ACCESS

MARCH 2017

Open Government and Protecting Privacy

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

CONTENTS

1. INTRODUCTION

The Office of the Information and Privacy Commissioner of Ontario (IPC) is a strong supporter of Open Government and encourages institutions covered by the ***Freedom of Information and Protection of Privacy Act*** (*FIPPA*) and the ***Municipal Freedom of Information and Protection of Privacy Act*** (*MFIPPA*) to be more open and transparent, and to enhance their engagement with the public.

To assist institutions in adopting Open Government, the IPC has published three papers:

- ***Open Government: Key Concepts and Benefits*** is an introduction to Open Government. It highlights two critical goals: enhancing access to government-held information and public participation.
- ***Open Government: Key Implementation Considerations*** provides institutions with an overview of important factors to consider when implementing Open Government.
- ***Open Contracting: Proactive Disclosure of Procurement Records*** details the benefits of proactive disclosure of procurement records and offers tips on designing and implementing a transparent procurement process.

The protection of privacy is essential to the viability and sustainability of Open Government. It is also necessary to creating and maintaining public trust and confidence.

While Open Government offers many benefits to government, businesses, and the public, the pursuit of increased government transparency and public engagement could negatively affect individuals' privacy if initiatives are not properly designed, implemented, and monitored. Privacy risks include:

- more **personal information** may be collected, used or disclosed than is necessary
- personal information may be used for unrelated purposes (for example, data profiling and mining)
- personal information may be published without authority
- individuals may be re-identified by combining published de-identified **data** or **information** with other publicly available records

The protection of privacy is essential to the viability and sustainability of Open Government. It is also necessary to creating and maintaining public trust and confidence. Institutions need to consider privacy at each stage of their Open Government programs to ensure that personal information is protected and they are complying with relevant legislative requirements.

The purpose of this paper is to help institutions understand that privacy is not a barrier to Open Government, and that proactively addressing **privacy risks** is critical to its success.

2. DEFINITIONS

- **Big data** is extremely large and diverse datasets that may be analyzed to reveal patterns, trends, and associations, especially related to human behaviour and interactions.[1]
- **Business identity information** is the name, title, contact information, or the designation of an individual acting in a business, professional, or official capacity. Generally, it is not personal information.[2]
- **Data** is raw, unorganized facts and figures that need to be processed, such as a database containing a collection of numbers.
- **Data subject** is the individual to whom personal information relates (that is, a natural person, not an organization).
- **Direct identifiers** are variables that provide an explicit link to an individual and can directly identify them. Examples include name, email address, home address, telephone number, health insurance number, and social insurance number.[3]
- **Indirect or quasi-identifiers** can be used, either by themselves or in combination with other available information, to uniquely identify individuals. Examples include information such as gender, marital status, postal code or other location information, a significant date (for example, birth, death, hospital admission or discharge, autopsy, specimen collection, or visit), diagnosis information, profession, ethnic origin, visible minority status, and income.[4]
- **Information** is processed, organized data, such as an analysis of numbers in a database that makes them understandable and reveals their meaning and context.
- **Metadata** defines and describes the structure and meaning of information resources, and the context and systems in which they exist.[5]
- **Open Data** is the proactive release of government data in free, accessible and machine-readable formats, to encourage its use by businesses, the public, and government.[6]
- **Open Dialogue** is active and intentional engagement, using new ways to give the public a meaningful voice in planning, decision-making, and the development of government policies, programs, and services.[7]

---

1 ***Oxford Dictionary***, Oxford University Press, 2017 (online), accessed January 16, 2017.

2 Section 2(3) of the ***Freedom of Information and the Protection of Privacy Act*** (*FIPPA)* and 2(2.1) of the ***Municipal Freedom of Information and Protection of Privacy Act*** (*MFIPPA*).

3 Information and Privacy Commissioner of Ontario (IPC), ***De-identification Guidelines for Structured Data***, June 2016, 8.

4 **Ibid.**, 8-9.

5 Treasury Board of Canada, ***Standard on Metadata*** (online), modified June 24, 2010.

6 Government of Ontario, Open Government Engagement Team, ***Open by Default: A new way forward for Ontario*** (online), modified April 1, 2016.

