ACCESS & PRIVACY

THE CHALLENGES AND OPPORTUNITIES

INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO
2008 ANNUAL REPORT

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

May 13, 2009

The Honourable Steve Peters
Speaker of the Legislative Assembly

I have the honour to present the 2008 Annual Report of the Information and Privacy Commissioner of Ontario to the Legislative Assembly.

This report covers the period from January 1, 2008 to December 31, 2008.

Sincerely yours,

Ann Cavoukian, Ph.D.
Commissioner

Enclosure

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

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

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

Commissioner's Message

There were significant advances in both access and privacy in 2008. On the privacy front, the events of the past year prompted me to revisit a concept I had developed some time ago – *Privacy by Design* – with a view to sharpening my focus.

The Evolution of Privacy

In the two decades that I have served as a privacy regulator, I have continually attempted to refine my views, approaches and methods of advancing privacy – and 2008 proved to be a milestone. Contrary to what some may think, privacy is not a static construct, but an evolving one, subject to changes in society and technology. In 2008, I challenged myself to think about privacy differently, resulting in the development of a new concept – one I am calling PETs *Plus* or *Transformative Technologies*.

This transformation, or perhaps a refinement of an earlier one, began in the autumn of 2007, after Toronto's mass transit system (the TTC) announced its plans for an expansion of its video surveillance program. The announcement resulted in a formal complaint to my office from Privacy International, a U.K.-based organization, citing concerns with the TTC's proposed expansion as a violation of privacy laws. In response to Privacy International's complaint, I launched an investigation and subsequently released, *Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report*, in which I ruled that the TTC's expansion of its video surveillance system, for the purposes of public safety and security, did not contravene any applicable privacy laws. In lockstep with this ruling, however, I called upon the TTC to undertake a number of specific measures to significantly enhance privacy protection. The TTC is implementing all of my recommendations, which will result in what I believe is the world's most privacy-protective system of mass transit.

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

This investigation report has been hailed by experts as a blueprint to embed privacy into surveillance programs in mass transit systems in other countries. *(See the article on page 5.)*

As part of our investigation report, I strongly encouraged the TTC to conduct a pilot project to test the use of a privacy-enhancing video surveillance technology, developed by researchers at the University of Toronto, Professor Kostas Plataniotos and Karl Martin. It was this exciting project that lead me to develop the concept of *Transformative Technologies*.

Back in the 1990s, when I first coined the term *Privacy by Design*, it was to advance the view that technology need not be an inherent threat to privacy – instead, its support could

be enlisted to *protect* privacy by embedding privacy into its design. While it is certainly the case that privacy can be eroded by technology, technology may also be designed to safeguard personal information through the use of *Privacy-Enhancing Technologies (PETs)* or, as I am now calling it, *PETs Plus*. When applied to technologies of surveillance, *PETs* can serve to literally transform an otherwise invasive technology into one that is protective of privacy, hence the term, *Transformative Technologies*. I use the word *transformative* because I believe that technology has evolved to the point where it now has the ability to protect our privacy while performing whatever function it was designed to serve – but only if privacy is embedded directly or built right into the architecture at the design stage, hence the term, *Privacy by* ***Design***.

Moreover, I also believe that with the advent of *Transformative Technologies*, we now have the opportunity to lay to rest the "zero-sum" mindset which has prevailed over the relationship between technology and privacy. No longer must we subscribe to the mentality that in order to enhance security, we must sacrifice privacy, or vice versa. I am urging that we move forward to a "positive-sum" paradigm, whereby adding privacy measures to technologies such as surveillance systems need not weaken security or functionality but quite the opposite – it may in fact enhance the overall design, resulting in a "win/win" scenario. By adopting a positive-sum paradigm, we can literally transform technologies normally associated with surveillance into ones that are no longer privacy-invasive – serving to minimize the unnecessary collection, use and disclosure of personal data, and promoting public confidence and trust. The future of privacy may depend on it.

Protecting Youth Online

Since 2005, my office has been proactively involved in reaching out to educate and inform our youth (and the public) of the potential dangers of engaging in online activities. Online social networking has progressed well beyond the point of being a passing fad – it has become the preferred way that millions of people choose to communicate, socialize and interact, on a daily basis. As with most innovations that have a major impact on the lives of a vast number of people, there can be serious, unexpected results if users, particularly the young, are not made aware of the potential implications. There is widespread concern that young people do not understand the privacy risks associated with revealing too much information about themselves online, ranging from cyberbullying, identity theft and Internet luring, to jeopardizing future job prospects.

In 2008, we continued our work with Facebook, one of the largest social networking sites, producing a video entitled, *Be A Player: Take Control of Your Privacy on Facebook*, in which I discuss the problems associated with weak privacy settings, and the protections students should be aware of when posting their personal information online. Further, my office also had the privilege of being involved in the launch of the first Toronto chapter of Teenangels, an organization consisting of 13 to 18-year-old volunteers who deliver programs in schools – intended to spread the word about responsible and safe surfing – to their peers, parents, and teachers.

We also hosted our first youth conference, *Youth Privacy Online: Take Control, Make it Your Choice!* – which brought together professionals from a diverse range of public and private sector organizations. The conference provided a forum for discussion and debate that focused on exploring a variety of approaches to safeguarding the privacy of children and youth on the Internet. I was delighted to be given the "Privacy Hero and Leadership Award," for helping to keep children safe in Ontario, by WiredSafety – one of the world's oldest and largest cybersafety organizations. Thank you very much!

Right to Know Week

My office marked Canada's third annual *Right to Know Week* in the early fall with three separate initiatives:

- a major event: a sold-out luncheon based on the theme of *Breaking Down Barriers to Freedom of Information: Ensuring the Public's Right to Know*;
- a special *Right to Know Blitz Day*, where IPC staff set up information tables in three Ontario cities to hand out IPC publications and answer questions from the public; and
- a special *Right to Know* section on our website which includes information about people's rights under Ontario's freedom of information laws and how to file a freedom of information request or appeal.

I employed these three tools because I wanted to reach as many people as possible to increase Ontarians' awareness of their access rights. I cannot stress highly enough the importance of freedom of information to our society. If citizens are to participate meaningfully in the democratic process and hold politicians and their governments accountable, they must have timely access to the information held by their government.

Access to Information

An access issue that I focused on in last year's Annual Report has led to a very positive outcome. I had urged police services across Ontario to recognize the intent of a then-recent legislative change by giving it a broad and generous interpretation, thereby allowing family members of a deceased person to obtain information regarding the circumstances of his or her death. From the time that we first drew attention to this issue – with my comments and a recommendation in the 2007 Annual Report, and through other educational efforts – there has been a major decrease in the number of appeals to my office related to this issue. We have seen examples of creative approaches to releasing this information, for which I applaud the police.

My Personal Thanks

As always, I would like to give my sincere thanks to all of my staff, whose dedication and hard work has made this office a first-class agency, and whose work is now well-known on a global scale. Our success is made possible by the passion and enthusiasm shown by the dedicated team who work here. I truly believe that the people of Ontario are very fortunate to have such talented professionals working on their behalf. I truly have the best team, for which I am very grateful. My heartfelt thanks to all of you!

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner

TABLE OF CONTENTS

Privacy Expert, Professor Fred Cate, says:

Commissioner's investigation report into Toronto's mass transit system 'will be invaluable to municipalities throughout the world'

Commissioner Cavoukian issued a special privacy investigation report in March 2008 on the use of video surveillance cameras in mass transit systems. While the investigation arose out of a complaint that the Toronto Transit Commission's (TTC) planned expansion of its video surveillance system contravened the privacy provisions in the *Municipal Freedom of Information and Protection of Privacy Act*, the Commissioner decided to broaden the investigation to include a review of the literature relating to the effectiveness of video surveillance programs and an examination of the role that privacy-enhancing technologies can play in mitigating the privacy-invasive nature of video surveillance cameras.

The report's sweeping recommendations include a set of strong privacy controls that render the TTC into one of the most privacy-protective transit systems worldwide. (The TTC has agreed to implement all of the Commissioner's recommendations.) The Commissioner's report has been recognized by well-known scholars and privacy experts as a seminal piece, that will be referenced worldwide as a practical model that meets both the need for public safety and respect for individual privacy.

As noted in correspondence from Fred Cate, Distinguished Professor at the Indiana University School of Law-Bloomington, and Director of the Indiana University Center for Applied Cybersecurity Research, "The report will be invaluable to municipalities throughout the world which are facing similar vexing questions about the proper use and management of video surveillance technologies. Your recommendations provide a principled yet workable model for how to protect individuals' legal and moral right to privacy, while also advancing the public's interest in safe, efficient, and affordable public infrastructure."

Prof. Cate, who specializes in privacy, security, and other information law issues, and appears regularly before Congress, is a member of the U.S. National Academy of Sciences' Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and other National Goals. He advised the IPC that he has recommended the Commissioner's report to the Department of Homeland Security as a best practice framework.

What makes the Commissioner's recommendations most notable is their scope. Among them: she called for an independent third party audit of the program, and asked the TTC to reduce its retention period for the video images obtained

from seven days to a maximum of 72 hours. In addition, the Commissioner called for very senior sign-off (by the Chief of Police or his designate) should access to specific video footage be required by the Toronto Police Service.

As Murray Long, editor and publisher of *PrivacyScan*, a leading Canadian privacy publication, notes of the IPC's investigation report: "It sets the benchmark for informed discussion of CCTV in mass transit systems such as Toronto's. It provides a road map for the most privacy-protective approach to CCTV. It offers potential technological solutions that can further enhance privacy with CCTV imagery. It presents specific recommendations and a requirement for an independent third-party audit of how they are introduced – this is the Commissioner flexing her muscles. Finally, it demonstrates that Canadian privacy laws have the capacity to meet technological challenges such as CCTV and that good system design, vigilant oversight and a commitment to privacy values can result in 'positive-sum models' as Commissioner Cavoukian describes them."

And *Privacy Journal*, a respected U.S. newsletter on privacy in the computer age, cited the Commissioner's seminal work in this area in its December 2008 edition in one of its 13 recommendations to the new U.S. administration to enhance the privacy protections of Americans. The fourth recommendation states:

> "provide guidelines and "best practices" for municipal and private sector camera surveillance, modeled after the protocols in Toronto and elsewhere in Canada;"

Another distinguished U.S. academic, Daniel J. Solove, Associate Professor of Law, George Washington University Law School, noted: "The report is a valuable step forward toward ensuring that video surveillance be carried out in ways that ensure that privacy is protected and that oversight exists."

The Commissioner's report also drew attention to a privacy-enhancing technology that could ultimately be embedded into the design of the Toronto system and far beyond – the innovative work of a University of Toronto team in the area of privacy-protected surveillance. They are focusing on secure visual object coding that uses cryptographic techniques to "encrypt" personally identifiable visual data – such as faces – from the video record while leaving intact the other visual details in the frame. People moving through an area can be viewed in real-time without their identities being revealed. If a situation from a crime scene occurs that requires identifying someone (e.g., a suspect or victim), then this encrypted data may be "decrypted," using a special cryptographic key held by designated authorities for that purpose.

The Commissioner's TTC investigation report "provides a road map for the most privacy-protective approach to CCTV." – Murray Long

"Adding privacy measures to surveillance systems need not weaken security or functionality but rather, could enhance the overall design," said Commissioner Cavoukian. "A positive-sum paradigm appropriately describes this situation in which participants may all gain together. To achieve this, privacy must be proactively built into the system."

In the 90s, the Commissioner coined the term "Privacy by Design," where privacy protections are engineered directly into the technology, right from the outset. "The University of Toronto's project, when applied to a mass transit application, is what I am now calling "Transformative Technologies," said Commissioner Cavoukian. "These privacy-enhancing technologies can literally transform technologies normally associated with surveillance into ones that are no longer privacy-invasive, serving to minimize the unnecessary collection, use and disclosure of personal data and promoting public confidence and trust in data governance structures such as the TTC."

The Commissioner's report "will be invaluable to municipalities throughout the world." – Professor Fred Cate

2008: Year of Transformative Technologies

In 2008, Commissioner Cavoukian built upon her *Privacy by Design* approach to enlarge understanding and expand the development of *Privacy-Enhancing Technologies (PETs)* in Ontario, and well beyond.

In an effort to overcome the prevailing zero-sum (win-lose) thinking relating to privacy vs. security, the Commissioner is seeking a paradigm shift. She is asking that a positive-sum (win-win) approach be taken wherein privacy *and* security can both prevail.

When a positive-sum paradigm is applied to privacy, the commonly held view that privacy is an obstacle that must be sacrificed when pursuing other desirable business or technical goals can be discarded. Examples would be surveillance, fraud detection, public security, system functionality, performance, and accountability. Protecting privacy need not involve any trade-offs. Done right, you can have both in a win-win scenario.

Privacy by Design, an approach developed in the 90s by Commissioner Cavoukian, seeks to build privacy early and systematically into information technologies, systems and architectures.

Applied to privacy-invasive realms, this philosophy and approach can be truly transformative in nature.

Beyond PETs To Transformative Technologies

Privacy-Enhancing Technologies, when systematically applied within an inclusive and positive-sum paradigm, become PETs *Plus*. When PETs *Plus* are applied to traditionally privacy-invasive technologies, such as monitoring and surveillance systems – without any meaningful loss of functionality – they can, in effect, be transformed into privacy-protective technologies. We call these *Transformative Technologies*.

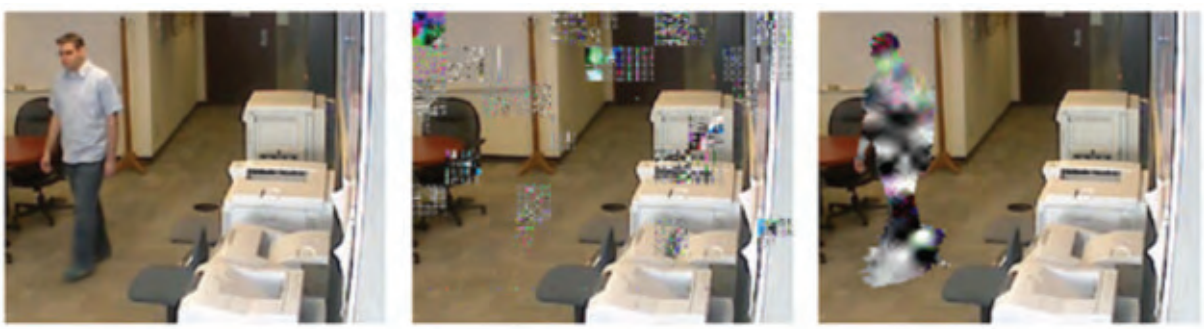
The Commissioner has identified *Transformative Technologies* in many historically "privacy-invasive" areas, such as video surveillance cameras; biometrics; radio frequency identification (RFID); whole body imaging; and others. She believes that, when privacy is built into the process early on, individuals can enjoy the benefits of these technologies AND also have their privacy protected – win/win, positive-sum.

In 2008, the Commissioner published a suite of new discussion and guidance papers setting out this vision, philosophy and methodology.

