's search for responsive records was reasonable in the circumstances. The Divisional Court dismissed the requester's application for judicial review, finding that the Commissioner's decision was "reasonable." The Court also characterized the requester's application as "frivolous and vexatious" and a "collateral attack on matters previously decided."

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

OUTSTANDING JUDICIAL REVIEWS AS OF DECEMBER 31,2005: 28

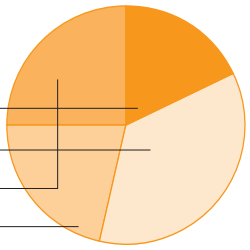
Launched by:

Institutions 6

Requesters/complainants 12

Institution & other party 4

Affected parties 6



NEW JUDICIAL REVIEW APPLICATIONS RECEIVED IN 2005: 14

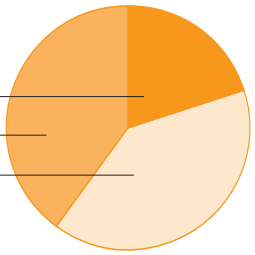
Launched by:

Institutions 3

Requesters 5

Affected parties 6

Complainants n/a



JUDICICAL REVIEWS CLOSED/HEARD IN 2005: 21

Abandoned (Order stands)[1] 4

Heard but not closed (decision pending)[2] 4

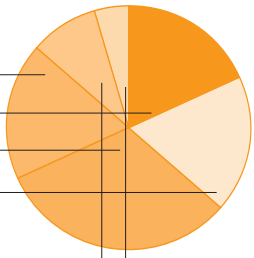
IPC Order upheld[3] 6

IPC Order upheld(appeal pending)[4] 4

IPC Order not upheld n/a

Dismissed for delay (Order stands)[5] 2

Appeal on procedural motion dismissed (further appeal pending)[6] 1



1 *Abandoned (Order stands): MO-1811, MO-1847, MO-1900-R, PO-2206*

2 *Heard but not closed (decision pending): MC-030028-1 and MC-030043-1, MC-030029-1 and MC-030029-2, MO-1892, PO-1664*

3 *IPC Order upheld: PO-1809, PO-1810, PO-2226, PO-1922, PO-1952, PO-2006*

4 *IPC Order upheld (appeal pending): MO-1844, PO-1993, PO-2028, PO-2084*

5 *Dismissed for delay (Order stands): P-1213, PO-2175-R*

6 *Appeal on procedural motion dismissed (further appeal pending): PO-1905*

working together

As part of its Institutional Relations Program, the IPC's Tribunal Services Department works collaboratively with selected municipal and provincial organizations as part of its ongoing efforts to:

- gain a better understanding of the business of the department's institutional clients in order to deal more effectively with appeals and complaints filed with the IPC; and
- provide IPC mediators and institutional staff with an opportunity to better understand each other's roles and needs, and thus develop more productive relationships.

During 2005, the IPC was asked by various institutions to attend their meetings to speak to their staff. Among these sessions were the following:

FREEDOM OF INFORMATION POLICE NETWORK

The IPC accepted an invitation from the Freedom of Information Police Network to have senior staff speak at both its spring and fall meeting/training workshops. These sessions were attended by freedom of information and privacy co-ordinators and their staff from local police services across the province and from the Ontario Provincial Police. As part of these sessions, the IPC team gave presentations on *video surveillance* and on the issue of *retention of fingerprints and photographs for non-conviction dispositions*, as well as providing an overview of the new *Personal Health Information Protection Act (PHIPA)*.

CITY OF TORONTO

At the request of the city clerk, the Commissioner and senior staff attended a meeting of all city managers and division heads. The Commissioner made a presentation on the importance of promoting a culture of openness and transparency in government and outlined key portions of her order, MO-1947, which dealt with four related FOI requests that the City of Toronto had denied. (See the article, *Building a Culture of Openness in Government*, in the *Issues* section of this annual report.) In her presentation, the Commissioner focused on accountability and the underlying principles of the public sector legislation.