7 **Ibid.**

- **Open Information** is the proactive release of information about government programs, services, and operations to improve transparency and accountability and increase public understanding and engagement.[8]
- **Personal information** is recorded information about an identifiable individual and includes, but is not limited to race, nationality, religion, age, sex, marital status, education, medical or criminal history, financial information, identifying numbers (for example, social insurance number), address, telephone number, fingerprints, blood type, and opinions. If there is a reasonable expectation that an individual can be identified from information (either alone or when combined with other information), such information will likely qualify as personal information.[9]
- **Privacy breach** occurs when personal information is collected, retained, used or disclosed in ways contrary to the provisions of *FIPPA* or *MFIPPA*.[10] A privacy breach may also occur when institutions subject to the *Personal Health Information Protection Act* (*PHIPA*) manage personal health information in ways that are contrary to the legislation.
- **Privacy risk** is something that could jeopardize or negatively impact the data subject's privacy such as an unauthorized collection, use or disclosure.

3. PROTECTING PERSONAL INFORMATION

Both *FIPPA* and *MFIPPA* define how personal information must be managed throughout its entire lifecycle, including:

- how and why personal information may be lawfully collected, used and disclosed
- its required level of accuracy
- how it should be secured
- how long it should be retained, at a minimum
- how it should be disposed of

Your institution may have other legislative privacy requirements (for example, some institutions may be health information custodians or employ them and be required to comply with *PHIPA* as well). Your institution may also have corporate policies that define other mandatory privacy requirements. The legislative and other privacy rules relevant to your institution are the framework within which your Open Government initiative must function.

8 **Ibid**.
9 Section 2(1) of *FIPPA* and *MFIPPA*.
10 IPC, ***Privacy Breach Protocol Guidelines for Government Organizations***, May 2014, 1.

You should identify and address privacy risks in the planning and design phases of your Open Government initiative. As your program evolves, continue to evaluate its impact on privacy to determine if new risks arise and if you need to mitigate them.

Staff responsible for access and privacy, such as your freedom of information and privacy coordinator, can help you understand your legislative and other privacy obligations so you can apply appropriate measures to protect personal information. Since Open Government programs operate alongside other programs and initiatives, it is important to harmonize the privacy protective measures undertaken by your institution.

Only collect, use, retain, and disclose personal information necessary to achieve your Open Government goals.

3.1 DEFINE PURPOSES

It is critical to define the specific goals or purposes of your Open Government initiative and whether you need personal information to achieve them. Your goals may include:

- providing the public with a way to request services or provide feedback
- communicating to the public and stakeholders
- gathering information about technical, policy, or regulatory problems
- collaborating on the design of new government programs
- surveying public interest about an issue[11]

Not all interactions with the public, stakeholders, or clients require the collection, use or disclosure of personal information. For example, if your goal is to gather information about a specific regulatory problem, you may be able to eliminate the collection of personal identifiers entirely and allow the public to participate anonymously. Or you may want to crowdsource information about road conditions, street lighting, and safety hazards. The system gathering this information could be designed to not record any identifying information about people making submissions.[12]

Compliance with privacy legislation is required if personal information is involved, so you need to know why or if you need to collect, use and disclose personal information, and you must clearly **communicate** those reasons to the **data subjects**.[13]

11 Jeff Jonas and Jim Harper, "Open Government: The Privacy Imperative," Chapter 29 in ***Open Government: Collaboration, Transparency, and Participation in Practice***, edited by Daniel Lathrop and Laurel Ruma, O'Reilly Media, Inc., 2010, 316 (online free sampler).

12 **Ibid.**, 317.

13 Sections 38 and 39 *FIPPA* and 28 and 29 *MFIPPA*.

3.2 AUTHORITY TO COLLECT, USE OR DISCLOSE PERSONAL INFORMATION

Determining if you have the authority to collect, use and disclose personal information is an essential step in protecting privacy and ensuring the sustainability of your Open Government program.

Early in your design process, consult with your access and privacy staff and legal counsel, if necessary, to ensure you have the authority to collect, use and disclose personal information relevant to your defined goals or purposes. *FIPPA* and *MFIPPA* prohibit you from doing so unless you meet specific criteria defined in the legislation.[14] If you do not have the authority, you may need to take action to obtain it, or re-design your Open Government initiative.

