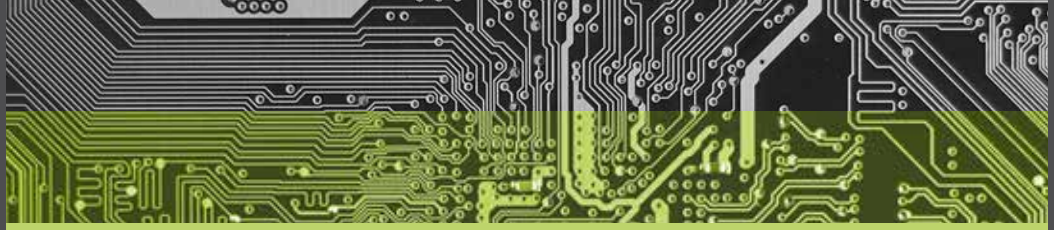

APRIL 2018

TECHNOLOGY FACT SHEET

Smart Cities and Your Privacy Rights

New technologies promise to help municipalities better manage urban environments and deliver services in a more effective and efficient way. They can help to make communities more liveable, sustainable, and fair. Many involve the collection and use of large amounts of information, including personal information. Cities or municipalities that use these connected technologies are often described as "smart cities."

This fact sheet was developed to help members of the public understand smart cities and how they can impact an individual's privacy

The Office of the Information and Privacy Commissioner of Ontario (IPC) provides independent oversight of the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*). This act protects the privacy of personal information by setting rules for its collection, use and disclosure by municipalities and municipal institutions. These rules also give individuals the right to access their own personal information.

The IPC has developed this fact sheet to help the public understand smart cities and how they can impact an individual's privacy.

WHAT ARE "SMART" CITIES?

Smart cities use technologies that collect data to improve the management and delivery of municipal services, support planning and analysis, and promote innovation within the community. By collecting large amounts of data, often in real-time, municipalities can gain a greater understanding of the quality and effectiveness of their services. For example, commuter traffic flow data can identify congestion

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

hotspots and inform planning and urban design. Insights can also be generated by linking the collected data with other data sources and using analytics technology to uncover patterns and connections in large data sets.

This can lead to "smart" actions, such as:

- sending a signal to garbage collectors when sensors indicate that garbage bins are full
- turning on park water sprinklers when sensors detect the soil is dry
- synchronizing street lights with traffic flows
- directing self-driving vehicles to available parking spots using GPS information collected from the vehicles.

Information collected, used, retained and disclosed by smart cities can, and often does, include personal information

WHAT INFORMATION IS COLLECTED AND HOW?

Information collected, used, retained and disclosed by smart cities can, and often does, include personal information. For example, some smart city technologies collect information about individuals from their mobile devices, including information about their movements around the city.

Personal information can also be collected from municipally owned and operated sensors, such as audio and video recording devices, or vehicle licence plate readers.

Municipalities may enter into information-sharing agreements with third parties, such as smartphone app providers, or companies that install and manage sensors and communications infrastructure. These agreements may require or allow third parties to collect and use personal information for their own purposes as well as for the purposes of the municipality.

WHO OWNS THE INFORMATION?

Municipalities need to take steps to ensure that the non-personal information collected by their private sector partners is available as a public resource. They can do this by ensuring that their contractual arrangements do not give proprietary rights over the information to private sector partners who would use the data for commercial purposes.

A U.S. police service contracted with a software provider to compile and analyze information about criminal and civil matters. When the contractual relationship ended, the service lost access to a significant amount of data and insights generated during that time due to the software company's claims over intellectual property rights.

HOW CAN SMART CITIES AFFECT PRIVACY?

When municipalities use technologies to collect personal information for any purpose, they must comply with *MFIPPA*. Smart cities raise concerns about compliance with *MFIPPA* in a number of different ways. For example:

Unauthorized collection of personal information and surveillance

MFIPPA permits the collection of personal information by municipalities where it is necessary to administer their lawfully authorized activities. Any collection of personal information that exceeds what is necessary for those activities is not permitted.

Smart city technologies enable the collection of information about residents going about their daily lives—potentially creating personal profiles of individuals' behaviour, interests and interactions with others, especially when that information is combined with other information.