ONTARIO PROVINCIAL POLICE

The Assistant Commissioner (Access) made a presentation at an Ontario Provincial Police training session in Orillia. Among those attending were OPP freedom of information liaison officers and staff members in the field who are responsible for responding to freedom of information requests. This opportunity was used to promote a culture of openness, explain the role and mandate of the IPC, and the importance of mediation, using the IPC enhanced mediation model. It was also an opportunity to learn about the roles and challenges faced by the OPP staff.

PHIPA SHORT NOTICES

Among other examples of the IPC, in this case, the Legal Department, and other organizations working together in 2005, was the *PHIPA* short notices working group.

Many notices about individuals' rights under new privacy laws are dense tombs packed with legal jargon and seemingly endless clauses and sub-clauses which very few people actually read. At Commissioner Ann Cavoukian's ini-

tiation, a joint task force was launched in the fall of 2004 to develop short but effective notices for *PHIPA*.The working group, which included the IPC, the Ontario Bar Association's Privacy and Health Law sections, the Ministry of Health and Long-Term Care, and the Ontario Dental Association, developed three sets of posters and brochures (for hospitals, the offices of medical practitioners, and long-term care facilities), which were released in June 2005 by the IPC.

These colourful posters, backed up by the more detailed but easily readable brochures, were an immediate hit. By the end of 2005, more than 325,000 of the IPC's posters and brochures were on display or being given out in medical offices, hospitals, and long-term care facilities across Ontario.

Outreach program

One of the core responsibilities of the IPC is to educate the public about Ontario's access and privacy laws. In order to accomplish this task, and to increase the public's awareness of access and privacy issues, the IPC has a multi-layered outreach program.

Many elements of the outreach program, from speeches to publications, to the *Reaching Out to Ontario* program, focused in 2005 on Ontario's new health privacy law, the *Personal Health Information Protection Act (PHIPA)*, which came into effect Nov. 1, 2004.

Commissioner Ann Cavoukian and senior staff made a series of presentations to health professionals and other organizations. In addition, the IPC produced a plethora of special publications – some aimed at health professionals, others at the public – as well as sponsoring a highly successful *PHIPA Summit* in Toronto in November. The *Summit*, hosted by the Commissioner, attracted about 300 health professionals. It included a number of sessions reviewing key areas of the law, issues that had come up during the first year, and best practices.

The IPC's *Reaching Out to Ontario (ROTO)* program was extensively revised in 2005 to focus on *PHIPA*. Under *ROTO*, an IPC team visits three or four Ontario cities or regions each year for a series of presentations and seminars. In 2005, IPC teams visited Halton Region, Durham Region, and Timmins. A presentation to area health professionals on *PHIPA* was a key part of all three educational initiatives. Copies of the IPC's *PHIPA* publications were given out at an information table at area malls and – for the final two initiatives, Durham Region and Timmins – an IPC information table was also set up at an area hospital during the visit, which proved to be very popular. Other aspects of the *ROTO* initiatives, including briefings/interviews with area media, also focused on the new health privacy law.

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

- the public speaking program, led by the Commissioner;
- the *What Students Need to Know about Freedom of Information and Protection of Privacy* school program;
- the publications program;
- the media relations program; and
- the IPC's extensive website.

SPEECHES AND PRESENTATIONS

In 2005, Commissioner Cavoukian gave 35 keynote or special presentations at major conferences and workshops to a diverse group of organizations in the public, private and academic sectors. The major themes that the Commissioner focused on included the protection of personal health information, living up to the underlying principles of freedom of information, identity theft, and the need for businesses to treat the protection of their clients' personal information as a bottom-line issue.

Among the presentations the Commissioner made in 2005 were those to: Harvard University, the Kennedy School of Government, the University of Toronto Faculty of Law, and the Rotman School of Business, the 27th annual

International Conference of Privacy and Data Commissioners, the Canadian Information and Privacy Commissioners' Annual Summit, the International Association of Privacy Professionals, the Council of Senior Security Executives, the Ontario Bar Association, the Sunnybrook and Women's College Health Sciences Centre, the Toronto Board of Trade, the Canadian Information Processing Society and the Canadian Wireless Telecommunications Association.

