INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO | 2011 ANNUAL REPORT

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

June 4, 2012

The Honourable Dave Levac
Speaker of the Legislative Assembly of Ontario

I have the honour to present the 2011 Annual Report of the Information and Privacy Commissioner of Ontario to the Legislative Assembly.

This report covers the period from January 1 to December 31, 2011.

Please note that additional reporting from 2011, including the full array of statistics, analysis and supporting documents, may be found within our online Annual Report section at www.ipc.on.ca.

Sincerely yours,

Ann Cavoukian, Ph.D.
Commissioner

Enclosure

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

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

416-326-3333
1-800-387-0073
Fax/Téléc: 416-325-9195
TTY: 416-325-9539
http://www.ipc.on.ca

Commissioner's Message

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner,
Ontario, Canada

2011 started off as a very promising year for advances in both access and privacy, but by year's end, I found myself once again (as I have many times in the past) having to marshal my resources to come to the defence of privacy. That is why I chose ***Ever Vigilant*** as the theme for this year's Annual Report.

While *Privacy by Design* (*PbD*) continues to grow at breakneck speed globally, having been recognized as the international standard for protecting privacy, and translated into 25 languages — a very real threat to privacy was emerging right here in Canada.

The anticipated reintroduction of so-called "lawful access" legislation, which died on the Order Paper when a federal election was called in March, commanded much of my attention this past fall. (At the time of this Annual Report, it had been presented to the new Parliament as Bill C-30). My office quickly launched an educational campaign to raise awareness about the serious privacy concerns I had about this proposed legislation which, in my view, would represent nothing less than a system of state-sanctioned surveillance.

With regards to access to information, I am happy to report that it has been another productive year. I spent much of 2011 consulting, collaborating and cooperating with Ontario's hospitals to help them prepare for operating under the *Freedom of Information and Protection of Privacy Act (FIPPA)*, which I have been looking forward to for many years. My message to them was to take a proactive, rather than a reactive approach to public disclosure, releasing information as part of an automatic process.

Further, I have been greatly encouraged by the ever-growing concept of Open Data. I am very supportive of this concept which calls for certain types of non-personal, general records to be made freely available to everyone to use and republish, without restriction.

All in all, 2011 proved to be a balanced year — it was the best of times, it was the worst of times; a year of great successes and yet, tremendous challenges.

Lawful Access

At the beginning of this year, I could not have been happier with the progress we had made in advancing *PbD* globally. In fact, I was told on more than one occasion that it was "raining *PbD*." This success gave me great faith that we could indeed protect privacy in this ever increasing world of online connectivity. That is why I was truly taken aback when I discovered mid-year that one of the greatest threats to privacy was materializing from within our very own country.

During the federal election, the government pledged to reintroduce lawful access legislation if re-elected. If passed in its original form, police would be given the ability to access subscriber data about identifiable individuals held by telecommunications service providers, at times without a warrant or any judicial oversight. This should be of concern to all of us living in a free and democratic society.

I was taken aback when the Honourable Vic Toews, federal Minister of Public Safety, made the claim that the personal information in question was no different than "information you would find in a phone book." Nothing could be further from the truth! This assertion provoked me to draft an Open

Letter to the minister. I also engaged the public by writing two op-eds for the National Post and maintained a running dialogue with the minister in a series of letters to the editor, where we respectfully exchanged our divergent points of view.

My message to the minister, and those who supported his view, was that the information in question was *NOT* the same as phone book information — far from it. Subscriber data, consisting of six fields — your IP address, email address and four other fields of personally identifiable information, goes far beyond what is available in a phone book. Moreover, it gets farther away from the simple assertion that it is the same as phone book information, once you take data linkages into account. New analytic tools and algorithms now make it possible to not only to link a number like an IP address with an identifiable individual, but also to combine information from multiple sources, ultimately creating a detailed personal profile of an identifiable individual.

Privacy by Design: Time to Take Control (2011)

Privacy by Design in 2011

In 2011, more organizations than ever had operationalized the Principles of *PbD*. This helped to put to rest the frequently cited myth that a focus on privacy will somehow stifle innovation. Not true. In fact, the reverse is true – delivering on the promise of fully functional systems (including strong privacy protection), demands the highest levels of innovation imaginable. As a privacy professional, I believe that the widespread accommodation of privacy as a core system requirement is poised to become one of the key trends of our time – and justifiably so.

Privacy by ReDesign

PbD saw its first spinoff in 2011 with the introduction of *Privacy by ReDesign* (*PbRD*) which provided a framework for improving privacy protection in existing mature and legacy systems, where the opportunity to embed privacy from the outset had long passed. Introduced in a white paper co-authored with Dr. Marilyn Prosch, *Privacy by ReDesign: Building a Better Legacy*, *PbRD* is a transformative process which offers a framework for undertaking a proactive assessment of existing gaps, and how an organization can address those gaps systematically based on the 3 R's — *Rethink*, *Redesign* and *Revive*.

Privacy by Design Abroad

Considerable advocacy for *PbD* took place around the world in 2011, with a number of remarkable highlights.

- The European Union announced the *Privacy and Data Protection Impact Assessment Framework for RFID Applications* — a milestone agreement to put consumers' privacy at the centre of smart tag technology using a *Privacy by Design* solution.
- U.S. Senators John Kerry and John McCain cited *Privacy by Design* in their *Commercial Privacy Bill of Rights*.

Privacy by ReDesign — A Transformative Process (Mexico City), Nov 1, 2011: Peter Hustinx, European Data Protection Supervisor; Mary Ellen Callahan, Chief Privacy Officer, U.S. Department of Homeland Security; Dr. Ann Cavoukian, Information & Privacy Commissioner, Ontario; Tom Marinelli, Executive Vice President and Chief Information Officer, Ontario Lottery and Gaming Corporation; Jules Polonetsky, Co-Chair and Director of the Future of Privacy Forum

- The inaugural *Develop for Privacy Challenge* organized by the American Civil Liberties Union of Northern California and Washington, encouraged developers of mobile applications to embed *PbD* in new and innovative ways, to allow users to take control of their information.
- The California Public Utility Commission recognized that, *"…the PbD* methodology offers a promising approach to ensuring that data practices promote privacy, not just in the FIP of data minimization, but in all aspects of privacy planning."
- There were many collaborative *PbD* projects in 2011. My office announced a partnership with San Diego Gas & Electric (a division of Sempra) to embed *PbD* into their Smart Pricing Program; we released a joint paper with the International Working Group on Data Protection in Telecommunications, Berlin on *Privacy by Design and Smart Metering: Minimize Personal Information to Maintain Privacy*; and we began work on a new paper based on European research and utility companies' experience embedding *PbD* into their smart meter implementation, to be published in 2012.

Privacy by Design at Home

My office also focused considerable energy in 2011 on advancing *PbD* in Ontario by leveraging partnerships to help shape the future of privacy.

Beginning in January, I called 2011 the "Year of the Engineer." I felt very strongly that it was time to start reaching out to those who actually designed and built the systems and technology upon which we increasingly rely. I spent much of the year bringing *PbD* to engineers and developers, in an effort to operationalize it, at dozens of the world's most innovative "tech" firms.

In February, we published our third paper on privacy and the Smart Grid, *Operationalizing Privacy by Design: The Ontario Smart Grid Case Study*, which provided examples of how utilities, vendors and service providers could utilize the best practices for Smart Grid *Privacy by Design* in the implementation of Smart Grid systems.

In May, the Ontario Lottery and Gaming Corporation rolled out its long-awaited facial recognition program at all 27 of its gambling facilities in Ontario. I am proud to have played a small role in the development of this system — along with University of Toronto researchers Professor Kostas Plataniotis and Dr. Karl Martin — because it offers dramatically improved privacy protection over simple facial recognition, without compromising any functionality, security or performance — a real-world example of *PbD*.