Video Surveillance Transformed

The Commissioner's seminal publication in 2008 was *Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report* (MC07-68). In response to a complaint regarding the deployment of thousands of additional video surveillance cameras throughout Toronto's mass public transit system, the IPC carried out a full investigation. The IPC reviewed the effectiveness of video surveillance and assessed the role that *PETs* could play in protecting privacy. In March, the Commissioner issued a report finding that the TTC's video surveillance did not contravene Ontario privacy legislation. She made 13 recommendations aimed at making the TTC surveillance system the most privacy-protective mass transit system, anywhere in the

Enhanced Drivers' Licences (EDLs), which will be an alternative to passports for Canadians driving into the U.S., as of June 1, need an on-off switch on the RFID component to protect privacy, says Commissioner Cavoukian.



Now you see him, now you don't. We can have public surveillance and security without identification – until needed.

world. The TTC is implementing all of the Commissioner's recommendations.

The TTC report advances *PETs* as an alternative to the zero-sum paradigm that often persists in discussions on public video surveillance. *(For more information about the TTC report, see the article on page 5.)* One of the *PETs*, developed at the University of Toronto – Secure Visual Object Coding – is an innovative, made-in-Ontario *Transformative Technology*, with numerous exciting uses around the world. It was spotlighted in several 2008 IPC publications.

Once you know where to look, *Transformative Technologies* can be introduced everywhere. They can be identified by their pragmatic, innovative, and elegant approach to apparent dilemmas.

RFID ID Cards Transformed

Take, for example, the new *enhanced drivers' licences* (EDLs) that will be offered in Ontario, several other provinces and some U.S. states to satisfy the U.S. Department of Homeland Security requirements for travellers to demonstrate proof of citizenship as a condition of entry into the United States. The new EDLs will have an embedded Radio Frequency Identification (RFID) chip that contains unique serial number-like data strings that can be remotely "read" by interrogators from up to 30 feet away. These unique data strings will be used by U.S. border inspectors to access personal information in a database of citizen cardholders before they arrive at the inspection booth. The broad objective is to speed up border identification and clearance processes at land and sea entry points, in an effort to reduce delays.

But, as Commissioner Cavoukian and other Commissioners stated in a joint resolution in February, expressing their privacy-related concerns about the enhanced drivers' licences, this same RFID technology can permit the surreptitious tracking of individuals carrying an EDL card. Worse, the data on the RFID chip, if not adequately protected from unauthorized access, can be cloned and used to commit identity theft. The security and privacy concerns associated with using

RFID technology for human identification are well known and have been echoed by many authorities and technology experts. Recognizing this risk, EDL card holders will be offered a protective sleeve that will shield the RFID tag from unauthorized access. Of course, this would require the user to actually use the sleeve and keep his or her driver's licence encased in it. This is unlikely to occur since one normally keeps one's licence in one's wallet, which is made exceedingly difficult if the protective sleeve is actually used (since it is more cumbersome than the licence card).

The pragmatic solution that Commissioner Cavoukian has publicly proposed is to add a simple "on/off switch" to the new cards that, when pressed, would allow transmission of the unique ID to take place. So the default setting would remain at "off" until the cardholder decided to turn it "on." This solution is both inexpensive and elegant: it puts the individual firmly in control as to when and where his or her embedded identity data could be collected by others.

The IPC has already engaged a wide range of stakeholders to promote this security and privacy-enhancing feature, including: the Canada Border Services Agency, the Ministry of Transportation, the Department of Homeland Security, card manufacturers, engineers, standards groups, privacy advocates, public industry associations, the media and the public.

Biometrics Transformed

In 2007, the Commissioner spotlighted the potential for exciting new advances in *PETs* to achieve the key benefits of using biometrics – e.g. for strong user authentication and access control – without the privacy and trust drawbacks associated with second- and third-party collection, matching, and loss of sensitive biometric identity data. In 2008, the IPC continued advocating for Biometric Encryption (BE), engaging a growing range of stakeholders in the process, thereby widely increasing interest in BE. One example is the European Commission announcement of multi-million euro funding for an international pilot project involving use of BE in identity cards and travel documents.

Biometrics **convert unique human physical and behavioural characteristics into machine-readable format for automated comparison.**

Among other advances:

Private voice authentication: The Commissioner brought together international BE and voice recognition industry leaders in a 2008 trial that produced world-class results. The successful tests opened the door to exciting new possibilities for remote, voice-authenticated access, with little or no need for traditional passwords. Customers and staff using private voice authentication could be confident that their BE voiceprints would not be used for any other purpose.

Private face recognition: The Ontario Lottery and Gaming Corporation (OLG) is exploring the use of facial biometrics to assist Ontarians who voluntarily choose to opt into a self-exclusion program, as they would like to be denied entry into casinos (based on a self-identified gambling addiction). Due to sensitivities surrounding any use of automatic identification technologies in casinos, a privacy-enhanced solution is essential. Researchers at the University of Toronto Faculty of Engineering undertook research throughout 2008 to develop a "made-in-Ontario" BE solution that may be integrated with

facial recognition technology. A pilot project was being launched in 2009.

Data mining transformed

The Commissioner is also excited about pioneering work in Ontario to develop and market a *Privacy Analytics* risk assessment tool that statistically anonymizes health data sets for research and quality control purposes, while still protecting patient privacy. This innovative transformative technology has enormous potential applications around the world, including multiple areas that extend well beyond health care.

And the list of potential transformative technologies goes on: whole body image scanning, privacy-enhanced age verification, network monitoring. Many of these technologies are spotlighted in the IPC paper, *Privacy and Radical Pragmatism: Change the Paradigm*, published in August 2008. Extensive ongoing consultations allow the IPC to lead in fostering the development of innovative new technologies, trends and capabilities.

Positive-Sum Engagement

In order to succeed, the Commissioner's positive-sum approach to privacy and technology innovation depends upon proactive engagement of the widest spectrum of interests involved. There can be no "win/win" outcome if key stakeholders are excluded.

In 2008, the Commissioner extended her outreach efforts to a wider range of stakeholders in an effort to develop and adopt PETs *Plus* and *Transformative Technologies*. She engaged the research and standardization communities, technology developers, private sector companies and industry associations, public sector policy-makers and agencies, Privacy and Data Protection Commissioners, privacy rights advocates, the media and, throughout it all, citizens.

Identity, Privacy and Security Initiative

Through her work as Chair of the Advisory Board for the Identity Security and Privacy Initiative (IPSI) at the University of Toronto, the Commissioner is working to identify and encourage exciting new privacy technologies and market opportunities. The IPC was proud to assist in establishing a multi-disciplinary graduate research program in computing and engineering science, dedicated to addressing real-world privacy and security issues. IPSI will be comparable to Carnegie Mellon's CyLab, Cambridge (U.K.) University's Computer Laboratory Security Group, and the University of Waterloo's Centre for Applied Cryptographic Research.

PET Award

For the fifth year in a row, the IPC presented the prestigious *Privacy-Enhancing Technology Award* at the international *PET* Symposium. The 2008 *PET* Award was given in recognition of breakthrough research, showing how easy it was to re-identify individuals in supposedly "anonymous" large public data sets.

Inaugural Privacy by Design Challenge

In late 2008, the IPC was successful in attracting commitments from the largest technology corporations in the world – including Intel, IBM, Microsoft, Sun Microsystems and HP – to participate in the Commissioner's first "*Privacy by Design Challenge*," to showcase the latest innovations in privacy-enhancing technologies in a positive-sum paradigm.

Outreach on Enhanced Drivers' Licences, Youth Privacy Online

In 2008, the IPC also held public information workshops to bring together experts and the public to discuss important privacy and technology-related subjects, such as enhanced drivers' licences and youth online privacy and cyberbullying.

Consultation, Co-operation and Collaboration

The Commissioner's positive-sum philosophy of "consult, co-operate, and collaborate" is very much evident in the IPC's extensive participation – usually in an invitational advisory capacity – in government initiatives, research councils and industry associations. This open-door policy helps to ensure that real dialogue takes place on an ongoing basis, and that technology-related privacy problems are addressed as early and effectively as possible.

Online Social Networking

User-centric online identity management remains a priority for the Commissioner. Working directly with Facebook on some of the projects, the IPC has a multi-level campaign aimed at helping to provide those who use online social networks in Ontario and beyond with the knowledge and tools to make informed choices. As well, the Commissioner publicly addressed evolving online privacy issues, such as Facebook Beacon and Google FriendConnect.

Electronic Health Records / Personal Health Records

The IPC is also actively engaged in discussions regarding the design and development of electronic health records and, in particular, newly emergent personal health records. In 2008, the IPC worked with stakeholders at all levels, across virtually all areas, to help Ontario move forward, and to ensure the availability of interoperable health data for use wherever it is needed, with appropriate privacy assurances. The Commissioner herself has been trying out new personal health record offerings to explore first-hand this innovative development in user-managed health care, and to provide direct feedback and advice to the principal players.

Discussion And Guidance

The IPC was especially active in 2008 in addressing new and emerging technologies, and in shaping public understanding about the privacy impacts and approaches to resolving them. Several discussion and guidance papers were released during 2008.

Privacy in the Clouds, in Web 2.0

The Commissioner strongly believes that the PETs *Plus* approach is the right one to take in the new Information Age, where ever-growing volumes of personal identity data are being created, shared, used and stored by others "in the Cloud." In May 2008, the IPC published *Privacy in the Clouds*, a discussion paper that described this new information privacy landscape. The *Clouds* paper sketched

How can you control your personal information stored and used "in the Cloud?"

out critical technology building blocks and challenged readers, technologists, policy-makers and the public to pursue four technology directions to restore confidence and trust in online identity data transactions that **no longer directly involve the individual**. *Privacy in the Clouds* was subsequently accepted for publication in the inaugural edition of the peer-reviewed journal *Identity in the Information Society*, which the Commissioner helped launch at its first invitation-only organizational workshop. Since publication of the paper, the IPC's views on cloud computing and Web 2.0 privacy issues have been widely sought out.

Privacy and Government 2.0

In 2008, the IPC was invited by an international research group to comment on the effects of "Web 2.0" social technologies on public institutions and governance processes. As an independent oversight agency mandated to oversee the application of information access and privacy laws to Ontario's provincial, local government, and health-care sectors, the IPC offers a unique perspective on privacy and governance questions. As 2008 ended, the IPC was finalizing a discussion paper examining the promises and privacy pitfalls of applying social media to government 2.0.

Privacy Guidance for RFID in Health Care

The Commissioner's philosophy of educative, "win/win" pragmatism was also evident in the publication and launch of a white paper examining the uses of Radio Frequency Identification (RFID) in the health-care sector. *RFID and Privacy: Guidance for Health-Care Providers* documents the astonishingly wide range of uses for this remote identification technology in health care, from tracking bulk pharmaceuticals to patient implants. The IPC categorized these uses into three broad categories: (1) *tagging things*, (2) *tagging things linked to people*, and (3) *tagging people*, and identified key security and privacy issues associated with each type of use. After extensive work, the IPC determined that – in the right circumstances – tagging people was not only a beneficial and acceptable practice, but a perfectly justifiable one – for example, in protecting babies in maternity wards from the threat of abduction.

RFID Privacy Impact Assessment Tool

The IPC is following on the success of the RFID health-care paper with a practical *RFID Privacy Impact Assessment (PIA)* tool to help health-care providers, IT specialists, technology vendors, integrators and practitioners deploy RFID technology into their information systems in the most privacy-protective way, while achieving all the operational benefits. The draft PIA tool is being tested by a number of practitioners, and the IPC expects to finalize and publicly release it in 2009.

Privacy and Biometric Fingerprints

The IPC also published new authoritative guidance, advice and direction for organizations when deploying fingerprint biometric technologies. This guidance builds upon the considerable in-house biometrics expertise that has been devoted to advance Biometric Encryption and related pilot projects, discussed above. Other new publications, including a textbook chapter and a Biometric Encyclopaedia article on the subject of Biometric Encryption, are forthcoming.

Direction

As an oversight agency with investigative and order-making powers, the IPC also provides specific direction to organizations, where and when necessary. The main mechanism for accomplishing this is by issuing orders and privacy investigation reports. At times, there is an explicit technological direction, such as the two 2007 orders to secure laptops and wireless transmissions via encryption. Often, the investigation reports will carry an important technological component or recommendation, as in the case of TTC report.

Amend legislation to make it clear all Ontario universities are subject to the *Freedom of Information and Protection of Privacy Act*

The Ontario Government amended the *Freedom of Information and Protection of Privacy Act* to bring universities under the ambit of the legislation in 2006, an initiative that the IPC had long championed. Universities that receive direct operating funding from the government were listed in the schedule to Ontario Regulation 460 by name, thus bringing them within the scope of the *Act*. The government recognized that universities are recipients of significant public funding, and as such, have a responsibility to be open and transparent in their operations, as well as respectful of the personal information within their custody and control.

During 2008, however, the IPC learned that, despite the best efforts of the government, a potential gap remained, relating to "federated" or "affiliated" universities.

The case in point was a freedom of information request to Victoria University, which is federated with the University of Toronto. An access request was submitted to Victoria, pursuant to the *Act*. After that university declined to release the documents sought, an appeal was filed with the IPC. IPC Adjudicator Donald Hale ultimately issued Order PO-2683, which required the University of Toronto, as the "parent" institution named in Regulation 460, to disclose the non-exempt portions of the requested records. Implicit to Adjudicator Hale's order was the fact that Victoria was part of the University of Toronto.

Victoria University then submitted a request for reconsideration of the order. It sought an amendment to the order naming it as the responding institution, rather than the University of Toronto. Adjudicator Hale responded, emphasizing that, to give legal effect to the order, "it is necessary for me to instruct a scheduled institution under the *Act*, in this case the University of Toronto, to make the required disclosure." Accordingly, he declined to make the change requested by Victoria University.

Subsequently, a second request for reconsideration was received, this time from the University of Toronto itself. Integral to this reconsideration request was the position taken by the University of Toronto that, "as a clear matter of law and fact, Victoria University is not an 'institution' within the meaning of section 2(1) of the *Act*."

The basis for this position was that "Victoria University" was not specifically named in Regulation 460 as an institution subject to the *Act*. Further, the University of Toronto took the position that Victoria is an autonomous university and a separate legal entity, with its own governance structure, president and executive officers, property and employees. The university took the position, agreed upon by Victoria University, that the relationship between the two entities has been delineated in a series of "federation agreements" and that the relationship is simply an academic one.

After considering these representations and those provided by the appellant, Adjudicator Hale upheld his original decision and concluded that Victoria was subject to the *Act* through the inclusion of the University of Toronto in Regulation 460. He concluded that, in reality, Victoria was "part" of the larger university and the inclusion of the University of Toronto in the Regulation was intended to cover not just the University of Toronto itself, but also Victoria.

The adjudicator looked at the actual relationship between the two organizations, as well as the manner in which the universities had conducted themselves since the *Act* was amended to include universities, and also considered the intention of the government in bringing universities under the scope of the *Act*. He noted the existence of a "Memorandum of Agreement" between Victoria and Toronto, which indicates a significant operational and academic integration of the two organizations.

