Transparency, Privacy and the Internet: Municipal Balancing Acts

Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

CONTENTS

Acknowledgments

The IPC gratefully acknowledges the contributions of staff at the City of Vaughan and the City of Toronto, whose suggestions and insights have significantly informed this paper.

INTRODUCTION

In providing services to the public and meeting their mandated obligations, municipalities are required to collect, use and disclose personal information from and about their community members. This information is necessary for the provision of services, for informing the public of a municipality's actions and decisions, and for ensuring that its decision making processes operate in a fair and open manner.

Some information received and processed by municipalities is legally required to be made publicly available for the purposes of allowing public participation in decision making and for maintaining transparency and accountability with respect to the activities of these institutions.

Government transparency and access to information are vital to a free and functioning democratic society. Without them, the public cannot participate meaningfully in the democratic process or hold elected officials accountable. The IPC supports public institutions in their efforts to ensure that their work is conducted in open, transparent and accountable ways.

Government transparency and access to information are vital to a democratic society.

However, making personal information publicly available via the Internet can be challenging when the records involved contain personal information that may be sensitive or relate to vulnerable individuals. Personal information published on the Internet may be inappropriately used or may be used for purposes other than the public policy reason for making it public. Municipalities should balance the need to protect the privacy of their community members, in compliance with the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*), with the need to meet their other legislated obligations.

The Internet has transformed the mode of delivery and accessibility of information. It is seen as a key support of the Open Government movement which has been adopted by many municipalities in Ontario to assist them in meeting their democratic obligations of openness and transparency. Not surprisingly, municipalities are turning to the Internet as a means of making information public in an effort to improve accessibility, transparency and accountability. This can include publishing records directly to a municipality's website or including records in searchable databases that can be accessed

online. Publishing materials online is certainly an effective means of ensuring that the public has access to a municipality's information. However, when publicly available records include personal information, there are privacy implications that should be considered before that information is made available on the Internet.

The premise of this guide is that in many cases municipalities are required by law to make some personal information publicly available. Municipalities are increasingly recognizing the benefits of providing the public greater access to their information holdings to promote transparency and accountability. While many municipalities meet those obligations by making personal information available to those who request it over the counter, this method of access may no longer meet the general expectations of their constituents.

This paper will provide municipalities with options on how to implement privacy-protective measures when publishing publicly available documentation that contains personal information on the Internet. These options have been developed to help municipalities balance the interests of transparency and privacy while complying with their legislated obligation to make information publicly available. The options presented in this guide need to be adapted to the unique goals and needs of each municipality and the unique aspects of each information holding.

WHAT IS PERSONAL INFORMATION?

Section 2(1) of *MFIPPA* defines personal information as recorded information about an identifiable individual (that is, a natural person). This can include, but is not limited to:

- biographical details (name, sex, age, race),
- biological details (face, fingerprints, blood type, etc.),
- nationality,
- religion,
- marital status,
- education,
- medical or criminal history,
- financial information,
- identifying numbers (for example, social insurance number),

- an individual's contact details (address, phone number, etc.) and
- personal opinions and views.

This list of what defines personal information is not exhaustive, and additional information about an individual may be considered to be personal information either alone or by reason of the context in which it appears. There must be a reasonable expectation that an individual can be identified from the information itself or in combination with other information, whether or not it is publicly available, in order for it to qualify as personal information.

As a general rule, information associated with an individual in a professional, official or business capacity is not considered to be about the individual, and therefore, is not usually considered personal information. This may include information about an individual's business or professional contact details, a business or professional designation or title, or information relating to work product. In some limited circumstances, information that appears to be about a business may qualify as personal information if that information reveals something of a personal nature about the individual.

YOUR OBLIGATIONS

Under a number of statutes, municipalities are required to make certain information available to the public. Consider the following examples:

- Section 1.0.1 of the *Planning Act* requires that "Information and material that is required to be provided to a municipality or approval authority under this Act shall be made available to the public." This includes any information received in applications or proposals pertaining to

Personal versus business information: Information that may seem personal, such as name and contact information, may not be personal information if it relates to an individual's business activities. In other words, where the individual is acting in a professional capacity in the context of the information it may not qualify as that person's personal information. Consider the context in which the information arises in order to determine if it qualifies as personal information.

land use planning. While much of this information may be business related, some records will contain personal information. Consider, for example, applications for minor variances for an individual's residential property. These records may include personal information such as name, home address, personal telephone number, email address and signature.