In June, we undertook a collaborative effort with renowned digital identity expert Kim Cameron issuing a white paper entitled, *Wi-Fi Positioning Systems: Beware of Unintended Consequences — Issues Involving the Unforeseen Uses of Pre-existing Architecture*. In this paper we examined the unintended consequences for privacy that arise from tracking individuals' geolocation data through their mobile devices.

In September, we issued a joint white paper with IBM, *Privacy by Design: From Policy to Practice*, which examined how IBM operationalized *PbD* within its business operations and enabled process improvements that demonstrated reduced operational costs and documented compliance.

Additionally in September, we took *PbD* into the field of regulatory structures, issuing a white paper entitled, *Privacy by Design in Law, Policy and Practice: A White Paper for Regulators, Decision-makers and Policy-makers*, which examined incorporating *PbD* into policy, law, and practice.

We accomplished a great deal this year with regards to *PbD*, yet so much remains to be done — our work has just begun. My office will continue to remain committed to advancing the understanding of the application of *PbD*, here at home, and around the world.

Hospitals Under *FIPPA*

When the *Broader Public Sector Accountability Act* received Royal Assent in late 2010, I was delighted that Ontario had finally joined the other provinces in bringing our hospitals under freedom of information (FOI) legislation.

While this new legislation would not apply to hospitals until January 1, 2012, I took advantage of the opportunity in 2011 to reach out to hospitals, in order to help them prepare for operating under *FIPPA*. One of my first actions in this regard was to publish two documents, *Applying PHIPA and FIPPA to Personal Health Information: Guidance for Hospitals* and *Freedom of Information at Ontario Hospitals: Frequently Asked Questions*.

Further, I also spent much of the year giving presentations and meeting with the Boards of Directors at various hospitals to ensure that they understood the meaning of the new legislation. Most importantly, I wanted to dispel any fears they may have had that FOI legislation would interfere with the normal operations of their hospitals, or the delivery of health care.

Open Data

For the first time in the history of the IPC, we will make available raw statistics in our online Annual Report. Academics, researchers, policy-makers, and the public, will have access to data such as *Access Requests* and *Response Rate Compliance*. These data can also be cross-referenced against specific public institutions and other variables allowing for some very in-depth examination and research. I am very excited by this new endeavour as it brings my office even closer to the true spirit of access and freedom of information.

Right to Know Week 2011, Mount Sinai Hospital: Joseph Mapa, President & CEO, Mount Sinai Hospital; Rob Devitt, President & CEO, Toronto East General Hospital; Dr. Ann Cavoukian, Information & Privacy Commissioner, Ontario, Canada; Tom Closson, President, Ontario Hospital Association

My Personal Thank You

As always, I would like to give my heartfelt thanks to all of my staff, whose dedication and hard work has made this office a first-class agency, 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 I have the honour of working with. I truly believe that the people of Ontario are very fortunate to have such talented professionals working on their behalf. I unquestionably have the best team, for which I am very grateful! You have my utmost thanks, now, as always.

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner
Ontario, Canada

TABLE OF CONTENTS

Key Issues

Beware of "Surveillance by Design:" Proposed Federal Legislation Threatens Freedom and Privacy

The theme of my 2011 Annual Report — *Ever Vigilant* — was chosen in large part because this year Ontarians faced what I consider to be one of the most invasive threats to our privacy and freedom that I have encountered in 25 years of safeguarding citizens' rights and championing openness and transparency in government.

That threat presented itself as lawful access legislation proposed by the federal government. The legislation was designed to provide police with much greater ability to access and track information about identifiable individuals via the communications technologies that we use every day, such as the Internet, smart phones, and other mobile devices, and at times, without a warrant or any judicial authorization. Telecommunications service providers would also be required to build and maintain intercept capabilities in their networks for use by police.

It my view, it is highly misleading to simply call such legislation "lawful access" or to champion it as a child protection measure. The broad powers proposed represent much more — they represent a looming system of "*Surveillance by Design*."

Let me be clear, I hold our police services in the highest regard and have a deep appreciation for the critical public safety functions they perform. However, we must be vigilant in not allowing the investigative needs of police forces to outstrip our constitutional right "to be secure against unreasonable search and seizure."

In the absence of significant amendments, such a proposal risks intrusions on the privacy of too many innocent individuals. Electronic scrutiny of an individual paints a detailed and revealing digital biography and is likely to capture personal information of family, friends, neighbours, colleagues and acquaintances. Properly supervised, surveillance powers can be invaluable to law enforcement. However, the consequences of unsupervised powers can be devastating to innocent individuals subjected to unwarranted suspicions, to poorly-handled evidence, or to erroneous conclusions hastily drawn.

So disturbing was the legislation that I — and every privacy commissioner in Canada — wrote to the federal Deputy Minister of Public Safety in March 2011, detailing our concerns. We provided copies of our joint letter to the House of Commons Standing Committee on Public Safety and National Security and the Standing Committee on Justice and Human Rights.

The legislation (originally referred to as Bills C-50, C-51 and C-52) died on the Order Paper when Parliament was dissolved in March 2011. However, the government pledged to reintroduce it on its re-election. (At the time of this Annual Report, the legislation was reintroduced as Bill C-30. More information is available at www.realprivacy.ca.)

Sensing a critical opportunity to engage the public and the government before the legislation was reintroduced, I decided to write my own 22-page Open Letter to the federal Minister of Public Safety and the federal Minister of Justice and Attorney General of Canada to share my concerns. I also authored several op-eds in the fall of 2011. Then, in December 2011, I decided to expand my public educational campaign, beginning with a Symposium with highly-respected thought leaders scheduled for January 2012 — "Beware of 'Surveillance by Design:' Standing Up for Freedom and Privacy." I also committed to urging Ontarians, and indeed all Canadians, to write to their Member of Parliament to share their concerns about the proposed legislation. Finally, I instructed my staff to develop concrete recommendations so that the bill could be amended to ensure that Canadians will enjoy a modern, effective, and comprehensive approach to law enforcement in which privacy protection and government transparency are built directly into the legislation.

Privacy Engineers Wanted

We need better options for securing the Internet. Instead of looking primarily for top-down government intervention, we can enlist the operators and users themselves.

Jonathan Zittrain, *Scientific American* article 2011

Privacy by Design has reached a critical stage of evolution. The *PbD* approach and principles have become globally recognized as essential to meet current needs for:

- privacy by default, not by disaster;
- strong end-to-end safeguards;
- improved user engagement;
- real transparency and accountability;
- proactive privacy leadership;
- systematic, verifiable methods; and
- practical and demonstrable results.

Recognized as an international standard by international privacy and data protection commissioners in October 2010, *Privacy by Design* Foundational Principles have since been embraced by public policy-makers, legislators, industry groups and associations as integral to their efforts to update 21st century information privacy governance systems.

YOU ARE THE ENGINEER

As Lawrence Lessig famously wrote, "Code is Law." By extension, he showed that we could — and should — architect cyberspace to protect fundamental values. Failure to build those values in — and build them in early — may lead to negative unintended consequences. The privacy engineer's task, then, is to embed values and preferences into the design and operation of their information technologies, systems, and infrastructures.

Privacy by Design principles can help by stimulating:

- clear privacy goal-setting;
- systematic, verifiable methodologies;
- practical, demonstrable results; and
- vision, creativity, and innovation.

We want to empower engineers of all stripes to develop and adopt privacy best practices, share implementation experiences, and be recognized for their innovative solutions.