Great care must be taken to ensure that smart cities do not become infrastructures for mass surveillance

A major European city installed "smart" internet-connected garbage and recycling bins throughout the city featuring large video screens on each side to broadcast news, information and ads to the public. Unknown to passersby, the bins also collected signals from their Wi-Fi enabled devices, which can be used to identify individuals and track their travels. In the first month of operation, over a million unique devices were recorded. In response to a public outcry, the city shut down the "spying trash cans."

Personal information used for secondary purposes

MFIPPA limits how personal information can be used. The use limitations in the act are based on a key principle of privacy protection, which requires that, with some exceptions, personal information can only be used for the purposes for which it was collected, or for a consistent purpose. For example, personal information collected to assist with urban planning decisions should not be used to provide targeted advertising to individuals. Doing so constitutes an unauthorized secondary use under *MFIPPA*.

Smart city technologies such as gunshot detection systems use microphones installed on streetlights around a city to detect the location of gunshots and alert police quickly. These same microphones are also capable of recording street-level conversations for very different purposes.

Unauthorized disclosures of personal information

MFIPPA requires Ontario municipalities to have reasonable measures in place to protect personal information from unauthorized access and disclosure.

As with any complex, connected technology smart city systems are vulnerable to attacks by hackers. The more points of information collection, processing and access to the systems, the greater the risk of a security breach. Privacy breaches can also happen as a result of unauthorized access and misuse of personal information by individuals employed by the municipality or third parties.

Complex, connected technologies used by smart cities may be vulnerable to attacks by hackers

> A Canadian city that offered residents smartphone apps to track garbage, recycling and yard-waste pickup schedules discovered that the application's database had been hacked, exposing the personal information of thousands of residents.

There is a strong desire to make some information collected by smart city technologies publicly available to support innovation within communities. Municipalities need to take steps to ensure that any personal or identifying information has been removed from any data that is released to third parties, or made publicly available in support of open data initiatives.

HOW CAN PRIVACY RISKS BE MINIMIZED?

Good planning and design can minimize risk and ensure that individual privacy is protected. To protect privacy in smart city projects, municipalities should take a number of steps, including:

- Conducting **privacy impact and threat risk assessments**. These are widely recognized tools to identify privacy and security risks, and the measures needed to reduce those risks. They should be conducted when designing new technologies and programs involving the collection of personal information.
- Applying a **data minimization** approach to the design and operation of the technology. This means that municipalities should ensure they, and any contracted third parties, do not collect, use, retain or disclose personal information if other information will serve the required purpose. In all cases, where the goals can be achieved using less privacy invasive alternatives, those alternatives should be pursued.
- Ensuring that when it is necessary to collect personal information, steps are taken to remove any identifiable information at the earliest opportunity. Wherever possible, municipalities and their agents should only use, retain, and disclose **de-identified** information.

- Putting in place a privacy and access **governance** program that includes comprehensive security policies and procedures, strong oversight of third parties, and privacy breach response policies. The program will also need to include ways for individuals to exercise their right to access their own personal information.
- Ensuring **community engagement** and **project transparency** to help all members of the public understand how they might be affected and what options they may have to participate and provide input.
- Obtaining informed **consent,** where required by law**,** directly from the individuals whose personal information may be used and disclosed or requiring the third parties involved to get consent. When possible, individuals should be allowed to opt out of participating.

Good planning and design can minimize risk and ensure that individual privacy is protected

WHAT IS THE IPC DOING TO PROTECT MY PRIVACY?

The IPC is committed to ensuring your privacy is protected. Smart cities create new challenges and opportunities for Ontario's municipalities and communities. We believe that with careful planning and education about the unique issues raised by smart city technologies, personal information can be collected and used in a privacy-protective way. The IPC is working with local and national leaders to encourage transparency and ensure that privacy protections are built into smart city initiatives.

WHAT RIGHTS DO I HAVE UNDER ONTARIO'S PRIVACY LAWS?

It's your community too. You can help shape its future and protect your own personal information and privacy.

If you have questions about what personal information a municipality is collecting or how it is being used, consult their website or contact them for more information.

If you would like a copy of the information a municipality has about you, you can file an access to information request. To learn more about making an access to information request and what you can do to protect your privacy, visit the IPC's website: **www.ipc.on.ca**.

ADDITIONAL RESOURCES

- **What is Personal Information?**
- **Big Data and Your Privacy Rights**
- **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