- Section 374(4) of the *Municipal Act* requires that statutory declarations regarding the registration of property must be made available to the public upon request. These declarations contain the names and addresses of property owners.

- Sections 39(2) and 39(3) of the *Assessment Act* require that municipalities make the assessment roll available to the public. The assessment roll contains personal information such as a property owner's name and mailing address, the current value of a property and names of tenants who support school boards.

MFIPPA seeks to protect privacy by prohibiting the disclosure of personal information, except in limited and defined circumstances. In furtherance of the requirements of municipalities to make information publicly available, section 32 of *MFIPPA* includes the following exceptions:

> An institution shall not disclose personal information in its custody or under its control except,
>
> (c) for the purpose for which it was obtained or compiled or for a consistent purpose;
>
> (e) for the purpose of complying with an Act of the Legislature or an Act of Parliament, an agreement or arrangement under such an Act or a treaty;

In Privacy Complaint Report MC13-67,[1] this office determined that the disclosure of personal information in a minor variance application on a municipality's website was not in contravention of *MFIPPA*. The investigation concluded that the above-noted sections applied to the online publication of the application and that the disclosure via the Internet was permissible. It found that the notice of collection provided on the application clearly indicated that the purpose of the collection was to create a public record. Furthermore, the creation and public availability of that record is mandated by the *Planning Act*.

Where personal information is maintained for the purpose of creating a record that is available to the general public, section 27 of *MFIPPA* applies and the privacy provisions in Part II do not. Privacy Complaint Report MC13-67 refers to the findings of the Ontario Divisional Court in *Gombu v. Ontario.*[2] In that case,

1 *City of Vaughan* (20 March 2015), MC13-67, online: IPC, https://www.ipc.on.ca/images/Findings/MC13-67.pdf

2 *Gombu v. Ontario (Information and Privacy Commissioner)*, 59 OR (3d) 773 (available on CanLII), [*Gombu v. Ontario*], http://canlii.ca/t/2349t

the court noted that the public expects access to information online. It found that disclosing public records in electronic format makes them more easily accessible and does not impact privacy significantly, as the personal information contained in these records is already subject to disclosure.

The public expects to be able to access publicly available information online. Information can be made publicly available in this manner while protecting privacy.

Therefore, where either section 27 or sections 32(c) and (e) apply to the personal information in the custody or control of a municipality, the municipality's decision to make that personal information publicly available is not a contravention of *MFIPPA*.

MAKING PERSONAL INFORMATION PUBLICLY AVAILABLE

Generally, legislation requiring that information be made publicly available does not specifically limit or restrict the manner in which that information is to be made available. Some municipalities maintain records containing personal information on paper and make them available to interested members of the public only upon request, and only when the requester physically accesses the records during business hours. This type of disclosure practice results in a measure of privacy due to the "practical obscurity" of the personal information. Since access to this information, and in some cases even knowledge of its existence, requires substantial effort on the part of the individual seeking access, it is generally considered that this information has some degree of privacy protection. However, as indicated above, as government services move online, this method of access has become less acceptable to the public.

***MFIPPA* does not dictate the manner in which publicly available records containing personal information should be disclosed.**

There are many benefits to publishing publicly available information online, but when personal information is involved, there may be privacy risks.

WHAT ARE THE BENEFITS OF INTERNET PUBLICATION?

As mentioned above, the Open Government movement actively promotes the use of the Internet as a means of communicating with the public, and for good reason. Information is shared quickly and easily via the Internet and it can be made available in a myriad of previously unforeseen ways. The Internet has set new expectations on the part of the public in relation to publicly available information because it has changed the way that individuals engage with government. Individuals expect that information and services will be available to them online;[3] the days of attending at the municipal clerk's office to obtain a copy of a record are largely gone.

There are many benefits to publishing online. It can be a cost-effective way to meet statutory requirements to make information publicly available, while also improving transparency, accessibility and accountability. It can reduce administrative burdens associated with maintaining records on site for public access and even reduce the number of access to information requests that the municipality will need to respond to. In most cases, publishing publicly available information, including personal information, online is a viable solution.

WHAT ARE THE PRIVACY RISKS?