If you collect personal information without the authority to do so, it may be considered a **privacy breach**. As the oversight body, the IPC could order you to cease a non-compliant collection and to destroy the collected personal information.[15] This could adversely affect your institution's reputation and involve unnecessary expense.

The unauthorized disclosure of personal information to someone within your institution, or to an outside individual or organization, is a violation of privacy and may have significant consequences for both the individuals and your institution.

3.3 DATA MINIMIZATION

Data minimization is a principle of data protection enshrined in privacy legislation around the world including *FIPPA* and *MFIPPA*. It requires you to only collect, use, retain, and disclose the personal information necessary to achieve your specified goals or purposes. It also requires you to destroy personal information when it is no longer required to fulfil the defined purposes. In the context of Open Government, this principle applies to both data and information.

When determining whether you need personal information to achieve your objectives, the test to apply is one of necessity. Is personal information essential (that is, not just helpful) to accomplishing your purpose or function? Necessity means that there is no other way to perform the activity without the personal information. If personal information is required, consider data minimization when defining your information needs. Determine the minimum amount and type of personal information you need to collect, use and disclose.

14 Sections 38–43 of *FIPPA* and 28–33 of *MFIPPA*.
15 Section 59(b) *FIPPA* and 46(b) *MFIPPA*.

Data minimization is important to mitigate the risks posed by technology that enables the rapid collection, use and disclosure of data and information. Therefore, if possible, design restrictions or defaults into your Open Government systems, applications, or services to minimize personal information.

In particular, pay attention to **direct** and **indirect** identifiers such as internet protocol addresses and other device identifiers, cookies, and geolocation data. When this personal information is no longer needed (for example, the transaction or information exchange has concluded) it should be purged or de-identified at the earliest opportunity to minimize the risk of unauthorized use or disclosure. Unnecessary collection, use, retention and disclosure of personal information are significant triggers for privacy risks in the context of Open Government.

Over-collection of personal information can be a challenge when you interact with the public. Individuals may provide you with unnecessary personal information about themselves or others via social media or other means.

Your Open Government activities should be designed to enable individuals to only reveal the amount of personal information required for any given transaction or interaction.[16] For example, when engaging with the public through your feedback tools, determine if it is necessary for individuals to be identified. Consider:

- enabling the public to interact with your institution anonymously or pseudonymously
- generalizing the information being collected (for example, ask for an age range rather than specific age, or partial postal code instead of street address)
- providing clear notices advising that personal information is not required when you are engaging individuals
- including notices about the risk of sharing personal information through social media

3.4 EXCEPTION TO OPEN BY DEFAULT

The concept of open by default is a cornerstone of Open Government. It means that government-held data and information are presumed to be open to the public unless there is a compelling reason for them to remain unpublished.[17] The protection of privacy is one of those compelling reasons.

It is generally understood that personal information should not be published as part of Open Government because of the potential adverse impacts. For

16 Jonas and Harper, **"Open Government: The Privacy Imperative,"** 324.

17 Open Government Engagement Team, ***Open by Default: A new way forward for Ontario***.

example, Ontario's ***Open Data Directive*** requires that personal information not be released under the terms of the ***Open Government Licence—Ontario***. The City of Guelph's **Open Data Portal** only contains "public data that is not sensitive in nature (that is, data which is NOT personal or confidential) and does not identify or provide ways to identify individuals."[18]

However, for the purpose of transparency and accountability, there may be circumstances when it is in the public interest to make specific personal information publicly available, or when institutions are required by legislation to do so. Such circumstances do not mean that all personal information should be open by default. Making personal information public, when appropriate and authorized, is not the same as routinely publishing it as Open Data or Open Information under an Open Government licence.

If you publish personal information as part of Open Government, you have no control over how it may be used and by whom. There is nothing to prevent its use in profiling, data mining, and other activities that may have significant privacy implications for the data subjects. The growth of big data, with its ability to pull together and analyze disparate information, has heightened privacy concerns about the public disclosure of personal information or information that has not been sufficiently de-identified.[19]

The potential privacy risks associated with publishing personal information online are different from other forms of public access. You should carefully consider the privacy implications before you put any personal information on the internet.[20] It may not be appropriate to publish it as Open Data or Open Information.

