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

May 1, 2013

Edith Ramirez
Chairwoman
Federal Trade Commission
600 Pennsylvania Avenue N.W.
Room H-113 (Annex B)
Washington, DC 20580

Dear Chairwoman Ramirez:

Re: FTC call for input on the privacy and security implications of the Internet of Things

I am writing to share with you my response to the April 17, 2013, Federal Trade Commission's (FTC) release seeking input on the privacy and security implications of the Internet of Things, in advance of a public workshop to be held on November 21, 2013. I applaud your leadership in this area, and the thoughtful consideration I am certain you will give to some of the key challenges in privacy protection posed by the growing connectivity of consumer devices.

I have reviewed the call for input which asks for submissions to identify the technologies that make up the Internet of Things (e.g. RFID, barcodes, wired and wireless connections), their current and future uses, any significant developments, as well as consumer benefits within various consumer scenarios including the use of cars, appliances and medical devices. Examples provided in the call include the use of mobile phones to open car doors, physicians monitoring vital signs remotely, etc. My submission provides you with examples of my experience on the privacy and security implications of this important area, and hope that your staff will find them helpful as the FTC develops the agenda for the workshop.

Do not hesitate to contact me if you would like any further information. We would also be pleased to participate in the workshop to share our experiences.

Sincerely yours,

Ann Cavoukian, Ph.D.
Commissioner

Enclosures

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

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

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

Information and Privacy
Commissioner of Ontario

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

Submission of the Information & Privacy Commissioner, Ontario, Canada

Response to the *FTC call for input on the privacy and security implications of the Internet of Things*

April 29, 2013

Introduction

As the Information and Privacy Commissioner of Ontario, Canada, I oversee the freedom of information and privacy laws in Canada's most populous province. Over the past decade and a half, I have been actively engaged in raising awareness of how to build privacy into the many areas that are converging to create the Internet of Things, including near field communication, radio-frequency identification technology, as well as wireless and mobile technology. I have examined such technologies in many different contexts, including within the emerging Smart Grid, and remote home health care.

Examining the privacy and security implications of the Internet of Things is especially pressing at this time due to the incredible advances in the amount of information produced by information technology, as well as increased computer processing power and algorithms that can now make

sense of all this data. When considering the tracking and profiling potential of such 'Big Data' technology,[1] it becomes clear that a better understanding of the privacy implications of connected and automated devices is needed. As such, the FTC's plans to hold a workshop on these issues could not come at a better time.

Fortunately, advances in technology and business practices are also taking place in the area of *Privacy by Design* and are directly applicable to the Internet of Things. As you know, "privacy by design" has been my mantra since I published a paper in 1995 with the Netherlands on advancing privacy protection through the pursuit of privacy-enhancing technologies. I was very pleased to hear this message repeated in the FTC's *Report on Protecting Consumer Privacy*. In a number of my Office's publications, we have been able to show that the protection for privacy can be assured while also allowing devices to continue to connect and perform various functionalities. A few examples from those publications are provided below.

RFID and Sensor Technology

In the simplest terms, a sensor is an instrument that detects or measures a physical or environmental characteristic or state, and transmits and/or records the reading in some form (e.g., a visual display, audio signal, digital transmission, etc). Sensors appear in an endless array of applications, ranging from the simple everyday (e.g. mercury thermometers, gym equipment handles that measure heart rate) to the complex, such as powerful telescopes that can detect distant galaxies. Multiple sensors used jointly are referred to as a 'sensor network.' The Internet of Things can be considered a type of sensor network whose components (nodes, devices, etc.) interact via wired and wireless connections.

When considering issues such as privacy in sensor-based systems, it is not sufficient to focus on only the sensors themselves. Instead, the entire end-to-end flow of data generated by the sensor system must be examined. There are four primary points at which privacy should be considered in sensor-based systems: the monitored individual, the sensors, the processing/display device, and the people/organizations that are able to access the data at any point (including those who may attempt to access the data without a legitimate purpose).

A sensor system many are familiar with is Radio Frequency Identification (RFID), in which 'readers' are able to sense the presence of 'tags', and a communication protocol allows the sensed tag to transmit any data stored in its memory back to the reader for processing. RFID tags contain microchips and tiny radio antennas that can be attached to products and other items. They transmit a unique identifying number to an electronic reader, which in turn links to a computer database where information about the item is stored. RFID tags may be read from a distance quickly and easily, making them valuable for managing inventory but pose potential risks to privacy if linked to personal identifiers.