Among the other segments of the IPC's speakers' program are:

- a university program, where members of the IPC's Legal and Policy Departments make presentations to faculty and students in business and law programs;
- a media program, under which the IPC's Communications Co-ordinator addresses university and college journalism and electronic media classes. Presentations are also made to editorial boards or newsroom staff on the role of the IPC and access and privacy issues; and
- a general public speaking program, where IPC staff make presentations on access and privacy to various groups or organizations.

SCHOOLS PROGRAM

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

The three teachers' guides, which were developed by the IPC with the aid of curriculum experts and classroom teachers – and brochures that describe the guides – are available on the IPC's website in the *Resources* section.

Since the IPC's schools program was launched in 1999, with the release of the guide for Grade 5 teachers, more than 30,000 copies of the guides have either been sent to teachers or downloaded from the IPC's website.

IPC PUBLICATIONS

The IPC released 25 publications on access or privacy topics in 2005, including 16 papers, brochures and fact sheets on *PHIPA*. These included the *Privacy Impact Assessment Guidelines for the Personal Health Information Protection Act*, a self-assessment tool developed by the IPC to assist health information custodians in reviewing the impact that a proposed information system, technology or program may have on the privacy of individuals' personal health information.

Among other 2005 publications are the *Secure Destruction of Personal Information,* a fact sheet that includes suggested best practices for the destruction of personal information, and the *Disclosure of Information Permitted in Emergency or other Urgent Circumstances*, a fact sheet that explains that the protections provided by access and privacy legislation are not intended to stand in the way of the disclosure of vital – and in some cases, life-saving – information, in emergency or other urgent situations

Identity Theft Revisited: Security is Not Enough, a major policy paper released in the fall, stresses that the single largest cause of ID theft is poor information management practices by organizations that collect, use or store personal information. Two brochures, *Identity Theft: Business Take Note: Steps to Protect Customer Personal Information,* and *Identity Theft: How to Protect Yourself*, were released along with the policy paper.

A complete list of the IPC's 2005 publications is in the section that follows this *Outreach* report.

MEDIA RELATIONS

Through its proactive media relations program, the IPC tries to raise the media's consciousness about 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 staff also answer media inquiries relating to freedom of information, protection of privacy, and the *Personal Health Information Protection Act.*

The Commissioner gave 81 media interviews in 2005, to media organizations that ranged from small community radio stations to the largest daily newspapers and television and radio networks in Canada. She was also interviewed by a number of international media, including the *New York Times.* Overall, the IPC assisted more than 200 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 17 news releases in 2005.

IPC WEBSITE

The IPC website (**www.ipc.on.ca**) offers a plethora of information about access and privacy issues and the legislation that applies. It provides answers to frequently asked questions, access to IPC publications and orders, links to copies of the *Acts* (including the new *PHIPA*), educational material, news releases, selected speeches, other presentations by IPC staff, forms and more.

Further details about the IPC website are cited in a separate report on the website (which follows the *Publications* report).

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 released in 2005, in chronological order, included:

- *Safeguarding Personal Health Information* (fact sheet);
- *Your health information: Your access and correction rights* (fact sheet);
- *Ontario Regional Poison Information Centres and the 'Circle of Care'* (fact sheet);
- *Reporting Requests under PHIPA* (fact sheet);
- The spring 2005 edition of the biannual newsletter, *IPC Perspectives*;
- *Consent and Form 14* (fact sheet);
- *Fundraising under PHIPA* (fact sheet);
- *Your Health Information and Your Privacy in Our Office* (brochure) and accompanying poster, *Health Information Privacy in our Office;*
- *Your Health Information and Your Privacy in Our Hospital* (brochure) and accompanying poster, *Health Information Privacy in our Hospital*;
- *Your Health Information and Your Privacy in Our Facility* (brochure) and accompanying poster, *Health Information Privacy in our Facility*;
- The Commissioner's 2004 annual report;
- *Disclosure of Information Permitted in Emergency or other Urgent Circumstances* (fact sheet);
- *Lock-box Fact Sheet*;
- *Fact Sheet on Adoption Information Disclosure*;
- *A Review of the Literature on Adoption-Related Research: The Implications for Proposed Legislation*;
- *Alert for Birth Parents*;
- *Identity Theft Revisited: Security is Not Enough*;
- *Identity Theft: Business Take Note: Steps to Protect Customer Personal Information* (brochure);
- *Identity Theft: How to Protect Yourself* (brochure);
- *Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act*;
- The fall 2005 edition of *IPC Perspectives*;
- *Long-term Care Homes: Consent and Access under the Personal Health Information Protection Act, 2004* (fact sheet).
- *PHIPA Practice Direction 1: Clarifying Access Requests*;
- *PHIPA Practice Direction 2: Drafting a Letter Responding to a Request for Access to Personal Health Information*;
- *Secure Destruction of Personal Information* (fact sheet).