This is what I mean by "Year of the Engineer!"

The next stage of *Privacy by Design's* evolution is to translate its principles into more prescriptive requirements, specifications, standards, best practices, and operational performance criteria. For this task, specialized help is needed. The rise of the Chief Privacy Officer (CPO) role in organizations is testament to the strategic importance of good information management and the demand for CPO skill sets. Privacy management as a distinct discipline is becoming more standardized and professionalized, and there is a shortage of skilled privacy engineers and architects.

That's why I decided to make 2011 my personal "Year of the Engineer." In an effort to reach out to a wider spectrum of expert participants, 2011 saw continuous efforts from my office to engage:

- tech media;
- mobile app-developers;
- research labs and groups;
- local startups and multinationals;
- industry consortia;
- standards-setting groups;
- information and security architects; and
- engineers (broadly understood)

from around the globe in a dialogue about translating the 7 Foundational Principles of *PbD* into project requirements, procurements specifications, and positive-sum operational results.

You are Your Password

"Biometrics" is a fancy word for body measurements. The more unique and stable the biometrics, the better suited it may be to verify the identity of individuals. We have come a long way from signature and fingerprint cards. Today's biometrics are entirely digital and rely on computer systems to detect, measure, and match "fresh" body measurements (physical or behavioural) against stored "reference" samples, and to then take action based upon that match or non-match.

In fiction, biometrics are ubiquitous: the secret agent fails to access the enemy's high-security lab because entry is by authenticated iris scan only; the crime scene investigator compares a grainy photo of a suspect to an enormous database and in mere seconds, scores a hit; and the defence attorney derails her client's DNA-evidence-based conviction by unearthing an identical twin!

Reality is catching up to those movie scenarios; it is becoming more and more possible to automatically identify people in locations and environments where they don't want — or expect to be — identified.

Biometrics *are* personal information — your face, your fingerprint, or your pattern IS you. By extension, any data derived from your face or other biometric that are used to verify or identify you are also personal information. You have privacy rights in biometric data.

Some biometrics are ubiquitous and semi-public, for example, your face is visible to all, and your fingers leave prints everywhere, you shed DNA everywhere you go. Biometrics offer marvelous conveniences and benefits, from catching criminals to securing access to physical and electronic resources. We are fast approaching the era in which our daily activities, travels, and behaviours will be automatically identified, tracked and profiled using biometrics — without our knowledge or consent.

Fortunately, privacy solutions exist, but they must be embedded early into the biometric matching system to be effective. When deployed properly, Biometric Encryption (BE) defeats many of the major privacy concerns surrounding the collection and (mis)use of biometrics: there is no retention of a biometric image or template, which significantly enhances security and diminishes the risk of data-matching against other databases. BE can be deployed with no meaningful loss of system functionality.

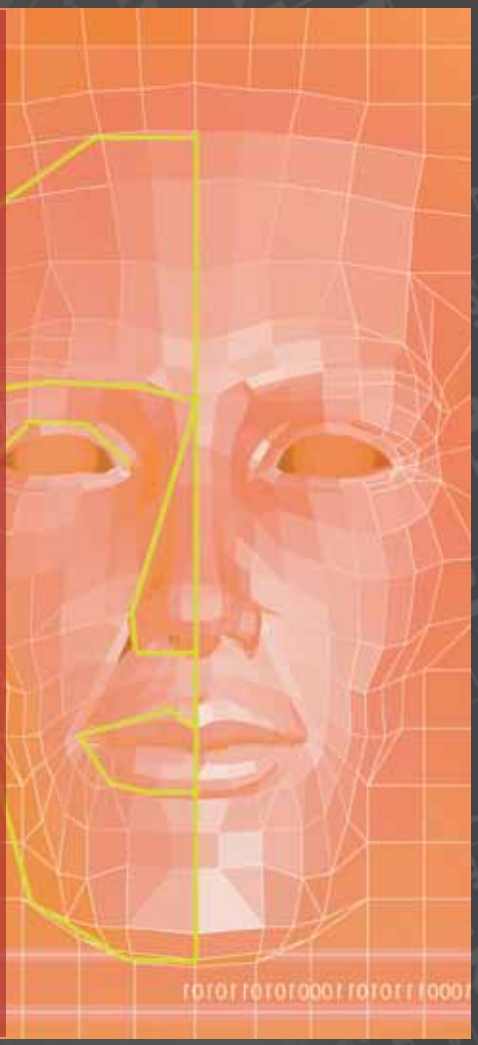
ONTARIO LOTTERY AND GAMING PROJECT

The challenge was to develop a face recognition system for casinos and gaming facilities capable of identifying 15,000 individual volunteer participants in a self-exclusion program for problem gamblers, while protecting the privacy of the other hundreds of thousands of patrons who are not on the list.

The dual goals were to protect the privacy of all people photographed — both those in the database and those visiting Ontario Lottery and Gaming facilities, and achieve a high accuracy rate in detecting, through the facial recognition system, people enrolled in the self-exclusion program. It was also important to keep existing and new data private and secure — in the event the information were to fall into the wrong hands, no one's identity would be compromised.

The privacy component of the system was designed by biometrics engineers at the University of Toronto Electrical and Computer Engineering Department, led by Professor Kostas Plataniotis with Dr. Karl Martin, and developed with video surveillance and biometric iView Systems.

The first-of–a-kind technology, coupled with refreshments to the photographic elements, achieves a best-case results of 91 per cent identification. A 2007 German test project achieved a 30-60 per cent accuracy rate, making this made-in-Ontario solution the most privacy-protected system using BE, in the world.



Your Mobile Device *is* You

Mobile communication devices are the new personal computer, and they bring with them enormous challenges for information security and privacy, and for usability and functionality. Last year the newswires were rife with mobile privacy horror stories, including:

- secret recording and backup of location history;
- poor default settings for location-based services;
- misleading and/or rogue applications;
- discovery of mobile device rootkits; and
- revelations of address book "snarfing."

The entire mobile ecosystem is facing unprecedented public attention and regulatory scrutiny regarding information management and privacy practices of ecosystem participants and it is not hard to understand why: mobile devices reveal highly personal information about their owners.

Spurred, in part, by public revelations (and poor transparency) of privacy-invasive practices, much quality research on current mobile practices was

published last year. Voluntary guidelines for the mobile sector emerged under the leadership of the Future of Privacy Forum, the GSMA, the Center for Democracy and Technology, the Digital Advertising Alliance, the Federal Trade Commission and the Federal Communications Commission, among others.

In December 2010, I weighed in with *The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users* — an effort to summarize the privacy risks, challenges and solutions facing the mobile ecosystem. The result of a roundtable workshop of experts convened by Professor Marilyn Prosch at the *Privacy by Design* lab at Arizona University, the paper groups privacy challenges into six categories and more than two dozen *PbD* recommendations targeted at device manufacturers, operating system and platform developers, network providers, application developers and processors, and consumers — all key stakeholders in the mobile ecosystem.

Systemic risks were also highlighted in our June 2011 paper, *Wi-Fi Positioning Systems: Beware of Unintended Consequences — Issues Involving the Unforeseen Uses of Pre-existing Architecture*, which explored the implications of a wireless communications infrastructure that, by default, could betray the identity, location and behaviour of connected devices.

In Summer 2011, we co-hosted, with the American Civil Liberties Union and The Tor Project, the first-ever *Developer Challenge for Mobile Apps*, a competition for application developers to build solutions for mobile privacy concerns, results of which were announced in Las Vegas at DEFCON and Black Hat security conferences.

In September 2011, we published *Safeguarding Personal Health Information When Using Mobile Devices for Research Purposes*, which provides guidance to custodians, researchers and research ethics boards for understanding and fulfilling their obligations with respect to safeguarding personal health information that is collected, used and disclosed for research purposes.