Adjudicator Hale agreed with the appellant that the intent of the amendments bringing universities within the scope of the *Act* was to extend the provisions of the *Act* to publicly funded universities, including affiliated or federated universities. Speaking about these amendments in the legislature, the Minister of Finance and the Chair of Management Board, Dwight Duncan, stated:

> This bill contains measures that will extend the spirit of our freedom of information legislation to include colleges and universities. We are introducing amendments that, if passed, will amend the Freedom of Information and Protection of Privacy Act to accommodate the inclusion of universities and colleges. This is a historic step and one this government is very proud of.

Amendments placing universities under the *Freedom of Information and Protection of Privacy Act* came into effect in 2006.

The adjudicator noted the legislature's intention to include publicly funded universities as institutions under the *Act*. He also noted that Victoria University receives public funding by means of "block grants" from the University of Toronto, in which government funding is streamed to Victoria University. As noted in Victoria University's 2008 Financial Statement:

> The relationship between the University of Toronto and Victoria University is governed by a Memorandum of Agreement. Under this Agreement, the University of Toronto records as

> income all government grants and tuition fees in respect of students of Victoria College. The Agreement also provides for Victoria University to receive a block grant which covers certain administrative and operating expenses, and an instructional grant, which supports part of the cost of Victoria University's programs.

Finally, the adjudicator noted that both universities conducted themselves in such a way as to indicate an acceptance that the *Act* applied to both entities. They had entered into an agreement regarding the administration of access to information requests received pursuant to the *Act*. Among other things, this agreement provided for the creation of mechanisms for the University of Toronto, and its federated universities such as Victoria, to respond to requests depending on the information sought. It also provided for the forwarding of requests between the University of Toronto and the federated universities, where appropriate. Victoria itself had established its own procedure to comply with the *Act*, including the designation of a "Freedom of Information Officer." That university had also created a special "Freedom of Information Request form" for requests made pursuant to the *Act*.

Although Adjudicator Hale concluded that Victoria University was subject to the *Act* and that he had correctly ruled in Order PO-2683, he also recommended that the provincial government amend Regulation 460 to specifically name all affiliated and federated universities and colleges in the province.

While Order PO-2683 examined the status of the Victoria University, there are more than 20 other affiliated and federated universities in the province. Each of those institutions may have affiliation agreements and relationships with their parent universities that differ from those that exist between the universities of Victoria and Toronto. By amending the regulation, the government can avoid future questions about whether those affiliates are covered by the *Act*. In this way, the government can ensure that its stated intention of bringing all publicly funded universities under the *Act* is accomplished.

There is no principled basis for affiliated and federated universities not being subject to the province's access to information and privacy regimes. The need for accountability for the expenditure of public funds remains the same, as does the need for a privacy framework to govern their operation. The exclusion of any federated or affiliated university from the *Act* simply through an anomalous relationship with the parent university would be an unacceptable result; one that can quickly and easily be avoided through the enactment of amendments to the Schedule of Institutions in Regulation 460.

(See the Commissioner's Recommendations section, which starts on the facing page.)

Commissioner's Recommendations

1 Make the creation of an on/off switch for Ontario's enhanced drivers' licence a priority

Last November, Ontario passed legislation authorizing an Enhanced Drivers' Licence (EDL) that Ontarians could use at the U.S. border as an alternative to the passport. As of June 1, 2009, Canadians will need either a passport or an EDL to gain entry when driving into the United States.

As I have stressed, however, the EDL needs a higher level of protection than presently exists because of the radio frequency identity (RFID) tag that will be embedded into the card. An RFID tag can be read not only by authorized readers, but just as easily by unauthorized readers. Over time, they could be used to track or covertly survey one's activities and movements. The electronically opaque protective sleeve – called a Faraday Cage – that will come with these special licences, only provides protection when the drivers' licence is actually encased in the sleeve. But individuals who voluntarily sign up for these enhanced drivers' licences will not only be required to produce them at the border, but will still have to do so in other circumstances where a drivers' licence or ID card is presently required, including in many commercial contexts. Most of the time, the EDL will function as a drivers' licence when driving *within* Ontario – and pulled in and out of one's wallet countless times, for a variety of purposes. The reality is that most drivers will abandon the use of the protective sleeve, which does not fit easily into the slots found in most wallets.

An on-off switch on the RFID tag would provide greatly enhanced protection. The default position would be *off* since drivers don't need the RFID to be "on" unless they are actually crossing the border. A driver would only require it to be turned "on" when approaching the border checkpoint. In all other circumstances, the RFID tag would remain off, no matter how often you needed to pull out your drivers' licence for other purposes.

I am urging the government to work with the selected vendor to pursue adding a privacy-enhancing on-off switch for the RFID tag embedded in the EDLs. Time is of the essence.

2 Amend the law to make it clear that all Ontario universities fall under *FIPPA*

The Ontario Government amended the *Freedom of Information and Protection of Privacy Act* to bring universities under the ambit of the legislation as of June 2006. Universities that receive direct operating funding from the government were listed in Ontario Regulation 460, thus bringing them within the scope of the *Act*. My office had strongly encouraged the government to bring in such legislation. Universities are recipients of significant public funding, and as such, have a responsibility to be open and transparent in their operations, as well as respectful of the personal information within their custody and control. (Colleges of applied arts and technology were already covered by the *Act*.)

During 2008, it came to my office's attention that, despite the best intentions of the government, a gap still remains. This relates to what are known as "federated" or "affiliated" universities. The case in point dealt with a freedom of information request to Victoria University, an institution that is federated with the University of Toronto and is not listed under Regulation 460. While an IPC adjudicator concluded that Victoria University was subject to the *Act* – because of the relationship between the University of Toronto and Victoria University – there are more than 20 other affiliated and federated universities in the province. Each of these may have affiliation agreements and relationships with their parent universities that differ from those that exist between the universities of Victoria and Toronto. The government needs to amend the regulation relating to this, in order to avoid future questions about whether affiliate universities are covered by the *Act*.

By doing so, the government can ensure that its stated intention of bringing all publicly funded universities under the *Act* is accomplished.

There is **no** principled basis for affiliated and federated universities not being subject to the province's access to information and privacy regimes. The need for accountability for the expenditure of public funds remains the same, as does the need for a privacy framework to govern their operation. The exclusion of any federated or affiliated university from the *Act* simply through an anomalous relationship with the parent university would be an unacceptable result – one that can be easily avoided through the enactment of an amendment to the Schedule of Institutions in Regulation 460.

3 The government needs to set specific fees for access requests under *PHIPA*

Subsection 54(11) of Ontario's *Personal Health Information Protection Act (PHIPA)* provides that the fee charged by a health information custodian for making a record of personal health information available to an individual shall not exceed the amount set out in the *regulation* under the *Act* or the amount of reasonable cost recovery, if no amount is provided for in the regulation. To date, no such regulation has been passed, although my office has called for the creation of a fee regulation since the *Act's* inception in 2004. The IPC has responded to many inquiries and complaints from members of the public regarding the fees charged by some health information custodians.

In my August 28, 2008 submission to the Standing Committee on Social Policy, charged with conducting a statutorily mandated review of *PHIPA*, I again cited the need for a fee regulation. I have made it clear that I would support a fee regulation that is substantially similar to the regulation drafted by the Ministry of Health and Long-Term Care, which was posted in the Ontario Gazette for public comment on March 11, 2006. In its October 2008 report to the Speaker of the Assembly, the Standing Committee indicated its agreement with our recommendation, stating that the determination of what constitutes "reasonable cost recovery" should not be left to the discretion of individual health information custodians and their agents.

The Ministry of Health should make the creation of a fee regulation a priority.

Requests by the Public

Provincial and municipal government organizations are required under the *Acts* to report to the IPC early each year on the number of requests for information or correction of personal information they received during the past calendar year, as well as timeliness of responses, outcomes and fees collected.

There were 37,933 freedom of information (FOI) requests filed across Ontario in 2008 – the second highest total ever. The record, 38,584, was set in 2007.

Provincial government organizations received 13,451 FOI requests in 2008, a 5.8 per cent drop from 2007 (when 14,281 requests were filed). Of these, 3,601 (over one-quarter) were for personal information and 9,850 (just over 73 per cent) were for general records.

Every year since 2005, the Ministry of Environment has received the largest number of requests under the provincial *Act* – 5,256 in 2008. As in the previous three years, the Ministry of Environment was followed by the ministries of Community Safety and Correctional Services (3,774), Labour (820) and Community and Social Services (678). These four ministries received nearly four out of every five provincial requests (just over 78 per cent) in 2008.

Ontario's 19 **universities**, in their second full year under the provincial *Act*, received a total of 211 requests in 2008, down nearly seven per cent from the previous year. (For a chart listing the number of requests each Ontario university received, the number completed and compliance rates, please see the online paper, *A More Detailed Look at Compliance Rates and Other 2008 Access and Privacy Statistics*, posted with this Annual Report at www.ipc.on.ca.)

Municipal government organizations – which range from municipalities to police service boards to school boards to other local government organizations – received 24,482 requests in 2008, a slight (0.7 per cent) increase from 2007, when 24,303 requests were filed. Of the 2008 requests, 10,604 (approximately 43 per cent) were for personal information and 13,878 (approximately 57 per cent) were for general records.

Police services boards received the most requests under the municipal *Act* – 13,598 (57.5 per cent). Municipal corporations were next with 9,978 (just over 41 per cent), followed by school boards (234 requests, slightly under one per cent) and health boards (126, about one-half a per cent).

The majority of **provincial** requests in 2008 (just over 70 per cent) were made by businesses, while individuals made the majority of requests under the **municipal** *Act* (slightly over 69 per cent).

The *Acts* contain a number of exemptions that allow, and in some situations actually require, government organizations to refuse to disclose requested information. In 2008, the most frequently cited exemptions for **personal information requests** were the protection of other individuals' privacy, followed by law enforcement. Privacy protection was also the most frequently cited exemption for **general records requests**, followed by law enforcement.

The *Acts* give individuals the right to request correction of personal information about them that is held by government organizations. In 2008, provincial organizations received one request for a correction and refused two (including one received late in 2007). Municipal organizations received 28 correction requests and refused 16.

When a correction is refused, the requester can attach a statement of disagreement to the record, outlining why the information is believed to be incorrect. There was one statement of disagreement filed with provincial institutions and nine with municipal organizations.

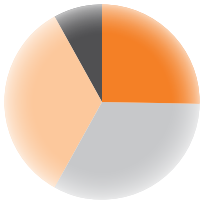
The legislation provides for a number of fees. In addition to the mandatory $5 application fee, government organizations can charge certain prescribed fees for responding to requests. Where the anticipated charge is more than $25, a fee estimate can be given to a requester before search activity begins.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

For provincial organizations, search fees were the most commonly charged fees (65 per cent, compared to nearly 57 per cent in 2007), followed by reproduction costs (nearly 17 per cent) and shipping charges (just over nine per cent). Municipal organizations, by contrast, most frequently charged for reproduction (nearly 45 per cent), followed by search fees (just over 25 per cent) and preparation costs (just over 20 per cent).

As in past years, the average fee for general records was higher (under both *Acts*) than the average fee for personal records, though the average fee for general information requests under the provincial *Act* has dropped for two straight years. (See accompanying chart.)

Outcome of Requests – 2008

PROVINCIAL REQUESTS



MUNICIPAL REQUESTS

Fees Collected – 2008

	Provincial $	Municipal $
Total Application Fees Collected	**65,030.00**	**120,791.45**
Total Additional Fees Collected	**359,392.74**	**278,203.01**
Total Fees Waived (dollars)	**52,253.26**	**11,810.31**

Average Cost of *Provincial* Requests

	2006 $	2007 $	**2008 $**
Personal Information	11.55	10.54	**11.26**
General Records	51.11	50.54	**42.74**

Average Cost of *Municipal* Requests

	$	$	**$**
Personal Information	8.64	9.67	**8.82**
General Records	21.04	23.49	**23.54**

Response Rate Compliance

Each year, to help focus attention on the importance of complying with the response requirements set out in the *Acts*, the IPC reports compliance rates for each ministry and selected other government organizations at the provincial and municipal level.

Two calculations for compliance rates are made, reflecting different provisions of the *Acts*. The first one shows what percentage of freedom of information requests were responded to within the *30-day* standard set by the *Acts*. The second compliance rate, cited as "**extended compliance**," is the 30-day compliance rate adjusted to also factor in *Notices of Extension* and/or *Notices to Affected Persons*. These *notices* permit government organizations to be in compliance with the Acts while taking more than 30 days to respond to a request in extenuating circumstances, such as having to search through a large number of records or consult with one or more people outside the organization. Notices of Extension are explained in more detail in section 27(1) of the provincial *Act* and section 20(1) of the municipal *Act*. The corresponding sections for Notices to Affected Persons are 28(1) and 21(1).

Only One Side of the Story

Since the IPC began emphasizing the importance of response times in 1999 by reporting the individual response rates of various government organizations, the provincial 30-day compliance rate has more than doubled, going from 42 per cent to 85 per cent.

While this is a significant step, it is also important to emphasize that the response rate **alone** does not indicate whether a particular government organization is performing well when it comes to freedom of information (FOI). Prompt replies to access requests do not necessarily mean that information that should be routinely available is always disclosed. Further, unreasonably high fees and a number of other reasons can also hinder an FOI request. For the *Acts* to function in their full and intended purpose, institutions must adhere not only to the wording of the *Acts* but also their spirit, which includes accountability, transparency, and openness.

Institutions Governed Under the Provincial *Act*

After achieving a record 30-day compliance rate in 2007, provincial ministries, agencies and other provincial institutions promptly broke that record in 2008 – producing an overall 30-day compliance rate of 85 per cent. The previous year's record was 84.8 per cent.

The overall extended compliance rate for 2008 was 91.6 per cent, just shy by 0.4 per cent of the record set in 2007. (Extended compliance rates have only been calculated since 2002.)

The accompanying chart of provincial institutions lists ministries and agencies ranked by the number of requests completed in 2008. As usual, the Ministry of the Environment and the Ministry of Community Safety and Correctional Services were the only provincial institutions to receive and complete more than 1,000 requests.

The Ministry of the Environment completed 5,538 requests, with 84.8 per cent of these completed within 30 days – virtually matching the provincial average despite the high number of requests. The 30-day rate was marginally higher than 2007, while, with notices, the ministry's extended compliance rate was 87.7 per cent, again reflecting a marginal increase.

The Ministry of Community Safety and Correctional Services completed 3,539 requests in 2008, with 83.8 per cent completed in 30 days, up slightly from 82.8 per cent in 2007. The ministry's extended compliance rate dropped slightly from 97.8 per cent in 2007 to a still highly commendable 96.3 per cent in 2008.

Universities

The overall number of requests **completed** by universities in 2008 was 234, an increase of 9.3 per cent from 2007, which was the first full year that universities fell under the *Freedom of Information and Protection of Privacy Act*.