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.

website resources

THE IPC'S WEBSITE, WWW.IPC.ON.CA, A MAJOR EDUCATIONAL RESOURCE, IS ONE OF THE IPC'S KEY COMMUNICATIONS TOOLS.

It continues to attract an increasing number of visitors each year and the number of downloads keeps climbing quickly.

There were 313,951 downloads in 2005, a 34 per cent increase over 2004 (234,352), and a dramatic 158 per cent increase from 2003 (121,807).

With a significant increase in the number of IPC papers, orders, tools and other information posted to the site, and the increase in general traffic, the IPC began redesigning its website in early 2006.

Six *Personal Health Information Protection Act (PHIPA)* publications were among the top 10 downloaded files in 2005. Overall, nearly one-fifth (17.91%) of the 313,951 downloaded files were health-related publications.

A Guide to the Personal Health Information Protection Act (20,422) replaced the *Privacy Diagnostic Tool (PDT)* as the most downloaded file of the year. The *PDT* had been the most downloaded file for three consecutive years. The second most downloaded file was the *2004 Annual Report* (19,768), followed by *Identity Theft Revisited: Security is Not Enough* (at 13,104).

In 2005, the *PDT* was downloaded 5,565 times, but it narrowly missed the top 10, with the increased activity on the IPC's website.

Other popular resources downloaded in 2005 included *Guidelines for Using RFID Tags in Ontario Public Libraries* (11,281 downloads); HO-001 (the first *PHIPA* order, 8,689); the *Commissioner's PHIPA Highlights: Here's what health professionals are asking about Ontario's new health privacy legislation* (8,282); the *Lock-box Fact Sheet* (6,411); the *Privacy Impact Assessment Guidelines for the Personal Health Information Protection Act* (6,403, in less than two months after being posted in November); *Disclosure of Information Permitted in Emergency or other Urgent Circumstances* (6,015) and *Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology* (5,927).

If you have any comments about the content of the IPC website, please forward them to **info@ipc.on.ca**.

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 2005:

PROVINCIAL CONSULTATIONS

Ministry of Citizenship and Immigration:

- Collaborative Seniors Portal Network;

Ministry of Community and Social Services:

- Bill 183, the *Adoption Information Disclosure Act, 2005;*

Ministry of Community Safety and Correctional Services:

- Bill 28, *Mandatory Blood Testing Act*;

Ministry of Government Services:

- Bill 197, *Budget Measures Act, 2005* (amendments to the *Freedom of Information and Protection of Privacy Act,* including making universities subject to the *Act*);
- Integrated Birth Registry;
- Public sector outsourcing;

Ministry of Labour:

- Bill 190, Amendments to the *Occupational Health and Safety Act*;

Ministry of Municipal Affairs and Housing:

- Bill 53, S*tronger City of Toronto for a Stronger Ontario Act, 2005*;

Ministry of Training, Colleges and Universities:

- Bill 197, *Private Career Colleges Act, 2005*;

Ministry of Transportation:

- Disabled Persons' Parking Permit Program;

Democratic Renewal Secretariat:

- Bill 213, *The Election Statute Law Amendment Act, 2005*;

Liquor Control Board of Ontario:

- Video surveillance in LCBO stores.