Search engines automatically scan websites and catalogue information. This makes the contents of records posted on websites searchable. For example, a record containing an individual's name can normally be searched for and discovered via a search engine simply by entering that person's name.

It is also important to consider your metadata when publishing data and information because it can enable access and discoverability. Consideration of metadata is also important when engaging with the public because, depending on context, it may have privacy implications. It can facilitate tracking or monitoring of individuals, analytics, data mining, and re-identification of de-identified data.

If not managed correctly, metadata can reveal sensitive information about individuals or your institution, which may present significant privacy, confidentiality, security, or legal risks. It is vital to identify and consider what metadata is necessary prior to collecting, using or disclosing data or information.

18 City of Guelph, ***Open Data Frequently Asked Questions*** (online).

19 Teresa Scassa, Faculty of Law, University of Ottawa, ***Privacy and Open Government***, Future Internet, Volume 6, Issue 2, June 2014, 407.

20 IPC, ***Transparency, Privacy and the Internet: Municipal Balancing Acts***, August 2015, 2.

3.5 DE-IDENTIFICATION

De-identification is important to protecting privacy and, in turn, to building public confidence in Open Government programs.[21] Information is considered de-identified if it does not identify an individual directly or indirectly, and it is reasonable in the circumstances to conclude that the information could not be used, either alone or with other information, to identify an individual.[22] Personal information is de-identified through a process involving the removal or modification of both **direct identifiers** and **indirect or quasi-identifiers**.

Privacy requirements defined in *FIPPA* or *MFIPPA* only apply to personal information (that is, information about an identifiable individual). When a record containing personal information is properly de-identified, it is no longer personal information and not subject to Ontario's legislative privacy rules.

De-identification is important to protecting privacy and, in turn, to building public confidence in Open Government programs.

Depending upon the nature of the records involved and the context, de-identification may be a complex process. The amount of de-identification required should be proportional to the risk created by releasing the data. The level of risk depends on the sensitivity of the data, the number of data subjects involved, and how the data will be released (that is, to defined parties bound by a data sharing agreement or to the public on the internet). The higher the risk, the greater the amount and types of de-identification required in order to mitigate the risk of re-identification.

Do not assume privacy is protected simply by removing direct identifiers from a dataset. The large volume of data already available in today's big data environment means that even innocuous or anonymized datasets can contribute to the re-identification of individuals (that is, associating the data to an identifiable individual) when matched with other publicly available information.[23]

At a minimum, prior to publication, you should make sure that:

- a robust assessment is undertaken to identify the risks of re-identification in your particular circumstances
- direct and indirect identifiers are removed or appropriately modified in accordance with the results of the above assessment

Given the potential harm to data subjects, assessing the risks of re-identification is an essential step prior to publicly disclosing de-identified data or information. To do this effectively and to mitigate the privacy risks to an acceptable level, you need a defined and consistent de-identification process that involves subject-matter experts, which is discussed further in

21 Office of the Information and Privacy Commissioner for British Columbia, ***Investigation Report F13-03, Evaluating the Government of British Columbia's Open Government Initiative***, July 25, 2013, 33.

22 IPC and Khaled El Emam, ***De-identification Protocols: Essential for Protecting Privacy***, June 25, 2014, 3.

23 Scassa, ***Privacy and Open Government***, 398.

the following section. The IPC's ***De-identification Guidelines for Structured Data*** provides additional information about related processes and required analysis.

4. ADDRESS PRIVACY PROACTIVELY

To maximize open by default and public engagement, you need to proactively minimize the impact on privacy and ensure compliance with relevant privacy legislation. The best way to do this is to embed privacy protection so that it becomes part of the core functionality of your Open Government services. Consider privacy issues as you design, implement, and monitor your activities to ensure privacy risks are identified and appropriately addressed. There may be instances when the risks to privacy are too great to proceed with an Open Government activity.

Outlined below are key factors to help you proactively protect privacy as you advance your Open Government agenda.