The University of Ottawa completed by far the most requests of any Ontario university in 2008 – a total of 72 – more than double the 28 it completed in 2007. Its 30-day compliance rate also increased from 75 per cent the previous year to 79.2 per cent. However, its extended compliance rate slipped slightly from 100 per cent in 2007 to 91.7 per cent in 2008.

The University of Toronto also nearly doubled the number of completed requests, climbing to 32 in 2008 from 19 in 2007. The university's 30-day compliance rate was 90.6 per cent in 2008, compared to 94.7 in 2007, but it maintained its extended compliance rate of 100 per cent.

Provincial Institutions – 2008

(Including institutions where the Minister is the head.)

			Within 1–30 Days		Extended Compliance*	Over 90 Days	
Ranked by the number of requests completed in 2008	Requests Received	Requests Completed	No.	%	%	No.	%
Environment	5256	5538	4698	84.8	87.7	207	3.7
Community Safety and Correctional Services	3774	3539	2964	83.8	96.3	65	1.8
Labour	766	778	708	91.0	91.0	25	3.2
Community and Social Services	678	649	565	87.1	92.6	14	2.2
Attorney General	445	403	369	91.6	95.8	8	1.2
Transportation	295	282	269	95.4	99.3	0	0.0
Government Services	264	245	201	82.0	91.8	1	0.4
Health and Long-Term Care	152	141	85	60.3	80.1	7	5.0
Natural Resources	92	102	50	49.0	80.4	13	12.7
Finance	66	53	40	75.5	94.3	0	0.0
Municipal Affairs and Housing	51	51	43	84.3	96.1	1	2.0
Revenue	50	51	41	80.4	90.2	2	3.9
Training, Colleges and Universities	51	50	36	72.0	86.0	2	4.0
Education	52	49	30	61.2	89.8	2	4.1
Children and Youth Services	40	36	29	80.6	94.4	1	2.8
Energy and Infrastructure	23	32	17	53.1	65.6	10	31.3
Cabinet Office	28	25	22	88.0	88.0	0	0.0
Aboriginal Affairs	15	19	14	73.7	73.7	4	21.1
Culture	15	18	11	61.1	88.9	1	5.6
Agriculture, Food and Rural Affairs	18	16	12	75.0	100.0	3	18.8
Economic Development and Trade (Jan. 1 to Sept. 17)	9	10	8	80.0	100.0	0	0.0
Tourism	10	10	9	90.0	100.0	0	0.0
Northern Development and Mines	8	8	6	75.0	75.0	1	12.5
Citizenship and Immigration	6	7	4	57.1	85.7	1	14.3
Health Promotion	7	7	4	57.1	71.4	0	0.0
Small Business and Consumer Services	7	7	7	100.0	100.0	0	0.0
Economic Development (Sept. 18 to Dec. 31)	6	5	5	100.0	100.0	0	0.0
Francophone Affairs	4	2	2	100.0	100.0	0	0.0
International Trade and Investment	5	2	1	50.0	100.0	0	0.0
Research and Innovation	4	2	2	100.0	100.0	0	0.0
OMERS Administration Corporation	1	1	0	0.0	100.0	0	0.0
Women's Directorate	1	1	1	100.0	100.0	0	0.0

** Including Notice of Extension, section 27(1) and Notice to Affected Persons, section 28(1). Such notices are used in circumstances where, for example, there is a need to search through a large number of records or consult with one or more people outside the organization.*

Three universities significantly increased their 30-day compliance rates: the University of Guelph (to 100 per cent from 42.9 per cent), McMaster University (to 61.5 per cent from 16.7 per cent), and York University (to 83.3 per cent from 61.9 per cent).

(For a chart listing the number of requests each Ontario university received, the number completed and compliance rates, please see the online paper, *A More Detailed Look at Compliance Rates and Other 2008 Access and Privacy Statistics,* posted with this Annual Report at www.ipc.on.ca.)

Institutions Governed by the Municipal *Act*

Municipal government institutions responded in 2008 to freedom of information requests within the statutory 30-day period at a pace – 85.6 per cent – that even surpassed the new provincial record. (The municipal 30-day compliance record is 91 per cent, set in 1992 and tied in 1993.) With notices, the 2008 response rate rises to 88.5 per cent. The 2008 municipal compliance percentages are down marginally from 2007.

The accompanying *Top 30 Municipal Institutions* chart lists the 30 institutions governed by the municipal *Act* that completed the most freedom of information requests in 2008. In addition to municipalities, the *Act* covers police services, school boards, health boards and other local boards.

Once again, the City of Toronto completed the most requests under this *Act* in 2008 – 4,560, down 988 from the 5,548 it recorded the previous year, but it was still the second highest total in Ontario (behind only the Ministry of Environment). The city's 30-day compliance rate climbed slightly to 86.6 per cent from 2007's 85.5. Its extended compliance rate also climbed – to 91.2 per cent from 88.9.

Of the Top 30 municipal institutions, more than half are police services (18 out of 30). The Toronto Police Services held onto the No. 2 overall slot for municipal organizations with 3,287 completed requests, with a 30-day compliance rate of 75.5 per cent (80 per cent with notices), down from 79.4 and 83.1, respectively.

In 2008, eight municipal institutions in the Top 30 group maintained their near perfect or perfect scores from 2007 with regards to both their 30-day compliance rates and extended compliance rates. Halton Regional Police Service, Barrie Police Service, the Town of Oakville, and the cities of Kitchener and Mississauga all averaged 99 per cent or better. Even more impressive, Peel Regional Police, Waterloo Regional Police Service and the City of Cambridge all scored a perfect 100 per cent for both compliance rates.

Notable gains included those by the Region of Peel, which raised its 30-day compliance rate to 96.6 per cent from 61.2 per cent, and its extended compliance rate to 100 per cent from 62.1 per cent. The Brantford Police Service increased its 30-day compliance rate to 85 per cent from 64.7 per cent.

The London Police Service was the only institution in the Top 30 municipal list to experience significant decreases. Its 30-day compliance rate dropped to 37.6 per cent in 2008 from 70.3 per cent in 2007, and its extended compliance rate fell to 50.7 per cent from 97.6 per cent in the same time period.

The London and Sault Ste. Marie Police Services (50.4 per cent) were the only members of the Top 30 high-volume group to have 30-day compliance percentages under 60 per cent.

School Boards

The District School Board of Niagara again took top spot with 93 completed requests, with an excellent 100 per cent 30-day compliance rate, up from 88.1 per cent in 2007.

The Toronto District School Board and the Dufferin-Peel Catholic District School Board were the only other boards to complete more than 10 access requests.

For More Information

Extended charts of compliance statistics for municipalities (sorted by population), police services and school boards are available as part of a special report on the IPC's website, www.ipc.on.ca. This special report, *A More Detailed Look at Compliance Rates and other 2008 Access and Privacy Statistics,* has been posted as an adjunct to the Annual Report.

Top 30 Municipal Institutions – 2008

Ranked by the number of requests completed in 2008	Requests Received	Requests Completed	Within 1–30 Days		Extended Compliance*	Over 90 Days	
			No.	%	%	No.	%
City of Toronto	4,595	4,560	3,951	86.6	91.2	112	2.5
Toronto Police Service	3,441	3,287	2,482	75.5	80.0	57	1.7
Hamilton Police Service	1,322	1,322	989	74.8	84.9	5	0.4
Peel Regional Police	1,205	1,205	1,205	100.0	100.0	0	0.0
Durham Regional Police Service	1,149	1,093	899	82.3	85.7	33	3.0
Niagara Regional Police Service	1,072	1,065	952	89.4	94.9	1	0.1
Halton Regional Police Service	893	861	855	99.3	99.5	0	0.0
Town of Oakville	644	644	642	99.7	100.0	0	0.0
Windsor Police Service	618	628	554	88.2	95.4	0	0.0
London Police Service	621	625	235	37.6	50.7	34	5.4
City of Kitchener	529	528	525	99.4	100.0	0	0.0
City of Mississauga	494	491	487	99.2	99.2	0	0.0
Ottawa Police Service	466	468	367	78.4	99.1	1	0.2
City of Ottawa	474	452	360	79.6	83.6	10	2.2
Waterloo Regional Police Service	374	392	392	100.0	100.0	0	0.0
City of Brampton	379	379	368	97.1	97.6	2	0.5
Town of Richmond Hill	335	334	329	98.5	100.0	0	0.0
Barrie Police Service	330	332	329	99.1	99.4	0	0.0
Sarnia Police Service	324	327	264	80.7	99.1	0	0.0
Brantford Police Service	317	287	244	85.0	85.0	11	3.8
Guelph Police Service	315	292	183	62.7	63.4	14	4.8
York Regional Police	204	197	155	78.7	80.7	1	0.5
Thunder Bay Police Service	166	167	164	98.2	100.0	0	0.0
City of Greater Sudbury	156	151	131	86.8	86.8	0	0.0
City of Hamilton	139	140	138	98.6	100.0	0	0.0
Town of Aurora	121	121	119	98.4	99.2	0	0.0
Sault Ste. Marie Police Service	105	117	59	50.4	50.4	15	12.8
South Simcoe Police Service	118	117	90	76.9	81.2	9	7.7
City of Cambridge	113	113	113	100.0	100.0	0	0.0
Region of Peel	104	106	102	96.2	100.0	0	0.0

** Including Notice of Extension, section 20(1) and Notice to Affected Persons, section 21(1). Such notices are used in circumstances where, for example, there is a need to search through a large number of records or consult with one or more people outside the organization.*

Access

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 the IPC.

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.

Records that do not contain the personal information of the requester are referred to as *general records*. Appeals concerning general records may relate to a refusal to provide access, fees, the fact that the organization did not respond within the prescribed 30-day period, or other procedural aspects relating to a freedom of information request.

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

Statistical Overview

In 2008, a total of 919 *personal information* and *general information* appeals were submitted to the IPC. This represents a decrease of about four per cent from 2007, when 957 appeals were received.

Overall, 966 appeals were closed in 2008, compared to 873 in 2007 – an increase of slightly more than 10 per cent.

Access to *General* Records

Appeals Opened

Overall, 577 appeals regarding access to general records were made to the IPC in 2008. Of these, 261 (just over 45 per cent) were filed under the provincial *Act* and 316 (or about 55 per cent) were filed under the municipal *Act*.

Of the 261 appeals received under the provincial *Act*, 181 (just over 69 per cent) involved ministries and 80 (about 31 per cent) involved agencies.

There were 50 general information appeals filed with the IPC regarding decisions made by the Ministry of Community Safety and Correctional Services. The Ministry of Health and Long-Term Care was involved in the second highest number of general information appeals (24), followed by the Ministry of the Attorney General (18), the Ministry of the Environment (15), and the Ministry of Natural Resources (14).

The provincial agencies that were involved in the most general information appeals were the University of Ottawa (18), McMaster University (six) and the Ontario Reality Corporation (six).

Of the 316 general records appeals received under the municipal *Act*, 198 (almost 63 per cent) involved municipalities, 70 (about 22 per cent) involved police services, and 13 (or about four per cent) involved boards of education. Another 35 appeals (about 11 per cent) involved other types of municipal institutions.

The City of Toronto, which had the highest number of requests under the *Municipal Freedom of Information and Protection of Privacy Act,* also was involved in the most appeals related to general information requests under that *Act* – 66, followed by the Toronto Police Services Board (29), City of Vaughan (13), City of Ottawa (12) and Halton Regional Police Services Board (nine).

Overall, in terms of the issues raised, 266 (or almost 46 per cent) of general records appeals were related to the exemptions claimed by institutions in refusing to grant access. In 61 (about 11 per cent) of the appeals, the issue was whether the institution had conducted a reasonable search for the records requested.

Forty-eight (about eight per cent) of the appeals were the result of deemed refusals to provide access, where the institution did not respond to the request within the time frame required by the *Act*, while 45 (about eight per cent) related to exemptions combined with other issues. The remaining appeals were related to third party, interim decisions, time extensions, fees, and various other issues.

Of the provincial institutions, the Ministry of Community Safety and Correctional Services had the highest number of deemed refusal appeals, with eight. No other ministry or agency had more than two. Of the municipal institutions, the City of Toronto had seven deemed refusal appeals, while the Local Services Board of Rainbow Country had three. No other municipal institution had more than two.

Most appellants (just over 52 per cent) were individual members of the public.

Just over 82 per cent of appellants represented themselves. Lawyers (84) or agents (17) represented appellants in about 17 per cent of the general records appeals made in 2008.

In 2008, $11,455 in application fees for general records appeals was paid to the IPC and forwarded to the Minister of Finance.

Appeals Closed

The IPC closed 562 general records appeals during 2008. Of these, 260 (almost 46 per cent) concerned provincial institutions, while 302 (about 54 per cent) concerned municipal institutions.

Of the 562 general records appeals closed, 115 (just over 20 per cent) were closed at the intake stage, 239 (about 43 per cent) at the mediation stage, and 208 (or just over 37 per cent) at the adjudication stage.

About 73 per cent of general records appeals were closed without a formal order being issued. Of these, 309 (about 76 per cent) were mediated in full, 55 (13 per cent) were withdrawn, and 29 (just over seven per cent) were screened out.

Just over 27 per cent (153) of general records appeals were closed by an order. The IPC issued 74 provincial and 79 municipal orders related to general records. Nine interim orders were also issued, of which one was provincial and eight were municipal.

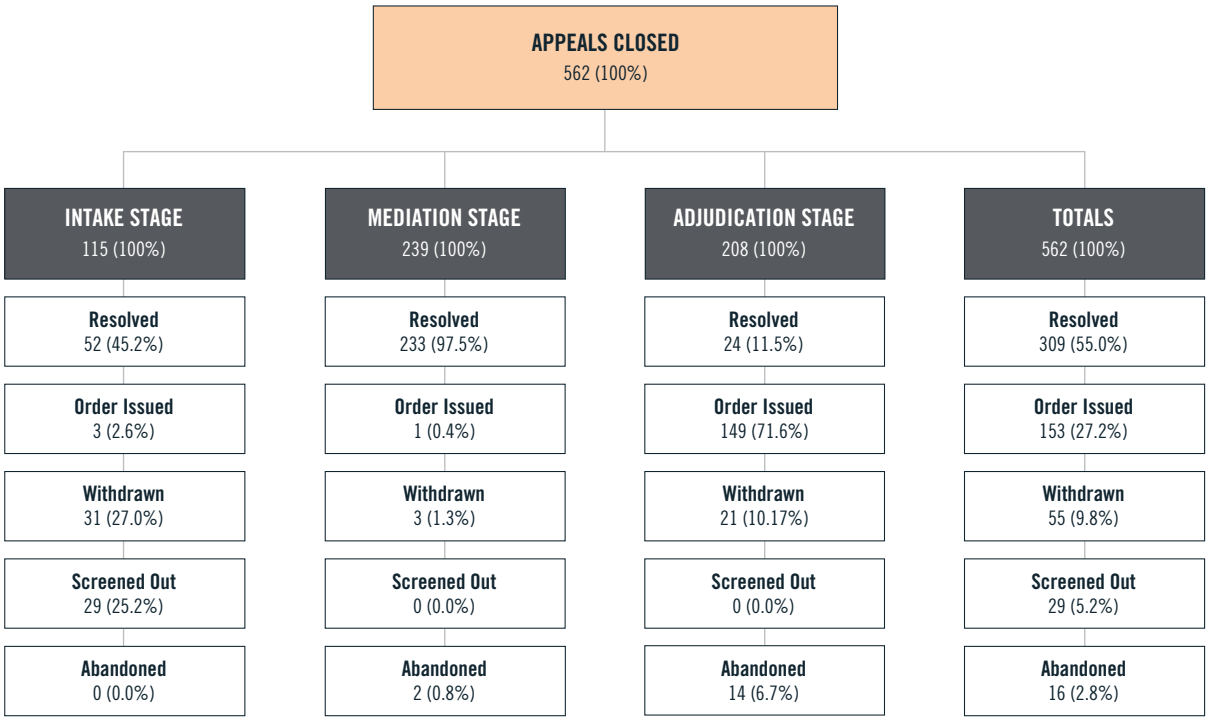
Overall, in appeals resolved by order, the decision of the head was not upheld or only partially upheld in nearly 69 per cent of the appeals. The decision of the head was upheld in about 29 per cent of the appeals. The remaining appeals – slightly over two per cent – had other outcomes.