The potential risks associated with the Internet publication of personal information as opposed to making a paper record available for examination are very different. The degree of accessibility of records published online can go much further than simple access via the municipality's website. Search engines, such as Google, automatically trawl websites and catalogue materials that are found. This makes the contents of individual records that are posted on websites individually searchable. For example, a record containing an individual's name can normally be searched for and discovered via Google simply by entering that person's name.

In addition to this increased accessibility, the use of information obtained via the Internet is difficult to govern. Consider, for example, a marketing company looking to advertise building materials or services. Online records pertaining to

3 Information and Privacy Commissioner of Ontario, "Promoting Transparency through the Electronic Dissemination of Information" (Discussion paper, Information and Privacy Commissioner of Ontario, April 2004), https://www.ipc.on.ca/images/resources/up-protrans.pdf

building permits may provide the marketing company with a list of individuals and their contact information that may be used to directly market its products or services. While this type of secondary use of personal information, if by the municipality, would likely be in violation of *MFIPPA*, it is virtually impossible to prevent third parties from using the information in this manner once it is published online.

There are a number of other risks associated with making personal information available via the Internet. Identity theft and other forms of fraud are major concerns. Identity thieves collect information about individuals in order to make purchases and obtain credit in their victims' names. There is also a significant personal safety risk for some individuals. Consider, for example, an individual who has been the victim of a stalker, or has an abusive ex-spouse who may be looking for him or her. Broad access to that individual's name and contact information could put that individual at serious risk.

Many of the records that are subject to statutory requirements to be made publicly available are created for a transitory purpose. For example, in the case of a minor variance application, the application and supporting materials are created for purposes related to the application process. Once the application process is complete and the records have reached the end of the applicable retention period, there may be no ongoing need for those records to be made publicly available. However, due to the nature of Internet indexing and archiving, records that are published on the Internet remain there indefinitely.

It is possible to use the Internet to make records publicly available while still providing some privacy protection to individuals whose personal information appears in those records.

Finally, fear associated with the publication of one's personal information may result in people feeling unwilling to participate in municipal affairs. As more information is made available, and as the public becomes more aware of the consequences of this, it is not unreasonable to expect a drop in participation in activities involving municipal governments that require one to submit personal information.

HOW TO MITIGATE THE RISKS

It is possible to use the Internet as a means of making records publicly available while still providing some privacy protection to individuals whose information may appear in those records.

To mitigate the privacy risks of making personal information available on the Internet, consider all policy, procedural and technical options and determine the best solutions for your municipality.

The following measures should be considered as potential options for privacy protection, but they should not be seen as prescriptive or exhaustive.

REDACTION PROCESS

Develop a process for individuals who may wish to seek to have their personal information redacted from the records your institution publishes on the Internet if they can reasonably demonstrate that disclosure of their personal information would jeopardize their safety, or that of their family. Ensure that individuals are aware of their right to seek a redaction at the time of the collection of personal information, and identify the categories of information that are eligible for a redaction, the process for seeking a redaction and the factors that will be applied in reviewing their application for a redaction. At the conclusion of the process, individuals should be informed of the decision and the rationale behind it. [4]

DATA MINIMIZATION

Data Minimization refers to the practice of reducing the amount of personal information that is collected, used and disclosed to that which is necessary to achieve the legitimate governmental purpose. This practice protects both the collector of information and the person providing the personal information by preventing the potential release of personal information that was not needed in the first place. In fact, this principle is an explicit requirement of section 28(2) of *MFIPPA,* which prohibits the collection of personal information unless "expressly authorized by statute, used for

Reducing the amount of personal information that is collected, used and disclosed at every stage to only that which is necessary will greatly reduce the risks associated with making information available online.

4 The Municipality of Vaughan, to address privacy and confidentiality concerns, has implemented a procedure for redacting personal information from publicly available records before the records are published on the Internet.

the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity."

Where the collection is not expressly authorized by statute or not for law enforcement purposes, consider the applications or records that your municipality requires individuals to submit. Is any of the requested information useful but not necessary? If the information is useful but not necessary, then the municipality does not have the authority to collect it.

Consider whether or not it is necessary to publish the personal information in order to meet the obligations of the applicable legislation and ensure that you do not publish more than what is required to meet your legislative requirements.

Limiting the information that your municipality collects will not only prevent harm caused by the release of excessive personal information, it will also reduce the administrative work associated with the amount of information that needs to be processed, stored and protected.