In November 2011, we followed up with *Mobile Near Field Communications (NFC) "Tap 'n Go" — Keep it Secure & Private*, that examines Near Field Communications (NFC) technologies and their growing deployment in mobile devices, especially smartphones. We identified the main privacy and security risks associated with using RFID chips and readers embedded in mobile handsets, and offered solutions for NFC device and application developers that are informed by the 7 Foundational Principles of *Privacy by Design*.

Good user awareness and education, along with proper device design and configuration could go a long way to defeating many, if not all, mobile privacy risks, but some risks and challenges remain at the system level, requiring cooperation and standardization by mobile stakeholders.

Access by Design

I developed *Access by Design* (*AbD*) because I wanted to address the way that government and citizens interacted and to encourage public institutions to be proactive, rather than reactive, in their approach to disclosure of information. In short, I wanted governments to recognize that publicly-held information is a public good, and that access should be provided *by default* — as part of an automatic process. However, as I have said before, *AbD* goes much further than just routine disclosure. Consisting of 7 Fundamental Principles, *AbD* also calls for a more responsive and efficient government that forges collaborative relationships with citizens, the private sector, and other public institutions. The ubiquitous nature of the Web, and accompanying technologies, has driven dramatic new increases in public demand for government-held information, giving a new dimension to civic participation and allowing for greater citizen engagement in policy-making and service delivery.

I am also pleased to report that 2011 saw my office issue an Order that addresses some of challenges and principles laid out by *AbD*. On October 14, 2011, PO-3002 addressed the question of fees, which is reflected in *Principle No. 6 of AbD: Making Access Truly Accessible.*

In this case, an appellant requested access to a report that the Landlord and Tenant Board had previously provided to him on an ongoing basis, which was produced by electronic means. After it migrated to a new electronic case management system, the Board sought to impose a fee of $16,349 on the appellant to cover the cost of developing the same report. As Commissioner, I found this fee estimate to be completely unreasonable and disallowed it in its entirety. I ordered the Board to produce the report and to provide it to the appellant without charging a fee. It was my expectation that the Board would ensure that any new systems put in place would continue to produce the same report it had in the past.

If we are to make public information truly accessible, we cannot place obstacles such as unreasonable fees for information requests. Information has been called the lifeblood of the 21st century economy. Not only is it essential for government institutions to place public data on public databases, they must also ensure that the information is accessible. We need to embrace this new culture by making data readily available to the public and to join the rest of the world in providing opportunities for the public and private sector to work collaboratively with government in utilizing public data, with many potential benefits for our society and the economy as a whole.

Hospitals under *FIPPA*

My office spent much of 2011 networking and reaching out to hospitals all across Ontario in order to assist them in preparing for coming under the *Freedom of Information and Protection of Privacy Act* (*FIPPA*) on January 1, 2012. This is a historical milestone in the evolution of freedom of information in Ontario as it moved the province towards completing the circle by providing the citizens of Ontario a wide range of access to records held by public institutions that are funded by public dollars.

As a first step in assisting hospitals to prepare for this new legislation, my office published two documents early in 2011. The first, *Applying PHIPA and FIPPA to Personal Health Information: Guidance for Hospitals*, is intended to provide guidance for hospitals about the application of *PHIPA* and *FIPPA* to personal health information within the context of their operations. The second publication, *Freedom of Information at Ontario Hospitals: Frequently Asked Questions*, is a compilation of the most commonly asked questions regarding the new legislation, such as: "When will freedom of information be applied to hospitals?"; "Why have hospitals been added under the legislation?"; and "What changes with the introduction of hospitals to *FIPPA*?"

My staff and I also spent much of the year giving presentations and meeting with hospital officials to ensure they were ready for the upcoming changes. A few of the organizations that we worked with include the Ontario Hospital Association, Trillium Health Centre, University Health Network, Mount Sinai Hospital, St. Michael's Hospital and SickKids. Additionally, we also reached out past the Greater Toronto Area and engaged with over a dozen hospitals across Ontario during the *2011 Right to Know Week* by hosting educational outreach tables. This was a major effort by my staff given Ontario's geographic size, but we were nevertheless successful in reassuring hospitals and their staff that the new legislation would *not* interfere with the delivery of health care, but would provide another layer of legitimacy in making our public institutions more transparent and accountable.

Open Data

As every year passes, more and more jurisdictions around the world are joining the Open Data movement, which in its essence, is an initiative that began with the idea that certain types of *non-personal* government-held information should be made freely available to everyone to use and republish. The ubiquitous nature of the Web, and accompanying technologies, has driven dramatic new increases in public demand for government-held information, providing a new dimension to civic participation, and redefining the significance of freedom of information legislation.

With so much data now available, and in so many different formats, individuals, community groups and researchers now have the power to use public information for a variety of purposes — for example, to spot inefficiencies in government services, and make recommendations directly to the offices responsible for those services. Further,

our economy also benefits by giving businesses access to a wealth of new information from which to improve, or create new products and services, thus driving the potential to create entire new products where none existed before.

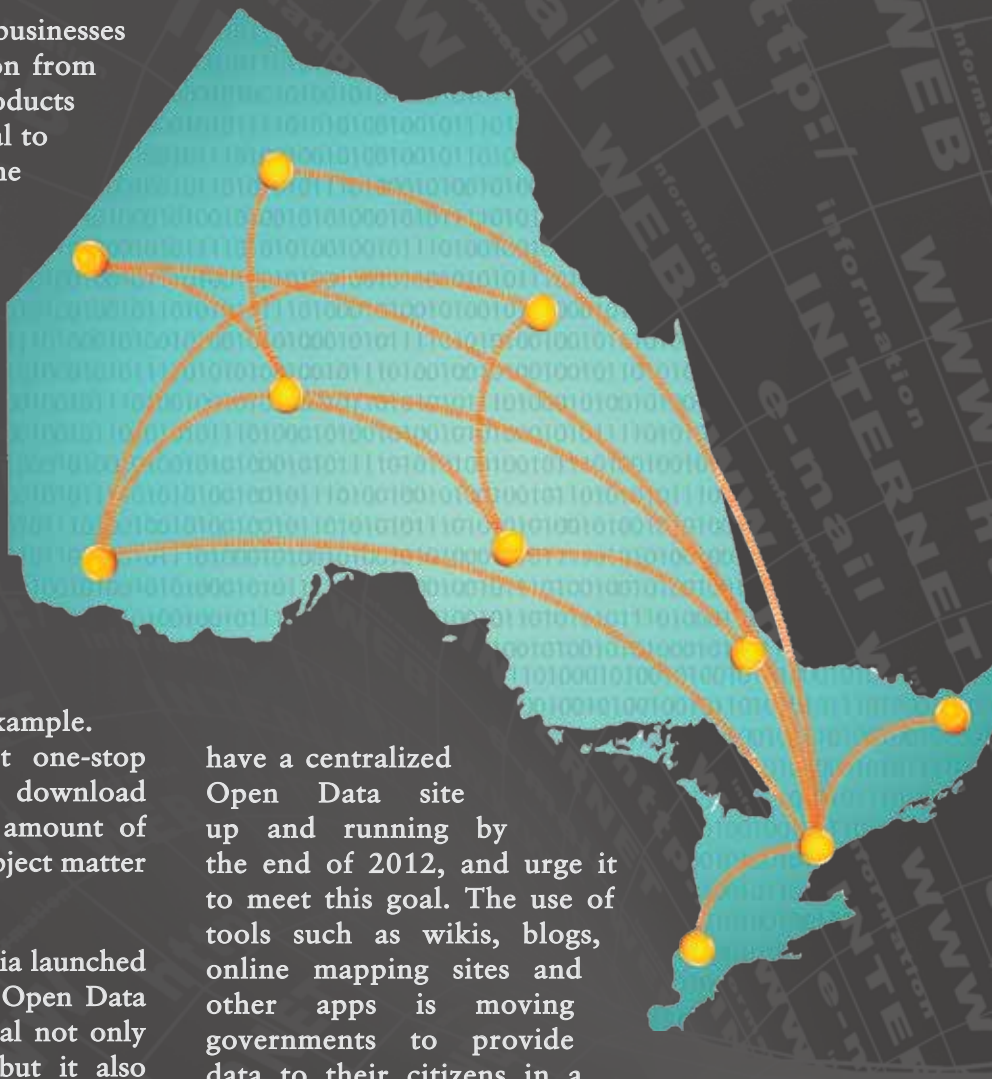
In 2011, the Government of Canada joined a number of other nations when it launched its own Open Data Pilot website as part of a commitment to Open Government with a vast array of datasets covering topics such as immigration, forestry and transportation.