Types of Appellants in General Records Appeals Opened

	Provincial		Municipal		Total	
	No.	%	No.	%	No.	%
Individual	130	49.8	211	66.8	341	59.1
Business	72	27.6	73	23.1	145	25.1
Media	21	8.0	17	5.4	38	6.6
Association/Group	22	8.4	8	2.5	30	5.2
Academic/Researcher	10	3.8	2	0.6	12	2.1
Government	5	1.9	2	0.6	7	1.2
Politician	1	0.4	1	0.3	2	0.3
Union	0	0.0	2	0.6	2	0.3
Total	**261**	**100.0**	**316**	**100.0**	**577**	**100.0**

Outcome of General Records Appeals Closed by Order

	Provincial		Municipal		Total	
Head's Decision	No.	%	No.	%	No.	%
Partially upheld	35	47.3	28	35.4	63	41.2
Upheld	22	29.7	22	27.8	44	28.8
Not upheld	15	20.3	27	34.2	42	27.5
Other	2	2.7	2	2.5	4	2.6
Total	**74**	**100.0**	**79**	**100.0**	**153**	**100.0**



High Profile Appeals

The IPC closed 966 appeals in 2008, which had been filed by individuals or organizations who were not satisfied by the response received from provincial or local government organizations to freedom of information requests. The seven appeals listed below were among the most high profile.

Orders PO-2657 and PO-2664 – Ontario Lottery and Gaming Corporation

In these decisions, Assistant Commissioner Brian Beamish ordered the Ontario Lottery and Gaming Corporation (OLG) to disclose records pertaining to its investigations verifying significant lottery wins by lottery ticket retailers, known as "insiders." With the exception of certain information about their ethnic origin, the OLG's decision to deny access to portions of the records containing the personal information of winners was not upheld in the order.

The Assistant Commissioner balanced the privacy interests of the insider winners against the need for public scrutiny of the OLG's lottery operations and concluded that the records ought to be disclosed. He found that the factors favouring the disclosure of the information outweighed those in favour of privacy protection. Specifically, the public scrutiny consideration in section 21(2)(a) of the *Freedom of Information and Protection of Privacy Act* was heavily relied upon, particularly given a recent investigation by the Ombudsman of Ontario into the OLG's response to the issue of insider winners. Further, the consideration listed at section 21(2)(c) was found to apply and the Assistant Commissioner determined that this factor leads to an expectation on the part of insider winners that they would not enjoy the same level of privacy protection as members of the general public.

The Assistant Commissioner also found that any harm to an individual's reputation under section 21(2)(i) which might result from the disclosure of the information was clearly outweighed by the need for public scrutiny of the OLG's approach to insider winners and the diminished privacy protection afforded to these individuals. Accordingly, Assistant Commissioner Beamish determined that the disclosure of most of the personal information relating to the insider winners would not constitute an unjustified invasion of their personal privacy.

(The application of the exemptions in section 14(1) {law enforcement} and 18(1) {economic interests of the institution} – were also not upheld.)

Order PO-2681 – Ontario Heritage Trust

In this decision, Senior Adjudicator John Higgins ordered the Ontario Heritage Trust to disclose to the requester certain reports that it had provided to the Minister of Culture concerning the future of the Lister Block, a heritage property located in downtown Hamilton. The Trust had claimed the application of the discretionary exemption in section 13(1) (advice or recommendations) to the responsive record.

In his decision, the senior adjudicator initially upheld the application of the section 13(1) exemption to portions of the record, acknowledging that they contain "a suggested course of action" from public servants to the Minister of Culture. He also found that additional portions of the records qualified for exemption under section 13(1), as their disclosure "would allow the drawing of accurate inferences about the nature of the recommended course of action."

However, the senior adjudicator then determined that the mandatory **exception** in section 13(2)(k) applied to the information which he had originally found to be exempt under section 13(1). This exception applies to a record that contains a report of a committee, council or other body attached to an institution that was established for the purpose of undertaking inquiries and making reports or recommendations to the

institution. He found that the records qualify as a "report" for the purposes of the exception and that the Ontario Heritage Trust is sufficiently attached to the Ministry of Culture to fall within the ambit of the exception in section 13(2)(k). The senior adjudicator also found that the Ontario Heritage Trust was established for the purpose of undertaking inquiries and making reports or recommendations to the Minister, thereby satisfying the third part of the test under section 13(2)(k).

The senior adjudicator also determined that the records should also be disclosed because there is a public interest in the disclosure of the information which outweighs the purpose of the section 13(1) exemption, which means that the "public interest override" in section 23 would apply.

Orders PO-2693 and PO-2694 – McMaster University and University of Western Ontario

In these two orders, Senior Adjudicator Higgins addressed the application of a recently enacted provision in the provincial *Act*, section 65(8.1), which operates to exclude "records respecting or associated with research" by staff or associates of an educational institution from the scope of the *Act*.

In Order PO-2693, the senior adjudicator addressed an appeal from a decision of *McMaster University* respecting its decision to deny access to records about clinical trials. In that case, the senior adjudicator applied the "modern" principle of statutory interpretation whereby the words of a statute are read "in their entire context and in their grammatical or ordinary sense harmoniously with the scheme of the *Act*, the object of the *Act*, and the intention of Parliament." He examined the purposes of section 1 of the *Freedom of Information and Protection of Privacy Act* and applied a definition of the term "research" which is in keeping with the modern rule of statutory interpretation. He found that the records at issue clearly related to research.

He also found that the phrase "respecting or associated with" in section 65(8.1) require that there by a substantial connection between the records and actual or proposed research and that this section must be read in the context of its statutory purpose, which is to protect academic freedom and competitiveness. In this case, the records had the necessary substantial connection to research. Finally, the senior adjudicator also determined that the records in question relate to research being conducted by individuals who are "associated with" McMaster.

As all of the component parts of the section 65(8.1) exclusion were satisfied, the senior adjudicator concluded that it applied to exclude the responsive records from the operation of the *Act*.

This was not the case, however, with respect to the records at issue in Order PO-2694, following a request to the *University of Western Ontario* (UWO). In that case, the senior adjudicator did not uphold UWO's decision to exclude records relating to the construction of an avian wind tunnel intended to be used in research. He applied the same principles as in the McMaster order, and concluded that the responsive records were not "respecting or associated with" actual or proposed research. He found that the records did not disclose any details of actual or proposed research and therefore did not have the required substantial connection to be considered as records "respecting or associated with" research. As a result, he ordered UWO to issue the requester with a decision letter respecting access to the records.

This decision is the subject of an application for judicial review before the Divisional Court.

Order MO-2358 – Halton Catholic District School Board

This appeal involved a request from a parent for access to educational materials that were distributed to his son's class during a two-month absence when the family was required to be out of the country. The Halton Catholic District School Board initially provided the requester with a fee estimate of $372, which was subsequently amended to $380.40, to cover the cost of its search time and photocopying of responsive records.

Adjudicator Bernard Morrow examined whether the fee charged by the board was in accordance with the requirements of section 45(1) and Regulation 823 under the *Municipal*

Freedom of Information and Protection of Privacy Act. In the order, he initially reduced the amount of the fee to $123.20 on the basis that some aspects of the search fee were inappropriate and not in compliance with the requirements of section 45(1) and the regulation.

Later in his order, the adjudicator expressed concern about the board's decision to require a parent to file an access request under the *Act* in order to obtain access to records which would have been provided to his son free of charge had he not been absent from school. He went on to state that, "I find the board's refusal to simply provide these materials as part of the child's education, to the best of its ability, to be unreasonable and inconsistent with the board's duties as a provider of public education. This course of conduct has imposed an unnecessary administrative burden on the [parent], since he had to make a request under the *Act*, followed by an appeal. The processing of this unnecessary appeal has also consumed significant resources of this office."

Accordingly, Adjudicator Morrow disallowed the fee in its entirety and ordered the board to provide the records to the parent without a fee.

Order PO-2730 – Office of the Public Guardian and Trustee

In this decision, Senior Adjudicator Higgins addressed the interpretation of the continuing access provisions in section 24(3) with respect to a request made to the Office of the Public Guardian and Trustee (OPGT). The requester sought access to information about deceased persons whose next of kin cannot be located by the OPGT. The requester wanted the information in the form of a monthly response listing the name, last known address, occupation and place and date of death for a two-year period.

The senior adjudicator decided to adopt a new approach to continuing access under section 24(3) from that taken in Order 164, which had found that section 24(3) applies only to records that are produced "in series." Citing the legislative history of the provision, which indicated that its intent was to promote access rights, the senior adjudicator determined that, unless there is no possibility that future responsive records will come into existence or access is denied in full to the requested information, there ought to be no restrictions placed on the type of record that can be subject to a request for continuous access under section 24(3).

The senior adjudicator also noted that the institution is empowered to determine the frequency of continuing access under section 24(4), which requires it to establish a schedule, and that this decision is appealable to the Commissioner if a requester disagrees with it.

Privacy

Ontario's 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 by a provincial or municipal government organization can file a complaint under the *Acts* with the IPC. In the majority of cases, the IPC attempts to mediate a solution. The IPC may also make formal recommendations to a government organization to amend its practices.

Privacy Complaints

A total of 223 privacy complaints were **opened** under the two public sector *Acts* in 2008 – an increase of 10 (or nearly five per cent) from 2007, when 213 complaint files were opened. Of those opened in 2008, 100 (roughly 45 per cent) were filed under the provincial *Act* and 120 (just under 54 per cent) under the municipal *Act*. There were also three non-jurisdictional complaints.

The increase in overall privacy complaints was driven by complaints filed under the municipal *Act* – up by 37 (or just under 45 per cent) from 2007.

Overall, 232 privacy complaints were **closed** in 2008, an increase of 10 from the 222 complaints closed in 2007, representing a five per cent jump.

The disclosure of personal information was raised as an issue in 112 (about 48 per cent) of the complaints closed. Another 22 (about nine per cent) were related to collection, while security was an issue in 18 cases (nearly eight per cent). The remaining complaints involved issues including use, retention, notice of collection and consent.

While processing privacy complaints, the IPC continues to emphasize informal resolution. Consistent with this approach, 223 of the 232 privacy complaints closed in 2008 – or about 96 per cent – were closed without the issuance of a formal privacy complaint report or order.

Of the complaints closed, individual members of the public initiated 154 (about two-thirds), another 34 (15 per cent) were Commissioner-initiated, and 44 (about 19 per cent) were self-reported by government organizations.

Personal Information Appeals

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

Personal information appeals can relate to 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.

When an appeal is received, the IPC first attempts to settle it informally. If all the issues cannot be resolved, the IPC may conduct an inquiry and issue a binding order that may require the government organization to release all or part of the requested information.

Statistical Overview

In 2008, a total of 919 *personal information* and *general information* appeals were submitted to the IPC. This represents a drop of about four per cent from 2007, when 957 appeals were received.

Overall, the IPC closed 966 appeals in 2008, compared to 873 in 2007 – an increase of slightly more than 10 per cent.

Summary of Privacy Complaints

	2007 Privacy Complaints				2008 Privacy Complaints			
	Provincial	Municipal	Non-jurisdictional	Total	Provincial	Municipal	Non-jurisdictional	Total
Opened	126	83	4	213	**100**	**120**	**3**	**223**
Closed	129	89	4	222	**110**	**119**	**3**	**232**

Where Privacy Complaints came from (sources of the Complaints that were closed in 2008)

	Provincial		Municipal		Non-jurisdictional		Total	
Year	No.	%	No.	%	No.	%	No.	%
Individual	62	56.4	89	74.8	3	100.0	154	66.4
IPC Commissioner Initiated	18	16.4	16	13.4	0	0.0	34	14.7
Self-reported Breaches	30	27.2	14	11.8	0	0.0	44	18.9
Total	**110**	**100.0**	**119**	**100.0**	**3**	**100.0**	**232**	**100.0**

Privacy Complaints by Type of Resolution and Stage Closed

	Intake		Investigation		Total	
	No.	%	No.	%	No.	%
Resolved	138	66.0	13	56.5	151	65.1
Screened Out	40	19.1	0	0.0	40	17.2
Withdrawn	29	13.9	1	4.3	30	12.9
Report	0	0.0	9	39.1	9	3.9
Abandoned	2	1.0	0	0.0	2	0.9
Total	**209**	**100.0**	**23**	**100.0**	**232**	**100.0**

Outcome of Privacy Complaints

	Provincial		Municipal		Non-jurisdictional		Total	
	No.	%	No.	%	No.	%	No.	%
Resolved – Finding Not Necessary	81	94.2	71	79.8	2	100.0	154	87.0
Complied in Full	3	3.5	7	7.9	0	0.0	10	5.6
Not Complied	2	2.3	8	9.0	0	0.0	10	5.6
Act Does Not Apply	0	0.0	3	3.4	0	0.0	3	1.7
Complied in Part	0	0.0	0	0.0	0	0.0	0	0.0
Total	**86**	**100.0**	**89**	**100.0**	**2**	**100.0**	**177**	**100.0**

** The number of issues does not equal the number of complaints closed, as some complaints may involve more than one issue. Abandoned, withdrawn and screened out complaint files are not included.*

Access or Correction of Personal Information

Appeals Opened

Overall, 342 appeals regarding access to or correction of *personal information* were made to the IPC in 2008 compared to 386 in 2007, a drop of nearly 13 per cent. Of these, 148 (over 43 per cent) were filed under the provincial *Act* and 194 (about 57 per cent) were filed under the municipal *Act*.

Of the 148 personal information appeals received under the provincial *Act*, 108 (73 per cent) involved ministries and 40 (27 per cent) involved agencies. The Ministry of Community Safety and Correctional Services was involved in by far the largest number of personal information appeals (83), followed by the Ministry of the Attorney General (six). The ministries of Education, and Community and Social Services each had five of their decisions appealed.