You should also consider data minimization when determining what information will be published on the Internet. Consider whether or not it is necessary to publish the personal information in order to meet the obligations of the applicable legislation and ensure that you do not publish more than what is required to meet your legislative requirements. For example, in appropriate cases, consider using initials instead of names and whether other personal identifiers such as birthdates, account or other identifying numbers need to be made publicly available online. Is there a requirement to publish this information? Will the information be needed by a member of the public to use the record for its intended purpose?

Finally, you may wish to consider separating records into two versions, where acceptable by law. For example, a document with personal information redacted may be published online, while the unredacted version is made available only to those who register with the website or who visit the municipal office. In doing this, an additional layer of obscurity is added to the personal information, without making the document wholly unavailable and therefore ensures you meet your legislative requirements. In considering this approach, review the specific legal requirements pertaining to the information that must be made publicly available. [5]

5 For example, the Canadian Human Rights Tribunal, the Social Security Tribunal and the Manitoba Labour Board actively replace names with initials in decisions posted online.

Technology can help balance transparency and privacy, but cannot be relied upon as the sole solution. The rapid evolution of technology and issues such as cost and availability must be taken into account.

TECHNOLOGICAL MEASURES

Technology can help address the balance between posting information to the Internet and the privacy of individuals. The following standards and practices can help limit the automated collection of website information and minimize secondary and unrelated uses, especially when applied together with administrative measures. These approaches can help ensure that information is still available to individuals who need it (such as by searching the municipal website) but limits discovery of this information under a general search (such as by searching for a particular name in a search engine). However, it is important to keep in mind that no technological tool is 100 per cent effective or foolproof. Technology evolves quickly, and it can be difficult to implement solutions to technological problems as quickly as they arise.

There are three main approaches:

1. Designating Site Content "Off Limits" to Search Engines
2. Preventing Robots from Accessing Site Contents
3. Enabling Enhanced Website Use by Humans

1. DESIGNATING SITE CONTENT "OFF LIMITS" TO SEARCH ENGINES

Using the Robots Exclusion Protocol

The robots exclusion protocol is a simple and widely-recognized Internet standard used by websites to identify directories and pages containing content that should not be indexed by automated agents or robots. Robots are commonly used by search engines (and other parties) to discover, capture and index web content, usually to improve searchability.

The robots exclusion protocol begins with one or more simple text files ("robots.txt") located in the site's root directory that identify areas of the site that should be avoided by robots. The protocol specifies that robots must always first check for this file before proceeding to scan the site and harvest content. This can prevent search engines from collecting and indexing information posted on the identified areas of the site, ensuring that this information will not appear in search results.

The main weakness of the robots exclusion protocol is that it is a voluntary standard. Search engines are legally able to ignore website requests to be excluded from harvesting by automated agents. In addition, as the standard is not legally required, there is no way to monitor compliance or enforce it. As such, the effectiveness of the robots exclusion protocol may be limited by bad actors that choose to ignore the instructions. That said, most major search engines (such as Google, Bing and Yahoo) adhere to this standard, and non-compliance will be detected quickly if the site's content turns up in search results.

Using Page-Specific Meta Tags

Meta tags are information embedded in a web page's HTML code that can provide additional instructions to robots, such as not to index page contents or to follow embedded links. Meta tags can be easily placed into a web page by the page's author and do not require intervention by the server administrator. Like the robots exclusion protocol, obeying meta tags is voluntary and cannot be enforced.

Excluding Site Content from the Website's Sitemap

Many web servers offer a sitemap that describes the site's directory structure and content for visitors and automated agents to use for better navigation and interaction. A sitemap that excludes the web pages and directories containing personal (or sensitive) information helps to obscure that content from being discovered and indexed by automated agents.

As with the robots exclusion protocol and meta tags, sitemap uses by automated agents are voluntary in nature and are not subject to reliable monitoring and enforcement.[6]

Search engines are able to discover, capture and index web context through the use of automated agents or robots. These robots trawl websites by following links around the web and collecting information from the sites they visit for inclusion in its index. When a user searches for a specific term, the search results show entries from the index where that specific term had been found.

2. PREVENTING ROBOTS FROM ACCESSING SITE CONTENTS

Blocking Robots

If it has been determined that some robots behave badly (that is, they disobey "robots.txt"), or have been reported as such by other websites, the robots' names or IP addresses can be blacklisted and blocked. This

6 The Canadian Judicial Council recommends this approach. The Canada Agricultural Review Tribunal and the Public Service Labour Relations and Employment Board currently employ these methods to protect information contained in the decisions posted on their website.

can be done through server-level or directory-level configurations. There are many "user agent" blacklists that are widely used, maintained regularly, and freely available.