There are also a number of municipalities in Ontario featuring Open Data portals with the City of Toronto setting a world-class example. DataTO.org is a clean and efficient one-stop website where anyone can find and download datasets that cover an unbelievable amount of information covering almost every subject matter relevant to the city.

At the provincial level, British Columbia launched Canada's first provincial government Open Data site known as DataBC. This data portal not only offers a large number of datasets, but it also provides computer apps and other programs featuring information ranging from environmental data, court services and demographics.

While Ontario still lacks a centralized data portal, there has been much discussion about it over the last year. I believe that Ontario needs to establish its own Open Data portal so that we may continue to demonstrate that we are a world leader in access to information.

The main focus of Government 2.0 is to engage citizens, and it is time for Ontario to enter the 21st century by providing Open Data and the right to open government for all its citizens. I am optimistic that the Government of Ontario can have a centralized Open Data site up and running by the end of 2012, and urge it to meet this goal. The use of tools such as wikis, blogs, online mapping sites and other apps is moving governments to provide data to their citizens in a manner that is efficient and useful. I believe this is completely possible. We can start with readily available data and continue to add more and more datasets as time goes on, creating an Open Data site that can be the envy of the world.



PHIPA IN 2011

The following are highlights from 2011 that are relevant to the *Personal Health Information Protection Act* (*PHIPA*), which my office has overseen since it was first passed in 2004.

Health Order No. 11 (HO-011) — Cancer Care Ontario

Following the loss of screening reports containing the personal health information (PHI) of over 7,000 Ontarians, on October 13, 2011, I issued Health Order No. 11 (HO-011) ordering Cancer Care Ontario (CCO) to discontinue its practice of transferring paper-based screening reports containing PHI to primary care physicians by courier.

In issuing Order HO-011, I took into consideration a number of factors, including the size, resources and sophistication of CCO; the persons or organizations to whom the records of PHI were being transferred (the records were being transferred to primary care physicians rather than to individuals who may not have the technology necessary to access the information in electronic format); the availability of alternative methods to securely transfer the records of PHI in electronic format; the number of individuals whose PHI was contained in the records (a single screening report contained the PHI of multiple individuals); and the fact that the transfer formed part of an ongoing, province-wide and long-term program involving large volumes of PHI.

I am pleased to report that CCO immediately ceased transferring screening reports in paper format by courier and co-operated fully in the review. It is exploring alternative methods of securely transferring these reports to primary care physicians by electronic means. CCO has also reviewed and amended its privacy breach management policies and procedures and conducted additional privacy training to ensure that those having an employment, contractual or other relationship with the agency are fully aware of their responsibility to immediately report any privacy breaches, suspected privacy breaches and/or privacy risks to appropriate individuals.

Order HO-011 highlights the need for those in the health sector to carefully evaluate the options, including technology-based choices, available for maintaining security and confidentiality when transferring records of PHI.

Review and Approval of Prescribed Entities and Persons

My office completed its mandated three-year review of the information practices of four prescribed entities and of three prescribed persons that compile or maintain registries of PHI using the new streamlined process established by my office in 2010, in the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*. These prescribed entities are: Cancer Care Ontario; the Canadian Institute for Health Information; the Institute for Clinical Evaluative Sciences; and the Pediatric Oncology Group of Ontario. These prescribed persons are: the Cardiac Care Network of Ontario in respect of its registry of cardiac services; INSCYTE (Information System for Cytology) Corporation in respect of CytoBase; and Cancer Care Ontario in respect of the Ontario Cancer Screening Registry. The new process applies only to prescribed entities and prescribed persons that have previously had their information practices reviewed and approved by my office.

During 2011, my office also reviewed and approved the information practices of two newly prescribed persons: the Children's Hospital of Eastern Ontario in respect of the Better Outcomes Registry and Network; and the Ontario Cancer Research Institute in respect of the Ontario Tumour Bank. These newly prescribed persons were required to submit for review and approval all applicable practices and procedures implemented to protect the privacy of individuals whose PHI is received and to maintain the confidentiality of that information. My office also conducted site visits to ensure appropriate safeguards were implemented to protect the PHI collected, used and disclosed by the newly prescribed persons.

Although, in 2006, Hamilton Health Science Corporation was prescribed as a person that compiles or maintains the registry of the Critical Care Information System, it has not yet had its information practices reviewed or approved by my office. Consequently, health information custodians are not yet permitted to disclose PHI to the Hamilton Health Science Corporation for the purposes of section 39(1)(c) of *PHIPA*, without the consent of the individual.

eHealth Regulation

My office was consulted on potential amendments to Regulation 329/04 under *PHIPA* to permit eHealth Ontario to have access to PHI as a service provider that creates or maintains electronic health records (EHR). As a result, Regulation 329/04 was amended to permit health information custodians to provide PHI to eHealth Ontario for the purpose of creating or maintaining one or more EHRs — provided that eHealth Ontario satisfies certain requirements in section 6.2 of Regulation 329/04. These requirements include, for example, performing an assessment with respect to the threats, vulnerabilities and risks to the security and integrity of the PHI contained in the EHR and an assessment of how it may affect privacy.

Guidance for Health-Care Researchers

In 2011, my office published two papers providing guidance to the health research community on steps that can be taken to enhance privacy and to comply with *PHIPA*.

The first paper, released in June, *Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy,* was co-authored with Dr. Khaled El Emam, who serves as the Canada Research Chair in Electronic Health Information at the University of Ottawa, and the Children's Hospital of Eastern Ontario Research Institute. This paper dispels a number of myths about de-identification of health information and supports the practice of de-identification as one of the most important steps to protect privacy when using PHI for purposes that extend beyond the delivery of health care, such as research.

The second paper, released in September, *Safeguarding Personal Health Information When Using Mobile Devices for Research Purposes,* was issued to assist health information custodians, researchers and research ethics boards in understanding and fulfilling their obligations with respect to safeguarding PHI that is collected, used and disclosed for research purposes.

Requests by the Public

2011 FOI Requests, by Jurisdiction and Records Type

	Personal Information	General Records	Total
Municipal	13,535	14,466	28,001
Provincial	5,221	11,937	17,158
Total	18,756	26,403	45,159

A new record number of freedom of information (FOI) requests were filed in Ontario in 2011. A total of 45,159 requests were filed, a significant 16 per cent increase from the previous record of 38,903, set in 2010.

Provincial government organizations received 17,158 FOI requests in 2011, an increase of 13.1 per cent from the 15,161 in 2010. Of the requests filed, 5,221 (30.4 per cent) were for records containing the personal information of the requestor, while 11,937 (69.6 per cent) were for general records.