4.1 PRIVACY PROTECTION FRAMEWORK

To ensure your institution meets its legislative privacy obligations, consider:

- including a requirement in your Open Government policy, by-law, mission, action plan, or other guiding instrument to protect privacy and comply with applicable legislation
- establishing a governance framework with defined accountability and decision-making for privacy protection
- ensuring your Open Government licence defines conditions or prohibitions related to the use of personal information
- engaging the appropriate parties to identify and address privacy risks, such as representatives from program, legal, privacy, information technology, security, and communications areas, as well as de-identification experts, as needed
- defining the roles and responsibilities for protecting privacy for each party involved in your Open Government program, including **third-party service providers**
- creating and consistently following a process that enables you to effectively identify data and information that:
    - should not be proactively disclosed (that is, define the exceptions to open by default)
    - needs to be de-identified prior to publication

- developing a de-identification process and ensuring that it is done by trained and knowledgeable parties:
    - determining the appropriate de-identification methodology, techniques, and tools to use in the circumstances
    - evaluating re-identification risks prior to publication, as well as periodically on an ongoing basis to determine if that risk has changed
- defining a privacy breach response protocol
- implementing audit procedures to determine if your privacy protective measures, including de-identification, are effective, current, and being followed
- defining a process to **monitor and evaluate** your Open Government program to ensure it protects privacy and complies with applicable privacy legislation

4.2 TRAINING

Regular and ongoing training in protecting privacy is vital to the success of Open Government. Appropriate and effective training builds capacity and enables your staff and third-party service providers to comply with privacy legislation and policies, and to make informed decisions about when and how to:

- appropriately limit the collection, use and disclosure of personal information when engaging with the public
- protect privacy when publishing data and information

The City of Toronto's 2015 staff survey on Open Government identified privacy as a top barrier to openness.[24] Privacy training for all parties involved with your Open Government initiative, including your decision-makers, can help ensure they understand when privacy is a legitimate concern and when it is not.

It is important that privacy not be mistakenly viewed as an impediment to Open Government. For example, sometimes **business**, property, or other information is incorrectly identified as personal information. With adequate training, you can ensure that these misunderstandings are corrected and do not impede the progress of your program. In addition, proper documentation defining your institution's **privacy protection framework** is an essential prerequisite and tool for training.

24 City of Toronto, ***Open Government Staff Survey***, 2015.

4.3 PRIVACY IMPACT ASSESSMENTS

Undertaking a privacy impact assessment (PIA) on your Open Government activities can help you proactively address privacy. A PIA is a risk management tool used to identify the actual or potential impacts that a proposed or existing information system, technology, program, process, or other activity may have on an individual's privacy.[25] By completing a PIA, you should be able to:

- determine whether your activity needs to involve personal information
- identify the privacy risks and take action to address them prior to implementation
- determine your legal authority to collect, use and disclose personal information
- demonstrate due diligence and evidence of compliance needed to support informed decision-making

Neither *FIPPA* or *MFIPPA* require that institutions complete a PIA. However, PIAs are widely recognized as a best practice. It is an essential tool in the analysis of privacy implications associated with information management and technology systems, programs, and applications, including those related to Open Government.

4.4 THIRD-PARTY SERVICE PROVIDERS

To enable some of your Open Government activities, you may need or want to engage third-party service providers. When you outsource a service or activity, your institution continues to be accountable for complying with applicable privacy legislation. You cannot contract out or avoid your privacy obligations through the use of a service provider. You also cannot require your service provider to do something that you would not be permitted to do.

To the greatest extent possible, you should enter into agreements with your service providers that define their duties and responsibilities to protect privacy. Your contracts need to address compliance with legislation, custody and control of personal information, appropriate security measures, data location, response to privacy breaches, audits, use of sub-contractors, staff training, and dispute resolution.[26]

If you want to use third-party services but do not have the ability to define the terms of service (discussed further in the following section) you should determine whether such services are appropriate to use, given the sensitivity of the information involved and the privacy risks.

25 IPC, ***Planning for Success: Privacy Impact Assessment Guide***, May 2015, 2.

26 IPC, PC12-39, ***Reviewing the Licensing Automation System of the Ministry of Natural Resources: A Special Investigation Report***, June 2012, 7–8.