Diverting Robots

It is possible to put in place technological measures to detect and deflect robots' activities away from the site, for example, by measuring and diverting excess traffic, creating robot honeypots (decoys), or putting hidden links on pages which only robots (but not humans) will follow. There are commercial products that can do this. In addition, several companies offer commercial anti-bot services for websites.

Using JavaScript

Few robots are able to execute JavaScript, a high-level, interpreted programming language that runs in the browser in response to some user input. Therefore, building the website's navigation scheme with JavaScript could disguise the website's navigation structure from robots. However, there are some security risks associated with JavaScript. When deployed incorrectly, JavaScript can carry out unwanted tasks on users' computers and introduce cross-site scripting vulnerabilities on the host web server.[7]

3. ENABLING ENHANCED WEBSITE USE BY HUMANS

Applying Access Controls

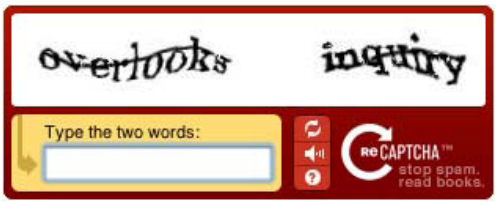
In some cases, you may wish to increase control over access to particular content through user registration. Depending on the sensitivity of the information being accessed, you may need only a simple registration (for example, by having a user provide a name or email address) or, in case of more sensitive data, appropriate authentication with a password. Modern content management systems can provide access controls on individual pages and collections of resources. This approach can be helpful if you have chosen to publish a redacted version of a document. Using access controls, you can make the unredacted version available to interested individuals who register for the website, but obscure the personal information from search engines.

Verifying Live Users

Tools are available to verify that it is a real person accessing the site, not a robot. One of the most popular tools is CAPTCHA. This tool requires users to

7 The Canadian Judicial Council recommends this approach. The Canada Agricultural Review Tribunal and the Ontario Government Open Data Portal currently employ these tools on their websites.

type characters from a distorted image that appears on the screen, or from a recorded sound. It is assumed that humans are superior to computers in pattern recognition. However, these days, there are automatic character recognition programs that might be successful in breaking the CAPTCHA patterns in about 30 per cent of cases. Progress in detecting "liveness" continues to evolve.



Generating Dynamic Web Pages

A dynamically-generated web page or site is one in which content is returned in response to information provided by the user. Dynamic web pages are typically controlled by a website application server that processes user inputs and delivers customized content. Page results are not static but are generated on the fly in response to a visitor's capabilities, preferences, or actions. For example, dynamic web pages are able to serve pages tailored for mobile browsers, or location-aware content based on the visitor's IP address or cookie information.

By developing a dynamic web page, a municipality can have more control over how information is displayed and made available to site visitors. For example, website administrators of dynamic web pages can restrict a user's ability to search for individual names and limit robots' ability to access content. This can include preventing URLs from being bookmarked or linked. In addition, dynamic web pages can administer page loading restrictions, such as limiting the display of page content and serving customized page content in response to user actions and capabilities. This can effectively slow-down information discovery and retrieval processes and prevent unauthorized or large-scale harvesting of information on your website by both humans and automated agents.

While dynamic web pages have numerous benefits, it is important to note that they are more complex to implement and maintain, requiring specialized knowledge of programming languages on specialized application servers that handle client-user interactions. This can be costly and time consuming, and you will need to consider if this approach is right for your municipality.

Using Static Images Instead of Searchable Text

As we have discussed above, robots are able to collect and index information from websites easily and quickly. However, these agents are not nearly as effective when working with images. A picture of text makes little sense to an automated agent. Using images instead of text is an easily implementable option. Scanned images of records (for example, JPG or BMP) are far less likely to be understood by automated agents such as robots, and therefore, are less likely to be indexed and made searchable.

When posting images, care must be taken not to embed identifiable information in the image filename or its metadata, as this information can be read by automated agents. For example, tagging a record with a meta tag that states, "This is an application filed by John Doe, of 123 Fake Street" will defeat the purpose of using an image.