The Ministry of the Environment continued to receive the largest number of requests under the provincial *Act* — 6,111 in 2011, an increase of 580 requests from 2010. In a continuing trend, the other ministries at the top of the list in terms of requests received were Community Safety and Correctional Services with 4,873, Community and Social Services at 1,338 (a 58.6 per cent increase from the 785 requests received in 2010), and Labour with 925 requests. Combined, these four ministries continued to receive the vast majority of requests with 77 per cent of all provincial requests in 2011.

Municipal government organizations received 28,801 FOI requests in 2011, an increase of 21.3 per cent from the 23,742 requests received in 2010. Municipal requests have continued to increase, climbing from 19,887 in 2008 to 28,801 in 2011. Of the FOI requests made to municipal institutions in 2011, 13,535 (47.0 per cent) were for personal information and 14,446 (53.0 per cent) were for general records.

Of the top 10 municipal institutions to receive FOI requests, six were police services boards, which continued to receive, by far, the most requests under the municipal *Act* — 16,834 (58.4 per cent). Municipal corporations were next with 10,615 requests, followed by school boards with 240 requests and health boards with 58 requests.

The average fees charged in 2011 for general records by provincial institutions saw a modest increase to $41.39 which is still significantly lower than the record of more than $51 in 2006.

See full statistics related to 2011 FOI requests at www.ipc.on.ca.

Average Cost of Provincial Requests

	2007	2008	2009	2010	2011
Personal Information	$10.54	$11.26	$ 9.47	$12.88	$11.35
General Records	$50.54	$42.74	$39.66	$39.97	$41.39

Average Cost of Municipal Requests

	2007	2008	2009	2010	2011
Personal Information	$ 9.67	$ 8.82	$ 8.11	$8.01	$8.83
General Records	$23.49	$23.54	$26.55	$25.68	$24.22

Response Rate Compliance

Top 10 Provincial Institutions: Ranked by the number of requests completed in 2011

	Requests Received	Requests Completed	Within 30 Days	%	Extended Compliance *	Over 90 Days	%
Ministry of the Environment	6,111	5,935	4,876	82.2	85.5%	321	5.4
Ministry of Community Safety & Correctional Services	4,873	4,692	3,971	84.6	95.1%	138	2.9
Ministry of Community & Social Services	1,338	1,264	999	79.0	79.9%	26	2.1
Ministry of Labour	925	885	813	91.9	91.9%	14	1.6
Archives of Ontario	474	446	382	85.7	98.4%	3	0.7
Ministry of the Attorney General	442	411	384	93.4	95.6%	6	1.5
Liquor Control Board of Ontario	376	393	382	97.2	97.2%	0	0.0
Ministry of Transportation	377	353	328	92.9	94.6%	3	0.8
Landlord and Tenant Board	317	344	336	97.7	97.7%	0	0.0
Ontario Lottery and Gaming Corporation	229	222	210	94.6	100%	1	0.5

*Including Notice of Extension, section 27(1) and Notice to Affected Person, 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 persons outside the organization.

My office reports compliance rates to help focus attention on the importance for government organizations to comply with FOI response requirements set out in the *Acts* (although, timeliness alone does not provide a full indication of the quality of FOI responses). The provincial 30-day compliance rate has continued to climb from 42 per cent to more than 80 per cent since the IPC first reported individual response rates in 1999.

Institutions Governed Under the Provincial *Act*

Compliance for provincial ministries, agencies and other institutions slipped slightly in 2011 to a 30-day compliance rate of 83.6 per cent, below the high of 85 per cent achieved in 2008. The majority of requests completed by provincial organizations came from the business sector at 11,170 (65.1 per cent) followed by requests from individuals at 4,223 (24.6 per cent).

2011's provincial extended compliance rate remained stable at 90 per cent, down from a record 97.2 per cent in 2009. (Extended compliance rates — where institutions can respond later than 30 days because of qualified extenuating circumstances — have only been calculated since 2002).

Institutions Governed by the Municipal *Act*

Municipal government organizations came in below their provincial counterparts in responding to FOI requests within the statutory 30-day period at 80.1 per cent. Including extended compliance, the municipal response rate rises to 83.5 per cent, a drop of 4.9 per cent from 2010. Requests from individuals made up the majority of requests completed by municipal organizations at 18,398 (67.7 per cent) followed by the business sector at 7,304 or 26.8 per cent.

The Toronto Police Services Board has continued to maintain its position, since 2009, as the municipal institution that has completed the most FOI requests at 4,862 with a 30-day compliance rate of 76.3 per cent (79.4 per cent extended). The City of Toronto — which formerly held the title of municipal institution with the most FOI requests — completed 2,386 requests with a 30-day compliance rate of 82.5 per cent (88.2 per cent extended). Peel Regional Police Service Board remained in third place completing 1,501 requests. However, for the first time since 2008, Peel Regional Police Service Board did not score a perfect 100 per cent completion record for both 30-day compliance and extended compliance rate, coming at 83.5 per cent for both in 2011.

See complete 2011 response rates for ministries, municipalities, police services, school boards, etc. at www.ipc.on.ca

FOI Appeals

Summary of Appeals: 2011 vs. 2010

2011	General Records			Personal Information			Total		
	Provincial	Municipal	Total	Provincial	Municipal	Total	Provincial	Municipal	Total
Opened	468	333	801	154	259	413	623	591	1,214
Closed	337	296	633	145	245	390	483	540	1,023

2010	General Records			Personal Information			Total		
	Provincial	Municipal	Total	Provincial	Municipal	Total	Provincial	Municipal	Total
Opened	328	306	634	121	222	343	449	528	977
Closed	257	302	559	139	218	357	396	520	916

If you make a written freedom of information (FOI) request under Ontario's provincial or municipal freedom of information and protection of privacy *Acts,* and are not satisfied with the response, you have a right to appeal that decision to my office. Appeals may relate to a refusal to provide access, fees sought, the fact that the institution did not respond within the prescribed 30-day period, refusal to correct your personal information, or other procedural aspects relating to a request.

2011 Appeals

In 2011, 1,214 appeals were submitted — the highest number ever. Overall, 1,023 appeals were **closed** in 2011, an increase of 107 from 2010.

Records that do not contain the personal information of the requester are referred to as *general records.* Overall, 801 appeals regarding access to *general records* were made in 2011. Of these, 468 were filed under the provincial *Act* and 333 under the municipal *Act.*

There were a further 413 *personal information* appeals filed in 2011, including 154 under the provincial *Act* and 259 under the municipal *Act*.

In 2011, the number of appeals opened under the municipal *Act* — 591 — was up by 63, while the number filed under the provincial *Act* — 623 — was up 174 from the previous year.

Of the 623 appeals filed with my office under the provincial *Act,* 151 (33.6 per cent) involved the Ministry of Health and Long-Term Care, while another 123 (27.4 per cent) involved the Ministry of Community Safety and Correctional Services. A further 25 appeals related to decisions of the Ministry of Government Services, followed by the Ministry of the Attorney General (24) and the Ministries of Natural Resources (19) and Environment (12). The University of Ottawa had more appeals filed against its decisions than any other provincial agency with 17, followed by the Ontario Lottery and Gaming Corporation with 10.

Of the 591 appeals received under the municipal *Act*, 275 (46.5 per cent) involved police services, while 226 (38.2 per cent) involved municipalities. Toronto Police Services, which again received more requests under the municipal *Act* than any other organization, was also involved in the most appeals under that *Act* (82), followed by the City of Toronto (48), Halton Police Services (34), Hamilton Police Services (22), Ottawa Police Services (19), York Regional Police Services (19) and the City of Ottawa with 12.