MUNICIPAL CONSULTATIONS

Toronto Police Services Board:

- In-car video surveillance;

Toronto Transit Commission:

- Video surveillance pilot project.

MULTIPLE-LEVEL CONSULTATIONS

- The Commissioner and her staff met with representatives from the Toronto Police Service, the Toronto Police Services Board, the Ontario Association of Chiefs of Police, and RCMP officials from the Canadian Criminal Records Information Services to discuss police retention of fingerprints, photos and other personal information of those charged with a crime but not convicted.

HEALTH INFORMATION CUSTODIANS CONSULTATIONS

Note: 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 regulating colleges, Cancer Care Ontario, the Canadian Institute for Health Information, the Institute for Clinical Evaluative Sciences, the Pediatric Oncology Group of Ontario, the Cardiac Care Network of Ontario, the Information System for Cytology, the London Health Sciences Centre (Ontario Joint Replacement Registry), the Canadian Stroke Network, the Ontario Hospital Association, individual hospitals and many more.

Ministry of Health and Long-Term Care:

- Client Registry and Identification Management;
- Emergency Department Access to Drug History Project;
- Provincial Diagnostic Imaging Picture Archiving and Communications System;
- Ontario Laboratory Information System;
- Integrated Public Health Information System.

INDIRECT COLLECTIONS

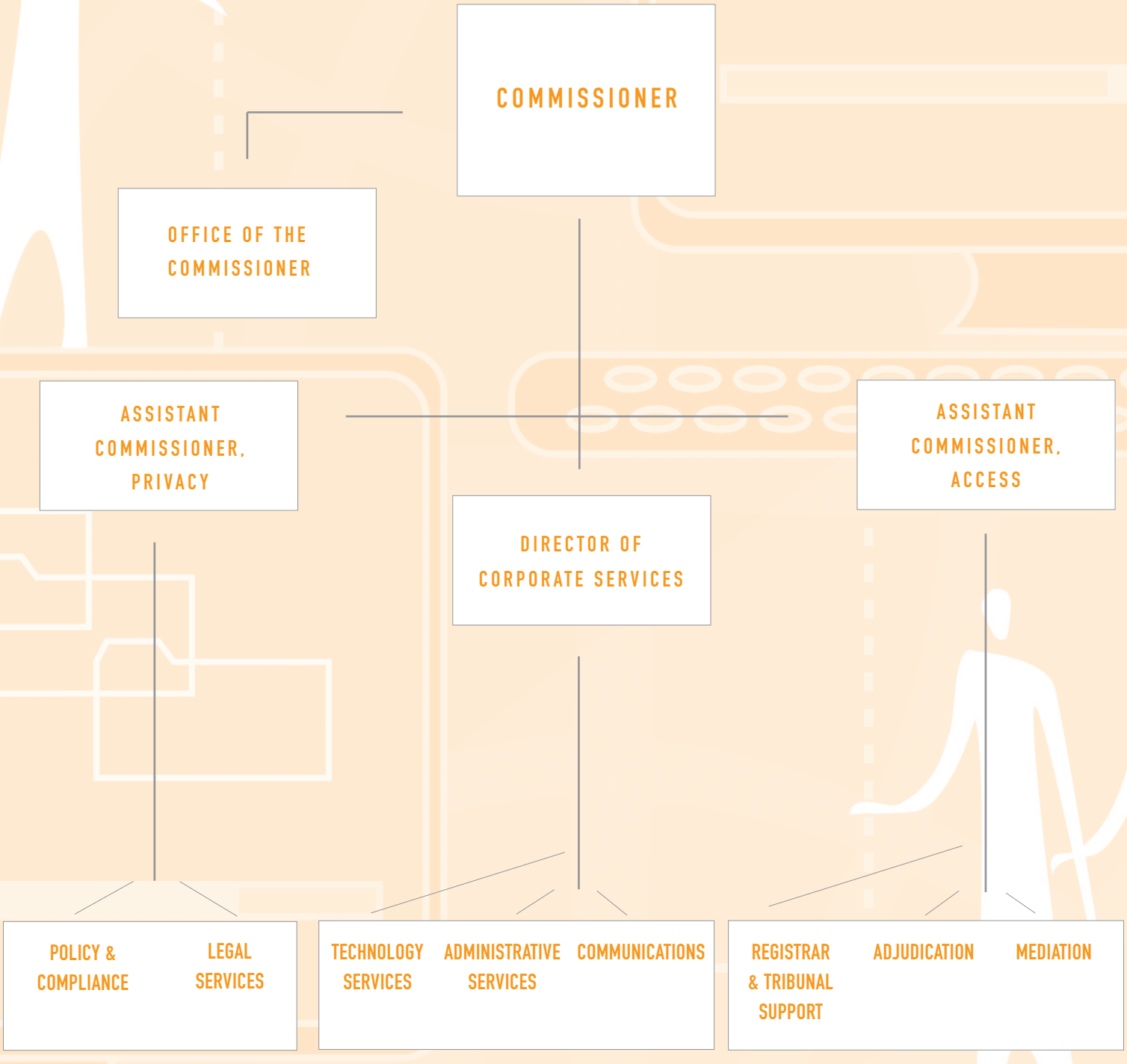
Ministry of Transportation:

- Roadside memorials (Mothers Against Drunk Driving).

SUBMISSIONS AND SPECIAL REPORTS

- *Submission to the Toronto Police Services Board regarding the board's policy for the destruction of adult fingerprint, photograph and criminal history records;*
- *Submission to the Chair of the Standing Committee on Social Policy regarding Bill 118, the Accessibility for Ontarians with Disabilities Act, 2004;*
- *Submission to the House of Commons Standing Committee on Justice, Human Rights, Public Safety and Emergency Preparedness regarding Bill C-13, which expands the federal DNA databank regime;*
- *Submission to the House of Commons Subcommittee on Public Safety and National Security regarding the Anti-Terrorism Act Review;*
- *Submission to the Minister of Justice and Attorney General of Canada on 2005 'Lawful Access' Consultations;*
- *Submission to the Standing Committee on Social Policy on Bill 183: the Adoption Information Disclosure Act, 2005;*
- *Submission to the Standing Committee on Regulations and Private Bills - Bill 123: Transparency in Public Matters Act, 2004.*

organizational chart



financial statement

	2005-06 Estimates $	2004-05 Estimates $	2004-05 Actual $
Salaries and wages	7,904,000	6,543,300	6,270,287
Employee benefits	1,699,400	1,648,000	1,235,140
Transportation and Communications	255,400	300,000	238,881
Services	1,492,000	1,733,400	1,349,472
Supplies and Equipment	374,900	533,900	736,067
Total	**11,725,700**	**10,758,600**	**9,829,847**

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

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

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, 2005.

APPENDIX 1

Name	Position	Earnings	Taxable Benefits
Cavoukian, Ann	Commissioner	$178,667.60	$301.84
Anderson, Ken	Assistant Commissioner, Privacy	$187,406.32	$290.52
Beamish, Brian	Assistant Commissioner, Access	$180,462.78	$285.36
Challis, William	General Counsel	$178,782.62	$290.52
Faughnan, Steven	Adjudicator	$109,894.65	$99.76
Geisberger, Janet	Director, Corporate Services	$107,585.09	$176.24
Goldstein, Judith	Legal Counsel	$156,031.48	$255.50
Goodis, David	Legal Counsel	$163,751.99	$266.52
Hale, Donald	Adjudicator	$103,078.90	$164.19
Higgins, John	Manager, Adjudication	$164,196.94	$266.88
McCammon, Stephen	Legal Counsel	$116,201.02	$0.00
Morrow, Bernard	Adjudicator	$109,587.36	$156.44
O'Donoghue, Mary	Manager, Legal Services	$166,448.00	$276.36
Senoff, Shirley	Legal Counsel	$107,789.71	$179.57
Swaigen, John	Adjudicator	$164,196.94	$266.88

Information & Privacy Commissioner/Ontario

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

Tel: 416 326 3333
Fax: 416 325 9195
Website: www.ipc.on.ca

1 800 387 0073
TTY: 426 325 7539