It is important to remember that the use of images instead of text can create challenges for individuals with visual impairments who may be using a screen reader or other assistive technology. Where applicable, ensure that your use of images is in compliance with accessibility requirements and standards. [8]

TRANSPARENT ADMINISTRATION

Complaints regarding the publication of information may be prevented by transparency around your municipality's information collection, use and disclosure practices. The public has a right to understand the purpose and authority for the collection of personal information, as set out in section 29(2) of *MFIPPA*, and how its personal information will be used and disclosed, prior to its submission to the municipality.

Being transparent from the beginning about how personal information will be used and disclosed is essential.

If you intend to make the personal information publicly available, you should provide the following to individuals at the time that the personal information is collected:

- information about why the personal information is being made publicly available and the relevant legislative requirement,
- specific details on what personal information will be made available and how, including whether information will be posted on a municipal website,
- the laws and policies governing the collection, use, retention and disclosure of the personal information,
- any processes that have been established to redact personal information from records (include in these processes specific instructions on how to request a redaction, what criteria an applicant will need to meet and how the process works) and

8 The City of Toronto uses static PDF documents to help obscure personal information from searches on its website.

- any tools that have been employed to limit the automated collection of information and minimize the secondary and unrelated uses of the information.

By taking these steps, you will manage public expectations about the processing of personal information and you will enhance the transparency of your organization.

FOR MORE INFORMATION AND FURTHER RESOURCES

If you have questions on how to implement any of the recommendations in this guide, or require any additional information on how to protect personal information, please contact the Information and Privacy Commissioner of Ontario at info@ipc.on.ca.

For further information, please see:

Robots Exclusion Protocol: Complete information and guidance is available at www.robotstxt.org and Web Server Administrator's Guide to the Robots Exclusion Protocol available online at http://grox.net/doc/web/robots-exclusion-admin.html

SITEMAP Protocol: at http://www.sitemaps.org/protocol.html

For Blocking and Redirecting Robots, see Perishable Press, Ultimate htaccess Blacklist at http://perishablepress.com/ultimate-htaccess-blacklist/ or 2013 User Agent Blacklist http://perishablepress.com/2013-user-agent-blacklist/ and for redirecting see Stupid htaccess Tricks at http://perishablepress.com/stupid-htaccess-tricks/

JavaScript (JS) see JS libraries e.g. at http://www.w3schools.com/js/js_libraries.asp

CAPTCHA: The term CAPTCHA (for Completely Automated Public Turing Test To Tell Computers and Humans Apart) was coined in 2000 by Luis von Ahn, Manuel Blum, Nicholas Hopper and John Langford of Carnegie Mellon University. For more information and examples, visit www.captcha.net

Server-Side Scripting: For more information on application servers and server-side scripting languages, see https://www.dmoz.org/Computers/Programming/Internet/Server_Side_Scripting

Guidance from Other Canadian Jurisdictions

- Office of the Privacy Commissioner of Canada, Electronic Disclosure of Personal Information in the Decisions of Administrative Tribunals. (Feb 2010);
- British Columbia Office of the Information and Privacy Commissioner, Balancing Privacy and Openness: Guidelines on the Electronic Publication of Decisions of Administrative Tribunals, (July 2011);
- Alberta Office of the Information and Privacy Commissioner, Report on a tribunal's decision to disclose a Decision on the internet. (July 2013);

- Saskatchewan Information and Privacy Commissioner: Electronic Disclosure of Personal Information in the Decisions of Administrative Tribunals (2011);
- Government of PEI, Electronic Disclosure of Personal Information in the Decisions of Administrative Tribunals, (2010).

ABOUT THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

The role of the Information and Privacy Commissioner of Ontario is set out in three statutes: the *Freedom of Information and Protection of Privacy Act*, the *Municipal Freedom of Information and Protection of Privacy Act* and the *Personal Health Information Protection Act*. The Commissioner acts independently of government to uphold and promote open government and the protection of personal privacy.

Under the three *Acts*, the Commissioner:

- **Resolves access to information appeals and complaints when government or health care practitioners and organizations refuse to grant requests for access or correction;**
- **Investigates complaints with respect to personal information held by government or health care practitioners and organizations;**
- **Conducts research into access and privacy issues;**
- **Comments on proposed government legislation and programs; and**
- **Educates the public about Ontario's access and privacy laws.**

Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

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

Web site: www.ipc.on.ca
Telephone: 416-326-3333
Email: info@ipc.on.ca

August 2015