The Toronto District School Board was involved in the most appeals against a school board (nine), followed by the Hamilton-Wentworth District School Board (eight).

For more detailed information about appeals filed and closed in 2011, see the statistical adjunct of this annual report, available at ***www.ipc.on.ca.***

Privacy Complaints

Summary of Privacy Complaints: 2011

	2010 Privacy Complaints				2011 Privacy Complaints			
	Provincial	Municipal	Non-jurisdictional	Total	Provincial	Municipal	Non-jurisdictional	Total
Opened	127	125	0	252	131	135	0	266
Closed	130	137	0	267	129	148	0	277

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 institutions.

If you believe that your privacy has been compromised by a provincial or local government organization, you can file a complaint under the *Acts* with my office. In the majority of cases, attempts are made to mediate a solution. We may also make formal recommendations to a government organization to amend its practices.

Privacy Complaints

A record 277 privacy complaints were **closed** in 2011, up 10 from the previous record of 267 in 2010.

The 277 privacy complaints we closed under the public sector *Acts* in 2011 included 148 under the municipal *Act* and 129 under the provincial *Act*. 214 *collection, use* or *disclosure complaints* under the *Personal Health Information Protection Act* (*PHIPA*) were also closed, taking the total number of privacy complaints closed in 2011 to 491.

There were 266 privacy complaints **opened** under the two public sector *Acts* in 2011 — the highest total since the first of these *Acts* — the *Freedom of Information and Protection of Privacy Act* — came into effect in 1988.

Of the 266 privacy complaints opened in 2011, 131 were filed under the provincial *Act* and 135 under the municipal *Act*. When the 223 *collection, use* or *disclosure privacy complaints* filed under Ontario's *PHIPA* are added, the total number of privacy complaints filed in 2011 climbs to 489 — an 11.1 per cent increase over the previous year.

As has been the case for years, the most cited reason for filing a privacy complaint under the two public sectors *Acts* was the disclosure of personal information. Disclosure was raised as an issue in 139 of the complaints closed (63.2 per cent). Another 27 (12.3 per cent) were related to security, while collection of personal information was an issue in 17 cases (7.7 per cent). The remaining complaints involved such issues as retention, use, notice of collection and disposal.

My office continues to emphasize informal complaint resolution. I am pleased to report that 97.1 per cent privacy complaints were closed in 2011 without the issuance of a formal privacy complaint report or order.

Of the complaints closed, 166 (almost 60 per cent) had been initiated by individual members of the public, while 11 (four per cent) were Commissioner-initiated. A further 100 (about 36.1 per cent) were self-reported breaches.

For more detailed information about privacy complaints in 2011, see the statistical adjunct of this annual report, available at ***www.ipc.on.ca.***

The *Personal Health Information Protection Act (PHIPA)*

Summary of *PHIPA* Complaints: 2010 vs. 2011

	2010 *PHIPA* Complaints					2011 *PHIPA* Complaints				
	Collection/Use/Disclosure					Collection/Use/Disclosure				
	Access / Correction	Individual	Self-Reported Breach	IPC - initiated	Total	Access / Correction	Individual	Self-Reported Breach	IPC - initiated	Total
Opened	100	62	95	31	288	123	64	135	24	346
Closed	112	59	98	22	291	109	64	123	27	323

The number of complaints filed with my office under the *Personal Health Information Protection Act (PHIPA)* rose to 346 in 2011, an increase of 20 per cent from the 288 filed in 2010 — and the highest ever total in the seven full years since *PHIPA* came into force.

Public hospitals were the subject of 160 of the 346 files opened, or about 46.2 per cent. Of these, 77 (57 per cent) were self-reported breaches related to the collection, use, or disclosure of personal health information. I actively encourage this kind of self-reporting by health information custodians and my office is committed to working with custodians to take quick steps to deal with breaches.

There were 38 complaints opened involving doctors — down from the 52 filed in 2010 — 17 of which related to access to and/or correction of personal health information. The number of complaints opened involving clinics climbed to 35 from 30 in 2010.

Complaints Closed

My office closed 323 complaints in 2011, an increase of 10 per cent from 2010 and 25 per cent from 2009. Notable in 2011 was the number of self-reported breaches closed rising to 123 from 98 in 2010, an increase of 20 per cent. The remaining 200 complaints closed in 2011 dealt with the collection, use, or disclosure of personal health information. Of these, 64 were filed by individuals; 123 were self-reported breaches; and 27 were initiated by my office.

As much as possible, I prefer to resolve complaints either informally or through mediation. Of the 109 complaints closed that were related to access to and/or correction of personal health information, 69 (63 per cent) were closed informally at the intake stage; 36 (about 33 per cent) were closed during the mediation stage; and four (just over three per cent) were closed during the adjudication stage.

Of the 123 complaints that involved self-reported privacy breaches by health information custodians, 114 (over 92 per cent) were closed at the intake stage, while eight were closed at mediation and one by adjudication.

Of the 64 complaints initiated by individuals related to the collection, use, or disclosure of personal health information, 57 (about 89 per cent) were closed during the intake stage and six were closed during the mediation stage. Finally, of the 27 complaints initiated by my office dealing with the collection, use, or disclosure of personal health information, 24 (over 88 per cent) were closed at the intake stage.

Personal Health Information Requests

Only health information custodians who also fall under *FIPPA* or *MFIPPA* are required to report to the IPC the number of written requests they receive from individuals seeking their own personal health information.

Custodians reported the completion of 7,822 such requests in 2011. The Ministry of Health and Long-Term Care completed 4,885 of these, over 62 per cent. The requests made to the ministry dropped by 159 from 2010's 5,044 requests, a decrease of slightly over three per cent. The ministry was able to complete 4,827 requests, or 98.9 per cent, within the statutory 30-day compliance period.

Type of *PHIPA* Complaint Files Opened in 2011

			Collection/Use/Disclosure							
	Access/ Correction	%	Individual	%	Self-reported Breach	%	IPC-initiated	%	Total	%
Public Hospital	52	42.3	26	40.6	77	57.0	5	20.8	160	46.2
Doctor	17	13.8	7	10.9	4	3.0	10	41.7	38	11.0
Clinic	12	9.8	6	9.4	14	10.4	3	12.5	35	10.1
Community or Mental Health Centre, Program or Service	6	4.9	5	7.8	19	14.1	3	12.5	33	9.5
Other Health Care Professional	7	5.7	2	3.1	6	4.4	0	0.0	15	4.3
Community Care Access Centre	3	2.4	2	3.1	2	1.5	0	0.0	7	2.0
Ministry of Health and Long-Term Care	5	4.1	2	3.1	0	0.0	0	0.0	7	2.0
Long-Term Care Facility	4	3.3	0	0.0	1	0.7	1	4.2	6	1.7
Nursing Home	4	3.3	2	3.1	0	0.0	0	0.0	6	1.7
Agent	4	3.3	0	0.0	0	0.0	0	0.0	4	1.2
Ambulance Services	0	0.0	1	1.6	3	2.2	0	0.0	4	1.2
Board of Health	0	0.0	1	1.6	2	1.5	0	0.0	3	0.9
Laboratory	0	0.0	0	0.0	2	1.5	1	4.2	3	0.9
Other	0	0.0	2	3.1	1	0.7	0	0.0	3	0.9
Other Prescribed Person	2	1.6	1	1.6	0	0.0	0	0.0	3	0.9
Pharmacy	1	0.8	2	3.1	0	0.0	0	0.0	3	0.9
Dentist	0	0.0	2	3.1	0	0.0	0	0.0	2	0.6
Minister of Health	1	0.8	0	0.0	0	0.0	1	4.2	2	0.6
Psychologist	1	0.8	0	0.0	1	0.7	0	0.0	2	0.6
Care Home - Tenant Protection	1	0.8	0	0.0	0	0.0	0	0.0	1	0.3
Charitable Home for the Aged	0	0.0	0	0.0	1	0.7	0	0.0	1	0.3
Home or Joint Home (Aged or Rest)	1	0.8	0	0.0	0	0.0	0	0.0	1	0.3
Independent Health Facility	0	0.0	1	1.6	0	0.0	0	0.0	1	0.3
Institution - Mental Hospitals Act	0	0.0	1	1.6	0	0.0	0	0.0	1	0.3
Nurse	0	0.0	1	1.6	0	0.0	0	0.0	1	0.3
Physiotherapist	0	0.0	0	0.0	1	0.7	0	0.0	1	0.3
Prescribed Entities	0	0.0	0	0.0	1	0.7	0	0.0	1	0.3
Radiological Technician	1	0.8	0	0.0	0	0.0	0	0.0	1	0.3
Social Worker	1	0.8	0	0.0	0	0.0	0	0.0	1	0.3
Total	**123**	**100.0**	**64**	**100.0**	**135**	**100.0**	**24**	**100.0**	**346**	**100.0**