The agencies with the highest number of personal information appeals included the University of Ottawa (10), Ontario Lottery and Gaming Corporation (five) and the Workplace Safety and Insurance Board (four).

Of the 194 personal information appeals received under the municipal *Act*, 130 (about two-thirds) involved police services, 37 (about 19 per cent) involved municipalities, and 22 (11 per cent) involved boards of education. Five appeals (2.5 per cent) involved other types of municipal institutions.

Overall, 197 (just under 58 per cent) of appeals were related to the exemptions claimed by institutions in refusing to grant access. In 38 (about 11 per cent) of the appeals, the issue was whether the institution had conducted a reasonable search for the records requested.

Another 26 (just under eight per cent) were the result of deemed refusals, where the institution did not respond to the request within the time frame required by the *Act*, and 24 (just under eight per cent) of the personal information appeals related to exemptions plus other issues. The remaining appeals were related to other issues, including correction, frivolous or vexatious and time extensions.

Since personal information appeals, by definition, relate to a request for access and/or correction of one's own personal information, all complainants are categorized as individuals. Overall, just over 73 per cent of appellants represented themselves in these personal information appeals. Lawyers (74) or agents (18) represented appellants in about 27 per cent of the appeals.

The IPC received $3,630 in application fees for personal information appeals in 2008; these fees were turned over to the Minister of Finance.

Appeals Closed

The IPC closed 404 personal information appeals during 2008, a 23 per cent increase from the 329 closed in 2007. In 2008, 181 (45 per cent) of these appeals concerned provincial institutions, while 223 (55 per cent) concerned municipal institutions.

Of the 404 personal information appeals closed, 118 (about 29 per cent) were closed at the *intake stage*, 172 (about 43 per cent) at the *mediation stage*, and 114 (about 28 per cent) at the *adjudication stage*.

Overall, 317 (almost 78 per cent) of personal information appeals were closed without the need to issue a formal order. Orders were issued to resolve about one-fifth of the appeals.

The IPC issued a total of 87 final orders for personal information appeals – 46 provincial and 41 municipal.[1] Eleven interim orders were also issued – five provincial and six municipal.

In appeals closed by order, the decision of the head was upheld slightly more than 54 per cent of the time, and was not upheld or only partially upheld in 29 per cent of cases. Nine appeals (10 per cent) had other outcomes.

1 One order may close more than one appeal.

Outcome of Personal Information Appeals Closed by Stage

	Intake		Mediation		Adjudication		Total	
	No.	%	No.	%	No.	%	No.	%
Resolved	38	32.2	166	96.5	15	13.2	219	54.2
Order Issued	2	1.7	0	0.0	85	74.6	87	21.5
Withdrawn	31	26.3	3	1.7	9	7.9	43	10.6
Screened Out	45	38.1	0	0.0	0	0.0	45	11.1
Abandoned	2	1.7	3	1.7	4	3.5	9	2.2
No Inquiry	0	0.0	0	0.0	1	0.9	1	0.2
Total	**118**	**100.0**	**172**	**100.0**	**114**	**100.0**	**404**	**100.0**

Outcome of Personal Information Appeals Closed other than by Order

	Provincial		Municipal		Total	
	No.	%	No.	%	No.	%
Resolved	93	68.9	126	69.2	219	69.1
Withdrawn	18	13.3	25	13.7	43	13.6
Screened Out	19	14.1	26	14.3	45	14.2
Abandoned	4	3.0	5	2.7	9	2.8
No Inquiry	1	0.7	0	0.0	1	0.3
Total	**135**	**100.0**	**182**	**100.0**	**317**	**100.0**

Outcome of Personal Information Appeals Closed by Order

	Provincial		Municipal		Total	
Head's Decision	No.	%	No.	%	No.	%
Upheld	25	54.3	22	53.7	47	54.0
Partially Upheld	11	23.9	14	34.1	25	28.7
Other	7	15.2	2	4.9	9	10.3
Not Upheld	3	6.5	3	7.3	6	6.9
Total	**46**	**100.0**	**41**	**100.0**	**87**	**100.0**

High Profile Privacy Incidents

The IPC received 507 complaints in 2008 under Ontario's three privacy *Acts* covering the public and health sectors. The following four privacy investigations were among the most high profile. *(See the separate story on the privacy complaint regarding the TTC surveillance cameras on page 5.)*

PC07-21: Ministry of Transportation

An individual (the complainant) who was a potential witness at a tribunal hearing became aware that a private investigator had been hired to follow her. The complainant further learned that the private investigator was able to obtain her address, her driver's licence number, her date of birth, and information pertaining to a vehicle she owned from the Ministry of Transportation (MTO) driver's licence database. The complainant was concerned that the disclosure of this information by MTO was inappropriate, and filed a complaint with the IPC.

In response to the complaint, MTO explained that the information in question was provided to the private investigator through MTO's Authorized Requester Program (ARP). Under the ARP, certain entities, which are known as ARP "clients," are permitted to obtain access to information contained in the MTO driver's licence database. MTO further explained that private investigators are one of the types of entities that are eligible to obtain this information.

MTO explained that it actively oversees the ARP by monitoring the business registrations of all ARP clients. In addition, MTO had established a *management assurance framework*, which, among other things, mandates training and audits for all ARP clients. MTO also made reference to its *notice of collection*, which provides additional information concerning the ARP, and is made available to the public on its website. MTO's notice explains that certain entities are considered to be authorized requesters, and that these entities have entered into a contractual agreement with MTO to obtain residential address information under the 13 enumerated circumstances that are set out in the notice.

In considering whether the disclosure by MTO was appropriate in this situation, the IPC investigator noted that none of the 13 circumstances set out in the notice of collection applied to the disclosure of the complainant's personal information. While the notice states that personal information may be disclosed for the service of legal documents or for legal proceedings, this could not be construed as sanctioning the use of MTO information to allow a private investigator to "tail" an independent witness to a tribunal hearing.

The IPC investigator ultimately concluded that the disclosure of the complainant's personal information by MTO to the private investigator was **not** in accordance with the provisions of the *Freedom of Information and Protection of Privacy Act*.

The IPC investigator recommended that MTO review all classes of ARP clients to assess whether the disclosures it was making were in accordance with MTO's core purposes. The investigator also recommended that MTO review its audit procedures to ensure that it responds to all complaints in a timely manner.

MC07-64: The City of Vaughan

The IPC received a privacy complaint from an individual involving the City of Vaughan. The complainant stated that the city had improperly used and disclosed her personal information, in contravention of the provisions of the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*, by mailing out applications for a credit card, on behalf of a credit card company.

Specifically, the complainant advised that the city used its property tax roll database to mail out applications for a credit card, which she received in the mail. The credit card

application displayed the complainant's pre-printed name, address and property tax roll number as the base information to be used when completing the credit card application.

The complainant also advised an IPC investigator that she had filed a complaint with the city regarding the use of the property tax roll in this manner, and that the city had, in turn, disclosed her identity as a complainant to the credit card company.

The city advised the investigator that the particular credit card at issue offered reward points to its users in the form of municipal property tax credits. As a result, the city had agreed to send the personal information on the property tax roll to a printer, who merged it with the credit card application. The city advised that the original purpose of collecting personal information for the property tax roll is to facilitate the payment of property taxes, and that its use in the credit card applications was therefore for a consistent purpose under *MFIPPA*.

The IPC investigator determined that there was no rational connection between the purpose of the collection (the payment of property taxes) and the way it was used with the credit card application, and that individuals in the complainant's position would not have reasonably expected the use of their personal information, including name, address and roll number, to promote a credit card. Therefore, the city's use of the property tax roll in assisting the credit card company was in breach of *MFIPPA*.

The investigator also determined that the city disclosed the complainant's name to the credit card company in breach of *MFIPPA*, as her complaint, which concerned the use of the property tax roll, could have easily been handled without the disclosure of her identity to the company.

The IPC investigator made two recommendations, namely, that the city cease the practice of using the name and address of individuals and property tax roll number to solicit potential customers on behalf of a credit card company, and that the city review its practices relating to receiving complaints from individuals to ensure that the disclosure of personal information to third parties is in accordance with *MFIPPA*.

MC07-23: Peel Regional Police Services Board and Regional Municipality of Peel, and

MC07-49: Northumberland County

The IPC initiated an investigation into an arrangement between the Regional Municipality of Peel and the Peel Regional Police. The arrangement, called the "Region of Peel Crime-Free Multi-Housing Program," involved a memorandum of understanding (MOU) between the police and the municipality. The MOU, among other things, provided for disclosure of police incident information by the police to the municipality.

In addition to the MOU, the municipality had prepared a *tenancy agreement addendum*, which was required to be signed by all prospective tenants and stated that neither they, nor any member of their household, would engage in any criminal activity on the property.

The primary issue in the investigation was whether the incident information collected by the municipality from the police constituted a permissible collection of personal information under *MFIPPA*. In order to make this determination, an IPC investigator considered whether the municipality and the police had satisfied the "necessity condition," which is a test used to determine whether a given collection of personal information is permissible under *MFIPPA*. Under the necessity condition, an institution must demonstrate that the collection of each item or class of personal information is necessary to administer a lawfully authorized activity.

The investigator considered the information provided by the police and the municipality, which showed that out of approximately 500 incidents that had been reported by the police to the municipality during an eight-month period, only 19 of these incidents resulted in more detailed discussions. The fact that only about four per cent of the 500 incidents were deemed to be serious enough to require a follow-up discussion suggested that the reporting of some of these incidents may not have met the necessity condition, and would therefore not be permissible under *MFIPPA*. Accordingly, the investigator concluded that the routine collection of

information about all listed occurrences by the municipality was not in accordance with *MFIPPA*.

As a result, the IPC investigator recommended, among other things, that the police and the municipality jointly develop written criteria that would be used to determine when police incident information may be reported to the municipality. In developing these criteria, the investigator recommended that both institutions be mindful of the necessity condition.

Subsequent to commencing the Peel investigation, the IPC received a letter from an organization raising concerns regarding a similar program in **Northumberland County**, and a separate investigation was initiated into that matter.

In that county, prospective tenants for municipal housing were required to sign an *addendum,* including provisions similar to those in the Region of Peel.

In response to the complaint, the county explained that the information collected from police services operating in the area was limited to information relating to criminal convictions, criminal charges, search warrants to be executed on municipal housing property, and information pertaining to crimes in progress.

In considering whether the county's actions were in accordance with the provisions of *MFIPPA*, the IPC investigator once again considered the application of the necessity condition. In this case, because the collection of personal information was more limited than what was taking place in the Region of Peel, the investigator determined that the county's collection of personal information was permissible and in accordance with *MFIPPA*.

However, the investigator concluded that the county was not meeting its obligation to notify individuals of the collection of their personal information. The investigator had reviewed the *addendum* and noted that it was only provided to prospective tenants, (not current tenants) and that its wording did not satisfy all of the notice requirements set out in *MFIPPA*.

As a result, the IPC investigator recommended that the county develop a *notice of collection* that satisfied all of the statutory criteria of *MFIPPA*, and further recommended that this notice be provided to all tenants.

The *Personal Health Information Protection Act*

The IPC actively participated in 2008 in the Legislature's review of the *Personal Health Information Protection Act (PHIPA)*. As well, throughout much of the year, the IPC's work focused on reviews and investigations of practices and procedures in the health sector to protect the privacy and confidentiality of personal health information. And, the IPC also conducted follow-up reviews of the information practices of the prescribed entities and prescribed persons that compile or maintain registries. With respect to privacy complaints under *PHIPA*, the IPC continued to focus on mediation and alternative dispute resolution. No orders were issued under *PHIPA* in 2008.

Reviews of Prescribed Entities and Prescribed Persons

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

These organizations are required to have their information practices and procedures approved by the IPC every three years. In 2005, the IPC completed its mandated reviews of the four prescribed entities: Cancer Care Ontario, the Canadian Institute for Health Information, the Institute for Clinical Evaluative Sciences, and the Pediatric Oncology Group of Ontario. Also that year, the IPC completed a review of four prescribed persons that compiled or maintained registries of personal health information: the Cardiac Care Network of Ontario, in respect of its registry of cardiac services; INSCYTE (Information System for Cytology) Corporation, in respect of CytoBase; the Canadian Stroke Network, in respect of the Registry of the Canadian Stroke Network; and the London Health Sciences Centre, in respect of the Ontario Joint Replacement Registry.

As of 2006, the London Health Sciences Centre, was no longer a prescribed person within the meaning of *PHIPA* (in respect of the Ontario Joint Replacement Registry). Also in 2006, the Hamilton Health Sciences Corporation, in respect of the Critical Care Information System, was prescribed as a person that compiles or maintains a registry of personal health information. In 2007, Cancer Care Ontario, in respect of the Colorectal Cancer Screening Registry, was also added to the list of prescribed persons and its information practices were approved in the spring of 2008.

Since the prescribed entities and prescribed persons are required to have their information practices reviewed and approved by the IPC every three years, in 2008, the IPC again reviewed and approved the information practices of all four prescribed entities and the prescribed persons that had previously had their information practices reviewed and approved by the IPC. All of the prescribed entities and prescribed persons that were reviewed were found to continue to meet the requirements of *PHIPA*. Reports on each of these reviews are available on the IPC's website.

Review of *PHIPA*

The Legislature's Standing Committee on Social Policy conducted a public hearing on August 28, 2008, concerning recommendations for amendment to *PHIPA*. The Commissioner made an oral presentation highlighting the IPC's detailed written recommendations for amending *PHIPA*.

The Commissioner's main message was that *PHIPA* appears to be striking the right balance between protecting the privacy of individuals with respect to their personal health

information and the equally important objective of ensuring the continued delivery of effective, efficient and timely health care – and that extensive amendments were not required. The IPC suggested a number of amendments to ensure that the proper balance continues to be struck between patients' privacy and the delivery of timely health care; to ensure that the exercise by individuals of their rights under *PHIPA* continues to be respected, and that the IPC has the powers necessary to independently review, investigate and adjudicate complaints under *PHIPA*.

On November 4, 2008, the Standing Committee on Social Policy issued a report to the Legislative Assembly of Ontario concerning amendments to *PHIPA*. In general, the Committee recommended very few amendments to *PHIPA*.

In the *Commissioner's Recommendations* section of this Annual Report, the Commissioner is urging that action be taken regarding establishing what fees can be charged when individuals request copies of their medical files.

Education and Awareness

During 2008, the IPC – through presentations and information booths, by responding to inquiries from health information custodians and members of the public, and through the publication of educational materials – continued to help educate health information custodians and the public about the requirements of *PHIPA*. For example, the IPC issued *RFID and Privacy: Guidance for Health-Care Providers* to inform the health-care sector about the benefits and risks associated with the use of this technology. The IPC also issued two publications – *Fact Sheet #15: Obtaining Personal Health Information About a Deceased Relative* and *If you wanted to know ... Can I get health information about my deceased relative?* – to explain the rights that individuals have with respect to obtaining personal health information about their deceased relatives.