4.5 TRANSPARENCY

For Open Government to be successful, you must be transparent about the collection, use and disclosure of personal information by your institution and other parties. This is particularly important because some users may not be aware of what they reveal when they enter digital environments.[27]

Both *FIPPA* and *MFIPPA* include an obligation to provide a notice of collection that explains your legal authority for the collection, the purposes for which the personal information will be used, and contact information of someone in your institution who can answer questions about the collection.[28]

You should also be transparent about:

- how your systems, applications, and services work (for example, the collection of cookies, use of web analytics, security measures, etc.)
- your privacy policies and practices
- what data or information you collect, use, retain and disclose, the sources/recipients, and for what purposes
- how you analyze and aggregate the data and information and for what purposes
- your use of third-party services and potential privacy risks
- alternative ways to communicate with your institution or participate in an activity
- the steps users can take to protect their personal information
- how users may access and correct their personal information
- how users may submit a complaint about how their personal information is collected, used and disclosed, and how you will deal with it

When designing your Open Government activities, ensure this information is clear and accessible so individuals can make informed choices about if, or how, they want to participate and what personal information they want to reveal.

Transparency is particularly important when third-party service providers are involved. Be aware that if you use a free web-based service or other third-party service where you cannot define the terms of use, you may be exposing your users to privacy risks.

27 Jonas and Harper, "**Open Government: The Privacy Imperative,**" 322.

28 Section 39(2) of *FIPPA* and 29(2) of *MFIPPA*.

Individuals may make incorrect assumptions about privacy protection if an institution utilizes social media to engage with them. They may not understand that online transactions and activities leave a data trail or that social media companies compile user-generated data, and then use or share this information in ways that may not be clear to them. Some individuals disclose their personal information willingly on social media sites without fully understanding the way their information is used, or the associated privacy risks.[29]

To achieve the full benefits of Open Government you need to facilitate the public's participation. Educating the public about your Open Government program supports this objective. Individuals need to understand the nature of digital technologies and the internet, and how their personal information is collected, used and disclosed by you and others.[30]

For example, using social media to engage the public about an issue or service as part of your Open Dialogue activities may involve soliciting as well as disseminating information. In such situations, there may be the potential for the collection of personal information. You should provide notice of collection and inform your users about the use of third-party service providers and potential privacy risks in a manner that is in keeping with the nature and practices of the social media used. For example, consider dialogue boxes or interactive tools that explain how the information will be used or disclosed; use of banners and other alerts, advertisement services, and reminder messages; and links to service providers' privacy policies.

Proactively integrating privacy into your design and implementation will help you anticipate and effectively address privacy risks.

4.6 ONGOING REVIEW

As your Open Government program expands and evolves you will need to refresh, re-assess, monitor, and evaluate your activities to ensure they continue to have value to both the public and your institution. Periodic reviews of the effectiveness of your privacy policies and practices is an important part of that evaluation process. Over time many factors can change that impact privacy including the type of information involved, nature of your users, and the capacity of technology. In addition, you should always review your practices if there is a **privacy breach** or other suspicious activity and take steps to address new risks.[31]

29 ***Privacy and Social Media in The Age Of Big Data***, Report of the Standing Committee on Access to Information, Privacy and Ethics, April 2013, 8.

30 Open Government Partnerships, ***Establish a programme of public education about protecting personal information***, Open Government Guide (online).

31 **Ibid.**

5. CONCLUSION

Government transparency and access to data and information are vital ingredients for a free and functioning democratic society. Without them, the public cannot participate meaningfully or hold government accountable.

The protection of privacy is essential to maintaining the public's trust and for Open Government to succeed.[32] Far from privacy being a barrier to Open Government, privacy requirements can help drive the need for institutions to identify their information assets, to understand the types of information they hold, and to develop appropriate governance.[33]

It is important to embed privacy protection into your Open Government initiative. Proactively integrating privacy into your design and implementation will help you anticipate and effectively address privacy risks. It is also important for your Open Government program itself to be transparent.[34]

32 Kieron O'Hara, ***Transparent Government, Not Transparent Citizens: A Report on Privacy and Transparency for the Cabinet Office***, 1–2.

33 Dr. Elizabeth Coombs, ***Privacy and the NSW Government open data initiative***, Open Data Forum, Speech, November 11, 2013.

34 O'Hara, ***Transparent Government, Not Transparent Citizens***, 1–2.

Open Government and Protecting Privacy

Information and Privacy
Commissioner of Ontario

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

March 2017