Judicial Reviews

Several Court decisions released in 2011 underscore the importance of the legislation in ensuring governmental transparency and accountability in a variety of contexts, including municipal expenditures and decision-making, provincial government efficiency and activity, and access to non-personal third party information. One decision also reaffirmed the importance of providing notice and fairness to potentially affected parties in administering the processes under the statutes.

Order MO-2521 – Vaughan (City) v. Ontario (Information and Privacy Commissioner)[1]

The Ontario Divisional Court upheld my office's decision ordering the City of Vaughan to disclose copies of the complete 407 ETR invoices it paid over a four-year period for the business and personal travel of an employee. The city had previously disclosed severed versions showing the amounts paid, dates of use and distances traveled, but withheld the entry and exit points and times of day, claiming that this was the personal information of the employee.

My office found that the complete invoices would disclose "the benefits … of an … employee" of an institution under section 14(4)(a) of *MFIPPA* and, accordingly, their disclosure is presumed not to constitute an unjustified invasion of personal privacy. We explained that the exit and entry points determined the amount of the toll charges attributable to personal and business travel and, therefore, the amount of the "benefit." We also rejected the city's argument that disclosure of the employee's whereabouts could reasonably be expected to threaten his health or safety under section 13 of *MFIPPA*.

On judicial review, the Court strongly endorsed the reasonableness standard of review applicable to my office's decisions dealing with personal privacy. It rejected the city's argument that section 14(4)(a) is intended to capture only general descriptions of benefits in an employment agreement. The Court looked at the accountability purposes of the legislation and a previous Court of Appeal decision recognizing that *MFIPPA* is not intended to provide "airtight" privacy protection. The Court also cited prior decisions emphasizing the responsibility and accountability of municipal employees to taxpayers in the use of public funds for personal purposes. While the Court upheld the decision as "reasonable," it also agreed that the decision struck the correct balance in this particular case.

2011 Judicial Review Statistics

New Judicial Review applications received in 2011:	**2**
Launched by:	
Institutions[2]	1
Requesters	0
Affected Parties	0
IPC Intervened in application[3]	1
Outstanding Judicial Reviews as of December 31, 2011:	**25**
Launched by:	
Institutions	11
Requesters	3
Institution and other party	4
Affected Parties	7
Judicial Reviews Closed/Heard in 2011	**14**
Abandoned (IPC Order/decision stands)[4]	3
IPC Order Upheld[5]	4
IPC Order Upheld with appeal pending[6]	1
IPC Order Partially Upheld with appeal pending[7]	2
IPC Order Not Upheld and remitted back to IPC[8]	2
IPC Intervened in application[9]	2

1 2011 ONSC 7082
2 MO-2659
3 London by-law
4 MO-2416 / MO-2449, MO-2489
5 MO-2425-I, MO-2521, PO-2739, PO-2807
6 PO-2811
7 PO-2872 / PO-2899-R
8 PO-2456, PO-2763
9 City of Toronto, London by-law

Looking Forward

As 2011 came to a close and 2012 was about to begin, the Office of the Information and Privacy Commissioner (IPC) entered into its 25th year of existence. Personally, it has been quite a journey for me since the autumn of 1987, when I first joined the IPC as the first Director of Compliance. For the last two-and-a-half decades, I have had the pleasure of working at the IPC, the last 14 years of which I have had the honour of serving as Commissioner. During that time I have seen many significant changes in both the access and privacy spheres — primarily arising from unprecedented advances in information and communications technology.

So much has happened over the years I have spent here, from the time the *Municipal Freedom of Information and Protection of Privacy Act* was enacted in 1990, to the passing of the *Personal Health Information Protection Act* in 2004, and the adoption of *Privacy by Design* as an International Standard. There is so much I could say about our accomplishments. The thousands of phone calls my office deals with each year — the long lists of media interviews, research and policy development, privacy investigations and appeals, speeches and white papers — all the work that goes into our website, cannot be given the proper accolades in this short space. I encourage you to visit our website at www.ipc.on.ca as I think the results will speak for themselves.

As the IPC begins its 25th year of service to the people of Ontario, I find myself concerned for the future of access and privacy. However, I remain confident that our right to access government-held information and the protection of our privacy will continue to be safeguarded by those who understand and appreciate the role access and privacy plays in our free and democratic society. In a perfect world, there would be no need for my office, but we do not live in a perfect world, and we have people such as my staff and the thousands of other access and privacy professionals around the world to thank, for their unceasing work in protecting our cherished rights.

Looking forward, I can say with certainty that one of the biggest challenges to access and privacy will come from the increasingly complex evolution of information and communications technology. However, I believe the greatest challenge will come not from technological advances, but from apathy. We have the resources and tools to transform the same technological advances that threaten access and privacy into ones that promote access and protect privacy, such as *Privacy by Design* and *Access by Design*. Yet, these will mean nothing if we do not remain committed to the protection of those rights.

Therefore, we must remain ***Ever Vigilant***. We must capitalize on our advances and continue to press for change within each of our countries, jurisdictions and organizations. We must remain committed to the ideals of access and privacy. We can never rest on our laurels and allow our hard-fought rights to disappear through complacency. That would be a fundamental error, setting a precedent capable of unwinding centuries of progress in the evolution of freedom. Access and privacy rights are fundamental to our freedom and liberty. To quote the ancient philosopher Plato, "The penalty good men [and women] pay for indifference to public affairs, is to be ruled by tyrants." Let that not be our legacy.

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner
Ontario, Canada

Financial Statement

	2011-2012 Estimates $	2010-2011 Estimates $	2010-2011 Actual $
Salaries and Wages	9,852,800	9,461,000	9,532,734
Employee Benefits	2,266,600	2,176,200	1,768,832
Transportation and Communications	337,500	313,500	323,661
Services	2,052,300	1,890,800	1,827,516
Supplies and Equipment	239,000	194,000	316,223
Total	**14,948,200**	**14,035,500**	**13,768,966**

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.

2011 Appeals Fees Deposit

(Calendar year)

General Info.	Personal Info.	**Total**
$12,590	$2,830	**$15,420**

See further financial information, including IPC Public Sector Salary Disclosure, at www.ipc.on.ca.

INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO
2011 ANNUAL REPORT

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

Tel: (416) 326-3333
Fax: (416) 325-9195
1-800-387-0073
TTY: (416) 325-9539

E-mail: info@ipc.on.ca
Web: www.ipc.on.ca