In addition, the IPC formed a working group towards the end of 2008 to help educate health information custodians about a specific issue – the provisions of *PHIPA* that allow certain custodians, in *defined circumstances*, to collect, use and disclose personal health information for the purpose of providing health care on the basis of *assumed implied consent*. These provisions were intended to allow for the immediate and unobstructed flow of personal health information among health-care providers, within the patient's "circle of care." However, since *PHIPA* came into force, there has been a general lack of understanding about who can reasonably be included within the "circle of care" and when health information custodians may rely on *assumed implied consent*. One of the main purposes of the working group is to ensure that health information custodians understand that *PHIPA* does not present a barrier to sharing information in the delivery of health-care services. Output from the working group was expected early in 2009.

Statistical Review

Statistics related to requests for access to personal health information or privacy complaints filed under *PHIPA* are collected in two different ways for this Annual Report: internally and externally.

The **internal** collection is from the IPC's own records, showing the number and nature of all complaints filed with the IPC in 2008 under *PHIPA*. These are reported in the *PHIPA Complaints* section of this chapter.

The **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. Only government organizations that fall under the *Freedom of Information and Protection of Privacy Act (FIPPA)* or the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)* and are **also** health information custodians – or that employ one or more health information custodians (such as doctors or ambulance services) – are required to report *PHIPA*-related information annually to the IPC. A few other custodians, such as some general hospitals, are reporting voluntarily.

The Ministry of Health and Long-Term Care receives far more access requests under *PHIPA* than other health information custodians. A brief review of access requests filed with that ministry is provided in the section of this chapter entitled *Personal Information Requests*.

PHIPA Complaints Opened 2008

Custodians, Agents and Others	Collection/Use/Disclosure: Access/ Correction	%	Individual	%	Self-reported Breach	%	IPC-Initiated	%	Total	%
Public Hospital	27	32.50	23	33.8	55	50.00	4	17.39	109	38.40
Doctor	20	24.10	9	13.2	4	3.64	8	34.78	41	14.40
Clinic	7	8.40	8	11.8	3	2.73	6	26.09	24	8.50
Community or Mental Health Centre, Program or Service	4	4.80	5	7.4	15	13.64	0	0.00	24	8.50
Other Health Care Professional	1	1.20	2	2.9	10	9.09	1	4.35	14	4.90
Ministry of Health	4	4.80	4	5.9	1	0.91	0	0.00	9	3.20
Laboratory	1	1.20	1	1.5	6	5.45	0	0.00	8	2.80
Pharmacy	0	0.00	6	8.8	0	0.00	2	8.70	8	2.80
Community Care Access Centre	0	0.00	0	0.0	7	6.36	0	0.00	7	2.50
Agent	4	4.80	1	1.5	0	0.00	0	0.00	5	1.80
Other	1	1.20	3	4.4	0	0.00	1	4.35	5	1.80
Ambulance Services	1	1.20	0	0.0	2	1.82	1	4.35	4	1.40
Long-term Care Facility	4	4.80	0	0.0	0	0.00	0	0.00	4	1.40
Home or Joint Home (aged or rest)	3	3.60	0	0.0	0	0.00	0	0.00	3	1.10
Psychiatric Facility	1	1.20	2	2.9	0	0.00	0	0.00	3	1.10
Psychologist	0	0.00	1	1.5	2	1.82	0	0.00	3	1.10
Dietician	2	2.40	0	0.0	0	0.00	0	0.00	2	0.70
Health Data Institute	2	2.40	0	0.0	0	0.00	0	0.00	2	0.70
Independent Health Facility	0	0.00	1	1.5	1	0.91	0	0.00	2	0.70
Recipient	0	0.00	2	2.9	0	0.00	0	0.00	2	0.70
Board of Health	0	0.00	0	0.0	1	0.91	0	0.00	1	0.40
Chiropractor	0	0.00	0	0.0	1	0.91	0	0.00	1	0.40
Dentist	0	0.00	0	0.0	1	0.91	0	0.00	1	0.40
Drugless Practitioner	1	1.20	0	0.0	0	0.00	0	0.00	1	0.40
Minister of Health	0	0.00	0	0.0	1	0.91	0	0.00	1	0.40
Total	**83**	**100.00**	**68**	**100.00**	**110**	**100.00**	**23**	**100.00**	**284**	**100.00**

PHIPA Complaints

Complaints Opened

There were 284 complaint files *opened* by the IPC under *PHIPA* in 2008, a decrease of just under 16 per cent from the 338 complaints opened in 2007, but the second highest total in the four full years since *PHIPA* came into effect.

Public hospitals accounted for 109 of the 284 complaints, or about 38 per cent, a decrease from 43 per cent in 2007.

There were 41 complaints opened involving doctors (roughly 14 per cent), 24 involving clinics (eight per cent), 24 involving community or mental health centres, programs or services (eight per cent), and nine (a little over three per cent) involving the Ministry of Health and Long-Term Care. Laboratories and Pharmacies were each involved in eight complaints (just under three per cent). The remaining privacy complaints involved other types of health information custodians or agents.

Overall, 83 (a little over 29 per cent) of the complaints opened in 2008 related to access to and/or correction of personal health information. The remaining 201 complaints dealt with the collection, use or disclosure of personal health information. Of these, 110 complaints were self-reported breaches by health information custodians (about 39 per cent of the total number of complaints), while 68 were filed by individuals (about 24 per cent). Another 23 (just over eight per cent) were initiated by the Commissioner.

Complaints Closed

The drop in the number of complaints opened was partially reflected in the number of complaints *closed*. The IPC closed 302 complaints in 2008, a decrease of about 11 per cent over the 338 complaints closed in 2007.

Of the complaints closed, 80 (over 26 per cent) dealt with access to and/or correction of personal health information, while the other 222 dealt with collection, use or disclosure. Of the second type, 123 (about 41 per cent of the overall number of complaints *closed*) arose from privacy breaches self-reported by health custodians. Commissioner Cavoukian actively encourages this kind of self-reporting.

The remaining privacy complaints related to collection, use or disclosure that were closed in 2008 included 77 (about 25 per cent) filed by individuals and 22 (about seven per cent) initiated by the Commissioner.

Of the 80 complaints closed that were related to access to and/or correction of personal health information, 27 (34 per cent of this category) were the result of deemed refusals, where a health information custodian fails to respond to the request within the statutory time frame. Fees were the issue in 12 (15 per cent) of the complaints, and 10 (over 12 per cent) were about whether the health information custodian had conducted a reasonable search for the records requested. There were four complaints (five per cent) related to the correction of personal health information. The exemptions applied to deny access to personal health information were the subject of four (five per cent) complaints. The remaining 23 (about 29 per cent) complaints involved other issues.

As much as possible, the IPC prefers to resolve complaints either informally or through mediation. All 80 complaints dealing with access to and/or correction of personal health information that were closed in 2008 were resolved without the IPC needing to issue an order. Of these, 56 (70 per cent) were closed informally at the intake stage, 23 (about 29 per cent) were closed during the mediation stage, and one (just over one per cent) was closed during the adjudication stage without an order having to be issued.

Similarly, the 222 complaints closed in 2008 regarding the collection, use or disclosure of personal health information were all resolved informally or through mediation.

Of the 77 initiated by individual complainants, 68 (about 88 per cent) were closed during the intake stage, eight (about 10 per cent) were closed during the mediation stage and one was closed in adjudication.

And, of the 22 complaints dealing with the collection, use and disclosure of personal health information that the Commissioner initiated, 21 (just over 95 per cent) were closed at the intake stage and one at the mediation stage.

Of the 123 complaints that involved self-reported privacy breaches by health information custodians, 116 (over 94 per cent) were closed at the intake stage, and seven (about six per cent) at the mediation stage.

Personal Health Information Requests

The Ministry of Health and Long-Term Care completed 3,023 requests from individuals seeking access to/or correction of their personal health information in 2008. (Only health information custodians who also fall under *FIPPA* or *MFIPPA* are required to report such information. This ministry traditionally receives about 85 per cent of the requests that are reported to the IPC.)

The requests made to the ministry in 2008 climbed by 573, from 2007's 2,450 requests, an increase of just over 23 per cent.

The ministry's 30-day compliance rate was 99 per cent. Full access was provided in 2,954 cases – nearly 98 per cent of requests. Both percentages match those of the previous year.

The ministry reports it did not charge any fees regarding the requests completed under *PHIPA* in 2008. In 2007, it charged fees related to about three per cent of such requests.

More Statistics Available

Additional charts regarding access requests or privacy complaints filed under *PHIPA* are available in the online paper, *A More Detailed Look at Compliance Rates and Other 2008 Access and Privacy Statistics,* posted with this Annual Report at www.ipc.on.ca.

Judicial Reviews

In 2008, the Ontario Courts issued several decisions affirming the importance of the principle of transparency as embodied in the *Freedom of Information and Protection of Privacy Act (FIPPA)* and the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*, as well as the IPC's interpretation and application of exemptions and exclusions under these statutes.

Among these:

(1) In a significant decision, the Ontario Court of Appeal restored the IPC's ruling on a request for records relating to the "Mega Studio Project" in the Toronto Port Lands. The requester, a film studio company, made requests to the City of Toronto and to the City of Toronto Economic Development Corporation (TEDCO). Both denied access based on their claim that TEDCO is not an "institution" under section 2(3) of *MFIPPA* and, for that reason, the statute does not apply to its record holdings. On appeal, the IPC found that TEDCO is deemed to be part of the city, because all of its members or officers are appointed or chosen by or under the authority of city council and are its "controlling minds."

On judicial review, a majority of the Divisional Court held that the IPC erred in interpreting the word "officers" in section 2(3) to include the directors of TEDCO. Rather, the majority stated that the IPC should have adopted the narrower meaning of officers contained in the *Business Corporations Act*.

The Ontario Court of Appeal reversed the Divisional Court's ruling, holding that "it would be wrong to exclude TEDCO from the *Act*'s reach merely because city council has delegated direct appointment power to the board of directors." Further, the IPC's decision was consistent with the purpose of *MFIPPA*, given that TEDCO carries out important public functions and the city is its sole shareholder. The Court restored the IPC's order directing the city to obtain the requested documents from TEDCO and make an access decision under the *Act*.

(2) In another case, the Divisional Court affirmed the IPC's interpretation and application of the third party commercial information exemption at section 17 of *FIPPA*. The requester sought access to records confirming agreed upon terms between the Ministry of Natural Resources and a third party relating to allocations for lumber harvesting given out by the ministry for a Crown forest. After considering submissions from the requester and the third party, the ministry issued a decision indicating that it was prepared to grant access to the records.

On appeal from this decision brought by the third party, the IPC upheld the ministry's disclosure decision. Because the records resulted from the give and take of a negotiation, the IPC determined that information was not "supplied" by the third party within the meaning of section 17 and thus could not qualify for exemption under that provision. The Divisional Court held that the Commissioner's conclusions on these issues were reasonable and consistent with the existing jurisprudence.

(3) The Divisional Court also released its decision in a case that had previously gone before the Supreme Court of Canada on a procedural issue of access to the IPC's private record by legal counsel. The requester, a broadcast reporter, sought records relating to allegations of abuse by employees of the Ministry of Community Safety and Correctional Services at a young offender facility in Cornwall. The IPC ordered partial disclosure and affirmed the ministry's decision withholding the bulk of the requested records on various grounds. Both the ministry and the requester applied for judicial review.

The Divisional Court rejected arguments variously raised by the ministry and the requester challenging the IPC's rulings on the exemptions at sections 19 (solicitor-client privilege) and 21 (personal information), as well as the labour relations exclusion at 65(6).

The Court agreed with the IPC that the Crown's letter to an opposing party in litigation did not qualify for exemption under section 19 as part of the Crown counsel's work product, nor was it protected by an implied undertaking rule applicable in civil discovery. The Court also agreed with the IPC that section 19 is capable of protecting Crown counsel records generated in both civil and criminal proceedings and that, in this case, the litigation privilege component of section 19 did not end with the termination of the civil proceedings.

In addition, the Court reaffirmed its deference to the Commissioner's expertise in holding that certain records did not qualify under the personal privacy exemption at section 21.

The Court also upheld the IPC's decision that records concerning the actions of an employee that might lead to vicarious liability are not excluded from the scope of the *Act* under section 65(6). The Court observed that since "Government institutions necessarily act through their employees," the application of this provision "would potentially exclude a large number of records and undermine the public accountability purpose of the *Act*."

Finally, in light of a recent decision of the Ontario Court of Appeal under the *Charter of Rights and Freedoms,* the Court referred back to the IPC the question whether the public interest override at section 23 applied to records found to be exempt under section 19.

(4) In another case involving the "labour relations" exclusion at section 65(6) of *FIPPA,* a requester sought a 2004 Memorandum of Understanding from the Ministry of Health and Long-Term Care describing formal arrangements between the ministry, the Ontario Medical Association (OMA), and the Canadian Medical Protective Association (CMPA) relating to government reimbursement of professional liability insurance premiums paid by physicians. The ministry denied access on the basis that the records were excluded from the *Act* pursuant to section 65(6). The issue on appeal to the IPC was whether the OMA could be considered a "trade union" for the purpose of the "agreement" exception to the exclusion at section 65(7).

The IPC relied on a previous decision of the Ontario Court of Appeal holding that documents generated in the pre-agreement context of negotiations between the ministry and the OMA were excluded from the *Act* as "labour relations" records. The IPC found that it would produce an "absurd" result if collective bargaining discussions between the ministry and the OMA are excluded from the *Act*, yet an agreement resulting from those negotiations is not subject to the same exceptions applicable in other labour relations contexts. The IPC concluded that the OMA was a "trade union" for the purpose of s.65(7) and that, accordingly, the *Act* applied. In addition, although the record contained commercial and financial information within the purview of section 17(1), the IPC found that it did not qualify for exemption because the information was the product of a negotiation process and not "supplied" to the ministry.

The Divisional Court affirmed the IPC's decision on the issues and dismissed the applications of both CMPA and OMA. The Court found that a broad interpretation of "trade union" to include the OMA is consistent with the purpose of *FIPPA* in general and section 65(7)1 in particular. The IPC also reasonably concluded that none of the information in the records qualified for exemption under section 17(1).

(5) In an important case involving the Privacy Commissioner of Canada (the PCC), the Supreme Court of Canada considered whether the PCC has the power to compel the production of documents over which a claim of solicitor-client privilege is asserted in an investigation under the *Personal Information Protection and Electronic Documents Act (PIPEDA).*

In light of the importance of the privilege, privacy and oversight issues involved, several public and quasi-public bodies intervened in the appeal, including the Information Commissioner of Canada, the Information and Privacy Commissioner of Alberta, the New Brunswick Office of the Ombudsman, the Federation of Law Societies, the Advocates' Society, and the Canadian Bar Association. The Information and Privacy Commissioners of Ontario and British Columbia also intervened and filed a joint submission with the Court.

The Supreme Court of Canada concluded that the language of a provision granting a general production power over records in *PIPEDA* was not sufficiently explicit to give the PCC authority to compel production of documents from a third party for which a claim of solicitor-client privilege has been made. The Court concluded that the examination and verification function under that statute is reserved to the courts.

The Court held that the power to order production of records claimed to be privileged in these circumstances is reserved to a body empowered to impartially adjudicate and decide disputed claims over legal rights. In contrast, the PCC is an ombudsman with investigative authority and the power only to recommend disclosure of disputed documents. Because the PCC's legislative functions also include disputing a claim of privilege before the Federal Court and, in limited circumstances, exercising a discretion to disclose information relating to the commission of an offense to the Attorney General of Canada, the Court found that the PCC could become a party adverse in interest to the privilege holder and was thus disabled from examining privileged records for that reason as well.

Significantly, the Supreme Court confirmed that: (i) the right of individuals to access information about themselves in order to verify its accuracy is an important corollary to the protection of privacy; and (ii) that claims of solicitor-client privilege must be independently verified in order to give proper meaning to the right of access to personal information.

(6) And in a very important ruling just days after 2008 ended, the Ontario Court of Appeal held that *MFIPPA* should be interpreted in a way that maximizes the public's right of access to electronically recorded information. The Court restored the IPC's decision on a newspaper reporter's request for access to electronic databases containing information about individuals with whom the Toronto Police have come into contact. The reporter had written a series of articles on "Race and Crime," and wished to test a claim that the Toronto Police do not engage in racial profiling. The requester did not want access to any information that would identify individuals, and requested that any personal identifiers be replaced with randomly generated numbers. The police denied access on the ground that it is not required to create a record under *MFIPPA*.

2008 Judicial Review Statistics

New Judicial Review applications received in 2008:

Launched by:	
Institutions[1]	2
Requesters	0
Affected Parties[2]	4
Total	**6**

Outstanding Judicial Reviews as of December 31, 2008:

Launched by:	
Institutions	12
Requesters	0
Institution and Other Party	2
Affected Parties	5
Total	**19**

Judicial Reviews Closed/Heard in 2008:

Abandoned (Order Stands)[3]	1
Heard but Not Closed (decision pending)[4]	1
Matter Remitted Back to IPC	0
IPC Order/Decision Upheld[5]	6
IPC Order Not Upheld (appeal pending)[6]	1
Total	**9**

1 MO-2294, PO-2694

2 MO-2249-I, PO-2497, PO-2620, PO-2641

3 PO-2641

4 PO-1779 (Ministry's appeal to S.C.C. heard, decision pending)

5 PO-1905 et al. (2 JR applications), PO-2496, PO-2497 (2 JR applications), MO-1966

6 MO-1989 (IPC's/Requester's appeals to C.A. heard, decision pending)

On appeal, the IPC found that the requested information was capable of being produced from existing records by means of computer software, and that replacing individual names with unique numbers does not constitute creating a record. The IPC concluded that the police were not relieved of their obligation to produce the information from a machine readable record, in the requested format, since the process of doing so would not unreasonably interfere with the operations of the police. The police appealed the IPC's decision to the Divisional Court.

On judicial review, the Divisional Court found that the IPC erred in failing to consider whether the record was capable of being produced by means normally used by the institution under the section 2(1) definition of a record in *MFIPPA*. The Court ruled that the police were not required to provide access by replacing individual names with randomly generated, unique numbers.

The Court of Appeal reversed the Divisional Court's ruling. It found that the IPC had considered and made findings concerning all of the requirements of the definition. The Court further held that the definition of "record" was satisfied because "the requested information can be extracted from the police databases by developing an algorithm through the use of technical expertise and software that is normally used by the institution."

The Court agreed that the definition of record must be read "subject to the regulations," which contemplate that institutions may be required to develop new computer programs to respond to requests and are permitted to charge a fee for this purpose, subject to any fee waiver the IPC may impose to relieve a requester of undue financial burden. The Court also noted that because municipal institutions function to serve the public, the *Act's* principle of "presumptive access" means that they ought in general to be open to public scrutiny.

Information about the IPC

Reaching Out

To help fulfil its mandate to educate the public about Ontario's access and privacy laws, the IPC has an extensive *outreach* program that is based on six key elements. These include:

- Targeted outreach through specially focused programs;
- A major public speaking program that is led by Commissioner Ann Cavoukian;
- A school-based initiative entitled *What Students Need to Know about Freedom of Information and Protection of Privacy;*
- An extensive publications program;
- A proactive media relations program; and
- A resource-packed website.

Targeted Outreach

Among the specifically targeted initiatives within the overall corporate outreach program are the *Helping Youths Protect Themselves Online,* the *Right to Know* and the *Reaching Out to Ontario* initiatives.

The *Helping Youths Protect Themselves Online* initiative focuses on getting practical, hands-on information to children and youth. As part of this initiative, the IPC is updating all three of its teachers' guides with lessons specifically addressing issues such as social networking sites and cyberbullying. Work is also continuing with Facebook, one of the largest social networking sites, on producing joint publications and videos that provide practical tips regarding the options youth have with the privacy settings on Facebook. A video featuring Commissioner Cavoukian and Facebook's Chief Privacy Officer, Chris Kelly, providing such practical tips, was among the educational material released in 2008. The IPC also organized and sponsored a highly successful conference, *Youth Privacy Online: Take Control, Make It Your Choice!,* in September 2008. Another IPC project under this initiative was assisting with the formation of the first Ontario chapter of Teenangels. Founded by Parry Aftab, a prominent cyber-lawyer, and executive director of WiredSafety.org, one of the world's oldest and largest cyber-safety groups, Teenangels trains 13- to 18-year-olds to help inform their peers, parents and teachers about online safety. Members of the Teenangels have assisted the IPC in delivering workshops that focus on online privacy and cyberbullying.

The IPC built its 2008 *Right to Know* initiative around three projects. These included a major, sold-out luncheon October 2 that featured a panel which included media representatives, the province's Chief Information and Privacy Officer and Commissioner Cavoukian; a *Right to Know Blitz Day* on September 29, when IPC staff set up information tables in three cities to hand out IPC publications and answer questions from the public; and a special section on the IPC's website devoted to *Right to Know Week* events and practical guides on how to file a freedom of information request and how to appeal to the IPC if you do not receive what you are looking for.

The IPC's *Reaching Out to Ontario (ROTO)* initiative is based on sending a small team to a specific region, where they split up to lead seminars, meet with area school board curriculum staff to discuss the IPC's free teachers' kits, and meet with area media to explain the IPC's role and discuss access and privacy issues. An IPC seminar on the *Personal Health Information Protection Act (PHIPA)* at University Hospital in London in October, part of a *ROTO* initiative, drew a *ROTO*-record 200 area health and privacy professionals, thanks to the help of the London Health Science Centre's privacy team in promoting the seminar.

The IPC also set up information tables at a number of major conferences, particularly those designed for health professionals – including the annual conferences of the Ontario Psychological Association, the Ontario Association of

Community Care Access Centres, the Ontario Pharmacists' Association and the Ontario Long-term Care Association, as well as a major Ontario Hospital Association conference. Information tables were also set up at conferences for municipal politicians and senior staff and at conferences or presentations dealing with access or privacy, including the Ministry of Government Services' annual access and privacy conference.

Speeches and Presentations

The IPC's extensive public speaking program is aimed at building awareness of privacy and access issues among government officials, senior executives and other decision-makers from all sectors, including health care, technology, education, legal, and business, as well as access and privacy professionals, students and parents.

Commissioner Cavoukian gave 40 keynote presentations at major conferences and other events in 2008. These included presentations at:

- The highly successful *Youth Privacy Online: Take Control, Make It Your Choice!* conference in Toronto that the Commissioner sponsored in September, which attracted speakers from across North America and drew a large, engaged audience of professionals who work with children;
- The *Breaking Down Barriers to Freedom of Information: Ensuring the Public's Right to Know* luncheon in Toronto, organized by the IPC and co-sponsored with the Toronto Regional Group of the Institute of Public Administration of Canada;
- A special presentation, entitled, *Radical Pragmatism and Transformative Technologies: The Future of Privacy,* at the 30th International Conference of Data Protection and Privacy Commissioners in Strasbourg, France; and
- A keynote speech, *New Ways of Dealing with Privacy: Think Positive-Sum, Not Zero-Sum,* at the International Association of Privacy Professionals' Canadian Privacy Summit in Toronto.
- Among the many other presentations made by the Commissioner were those at a number of universities, and at annual conferences, including those of the International Association of Business Communicators, and the Risk and Insurance Management Society of Canada. Other presentations included those to the Ontario Bar Association, Research in Motion, a Women's Executive Network Webinar, and the joint privacy task force set up by the Canadian Institute of Chartered Accountants and the American Institute of Public Accountants. She was also a keynote speaker at a number of health conferences, including the *RFID and Privacy – Guidance for Health-Care Providers* conference in Toronto jointly sponsored by the IPC and HP.

Assistant Commissioners Ken Anderson and Brian Beamish, and senior IPC staff, also made a number of presentations.

School Program

The IPC's popular school program, *What Students Need to Know About Freedom of Information and Protection of Privacy,* offers free teachers' kits tailored to three levels: the Grade 5 social studies curriculum (where students first study government), the Grade 10 civics curriculum (a mandatory subject for all students), and Grade 11 and 12 history and law courses.

All three teachers' guides were developed by the IPC with the aid of curriculum professionals and classroom teachers. Additional lessons were added in 2007 and a full major update is now underway.

Media Relations

The IPC has a proactive media relations program to help raise the media's – and thus the public's – awareness of access and privacy issues.

This program includes articles written by the Commissioner that are published in various print and online media; presentations to editorial boards, newsroom teams and media students; and letters to the editor by the Commissioner to support, clarify or correct points made in editorials, columns and news reports about access or privacy issues. A number of

major newspapers in Canada and beyond (including the *New York Times*) published letters by the Commissioner in 2008.

Commissioner Cavoukian also gave 85 interviews to media organizations from across Canada and around the world in 2008. IPC staff assisted more than 200 journalists who requested interviews or background information, or who had general inquiries about access and privacy, including where to file freedom of information requests to obtain specific types of information.

Commissioner Cavoukian also issued 18 news releases in 2008.

IPC Website

The IPC has an extensive website (www.ipc.on.ca) that provides access to IPC publications, videos, orders and privacy investigation reports. It also provides direct online links to the three Ontario *Acts* governing access and privacy, answers to frequently asked questions, educational material, news releases, selected speeches, forms, and much more.

IPC Publications

The IPC papers and videos released in 2008, in chronological order, include:

- *RFID and Privacy: Guidance for Health-Care Providers* (January);
- *The Commissioner's 2007 Annual Report* (May);
- *Compliance Statistics: A look at the compliance rates of Government organizations* (an adjunct publication to the 2007 Annual Report) (May);
- *Privacy in the Clouds: Privacy and Digital Identity – Implications for the Internet* (May);
- *Transformative Technologies Deliver Both Security and Privacy: Think Positive-Sum not Zero-Sum* (July);
- *Fingerprint Biometric Systems: Ask the Right Questions Before You Deploy* (July);
- *Your Rights under Ontario's Freedom of Information Laws* (July);
- *How to Protect your Privacy on Facebook* (updated in July and November);
- *Be a Player: Take Control of Your Privacy on Facebook* (**video**); (August);
- *Viacom vs. Google: Placing the Privacy of Users at Risk* (August);
- *Privacy and Radical Pragmatism: Change the Paradigm* (August);
- *IPC Perspectives* (August);
- *How to Preserve Freedom and Liberty: Design Intelligent Agents to be Smart and Respectful of Privacy* (August);
- *If you wanted to know...Canada's National Do Not Call List* (September);
- *What's New Again? Security Measures Must Be Real – Not Illusory* (October);
- *BlackBerry® Cleaning: Tips on How to Wipe Your Device Clean of Personal Data* (October, updated in December);
- *Practice Tool for Exercising Discretion: Emergency Disclosure of Personal Information by Universities, Colleges and other Educational Institutions* (October);
- *Fingerprint Biometrics: Address Privacy Before Deployment* (November);
- *If you wanted to know...What if you are a victim of identity theft or your credit/bank cards are lost or stolen?* (December);
- *If you wanted to know...Can I get health information about my deceased relative?* (December);
- *Fact Sheet 15: Obtaining Personal Health Information About a Deceased Relative* (December).

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.

Part of the IPC's mandate under the *Acts* is to offer comment on the privacy and access implications of proposed Government legislation or programs and on existing or proposed information practices of health information custodians.

In 2008, the IPC commented on the following:

Provincial Consultations

Ministry of Community and Social Services:

- Bill 12, *Access to Adoption Records Act (Vital Statistics Statue Law Amendment), 2008;*

Ministry of Transportation:

- *Bill 85 Photo Card Act, 2008.*

Municipal Consultations

City of Mississauga, City of Timmins, Greater Sudbury Policy Services, Municipality of North Perth, and City of Orillia:

- IPC's *Guidelines for the Use of Video Surveillance Cameras in Public Places;*

City of Ottawa:

- Aerial Imagery and Remotely Sensed Data for the Purpose of Photogrammetry.

Health Information Custodian Consultations

Ministry of Health and Long-Term Care:

- The Ontario Laboratories Information System;
- Expansion of the Drug Profile Viewer (DPV) System.

Submissions and Special Reports

Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report – Privacy Investigation Report MC07-68, March 3, 2008.

Recommendations for Amendments to the Personal Health Information Protection Act, 2004, August 28, 2008.

Submission from the Information and Privacy Commissioner/Ontario on Bill 85, An Act to permit the issuance of photo cards to residents of Ontario and to make complementary amendments to the Highway Traffic Act, October 20, 2008.

The special report and submissions can be found in the *Resources* section of the IPC's website at www.ipc.on.ca.

FINANCIAL STATEMENT

	2008-2009 Estimates	2007-2008 Estimates	2007-2008 Actual
	$	$	$
Salaries and Wages	9,359,000	8,773,000	8,491,382
Employee Benefits	2,105,800	1,886,200	1,671,810
Transportation and Communications	345,000	323,700	326,511
Services	1,699,800	1,523,800	1,826,643
Supplies and Equipment	257,500	274,800	268,609
Total	**13,767,100**	**12,781,500**	**12,584,956**

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

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

WHERE TO FIND MORE INFORMATION ABOUT THE IPC

Extended charts of compliance statistics for municipalities (sorted by population), police services and school boards are available as part of a special report on the IPC's website, **www.ipc.on.ca**. This special report, *A More Detailed Look at Compliance Rates and other 2008 Access and Privacy Statistics*, has been posted as an adjunct to the Annual Report. It also includes additional charts related to freedom of information appeals and privacy complaints filed with the IPC (including complaints filed under *PHIPA*), as well as information about the IPC's Role and Mandate, the Purposes of the *Acts*, an organizational chart, and a list showing which IPC employees received more than $100,000 in salary and benefits for the calendar year ending December 31, 2008.

DESIGN: Bus Stop Design + Communications www.busstopdesign.com PRINTED IN CANADA: Clockwork Productions Inc.

Information and Privacy Commissioner of Ontario/Canada
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8

Tel: 416 326 3333
Fax: 416 325 9195

1 800 387 0073
TTY: 416 325 7539

www.ipc.on.ca