My Office released *Privacy Guidelines for RFID Information Systems* (available online at www.ipc.on.ca) for the growing field of RFID in collaboration with GS1 Canada, an industry

[1] *Privacy by Design in the Age of Big Data,* Dr. Ann Cavoukian and Jeff Jonas, June 2012 (available online at www.ipc.on.ca).

association that sets standards for electronic product codes. It is important to note that although RFID technology deployed in the supply chain management process poses little threat to privacy, item-level use of RFID tags in the retail sector, when linked to personally identifiable information, can facilitate the tracking and surveillance of individuals. The *Guidelines* are based on three overarching principles:

- Focus on RFID information systems, not technologies: The *Guidelines* should be applied to RFID information systems as a whole, rather than to any single technology component or function;
- Build in privacy and security from the outset – at the design stage: A thorough privacy impact assessment is critical, and wherever possible, efforts should be made to minimize the identifiability, observability and linkability of RFID data; and,
- Maximize individual participation and consent: Use of RFID information systems should be as open and transparent as possible, and afford individuals with as much opportunity as possible to participate and make informed decisions.

Though the above represents the considerations that must be made when designing a sensor system based on a particular technology (RFID), I wish to point out the importance of determining and addressing the privacy and data security concerns specific to each sensor-based application. For example, RFID-based systems differ from other sensor-based systems in that the user can be allowed control of the device that pushes out data (i.e. the RFID tag), through on-off switches, shielding mechanisms or simply not carrying the tag (or item in which it is embedded).[2] Many other sensor-based systems, on the other hand, give individuals control over the collection point of information, through options regarding what sensors are installed, where they are installed, and when they are active.

Sensors and In-home Health Care

Sensors installed within a patient's home can alert caregivers to changes in behaviour or physical state that may go unreported or unnoticed by the patient, but which represent important symptoms for proper diagnosis and treatment. Patients may also see better clinical outcomes with monitoring devices installed in their homes without significant restriction on their daily activities. To demonstrate the integration of *Privacy by Design* into sensor-based home health care technologies, my Office worked with the Intelligent Assistive Technology and Systems Lab (IATSL) at the University of Toronto and Toronto Rehabilitation Institute. IATSL is considered to be an international leader in the development of intelligent home systems, with a focus on aging-with-choice (meaning the freedom to choose where one would like to live) and older adults with dementia.

---

[2] We have described this in: *Adding an On/Off Device to Activate the RFID in Enhanced Driver's Licences: Pioneering a Made-in-Ontario Transformative Technology that Delivers Both Privacy and Security*; *Transformative Technologies Deliver Both Security and Privacy: Think Positive-Sum not Zero-Sum, March 2009*; and, *Video: A Word About RFIDs and your Privacy in the Retail Sector, March 2006* (available online at www.ipc.on.ca).

Most of the assistive technologies developed at IATSL use computer vision as their primary sensor. Computer vision uses cameras (both still and video) to capture images that are then analysed by computers to extract and compile data of interest. One system employs various computer vision and artificial intelligence techniques to autonomously provide cues to an older adult with dementia to guide him or her through common activities of daily living, such as hand washing. Another system is designed to automatically detect when an adverse event, such as a fall, occurs and to work with the user to procure appropriate assistance.

In the case of the computer vision-based systems developed by IATSL, this collection creates particularly rich datasets regarding the user's actions within his or her home. IATSL researchers were able to avoid potential privacy issues through the design and implementation of features that adhere to *Privacy by Design* principles.[3] For instance, much of the data processing can usually be done within the sensor device itself, or on a local (in-home) processor to which the sensor is directly connected via a cable. Transmitted data can also be formatted to contain only the reading and a sensor ID and not transmit any information about the user, the type of sensor, or any kind of index that might indicate that readings from multiple sensors refer to the same individual (this information being added, as necessary, at the processing stage). For further information, please consult the paper *Sensors and In-Home Collection of Health Data: A Privacy by Design Approach* (available online at www.ipc.on.ca).

Mobile Devices and Remote Home Health Care

Health care organizations are recognizing that mobile devices can be employed to improve the delivery of patient care. In our paper *Innovative Wireless Home Care Services: Protecting Privacy and Personal Health Information* (available online at www.ipc.on.ca) we describe a pilot involving the use of BlackBerry smartphones and Bluetooth connected blood pressure monitors in the delivery of home health care services. The solution was designed to help clients with chronic hypertension effectively manage and monitor their condition, while maintaining an active lifestyle. The solution enables healthcare staff to monitor in real-time client blood pressure and other vital signs, such as blood glucose, weight and blood oxygen levels, so they may respond quickly when necessary. For example, if blood pressure readings and other vital signs trend abnormally, staff may send an email to the client's smartphone reminding him or her to take medications, or take other measures such as notifying the client's physician.

A major focus of the smartphone deployment was to maintain a high standard of privacy protection for their clients' personal health information. Privacy-protective features were engineered directly into the smartphone and applications at the outset. In case of loss or theft, safeguards include remote password and encryption, remote wipe and lock, and limiting the number of attempts to gain access before erasing memory. Also, end-to-end encryption is used to prevent interception. For example, data travelling through the Bluetooth connection between a patient's blood pressure monitoring device and smartphone is encrypted.

---

[3] *Privacy by Design: The 7 Foundational Principles,* Dr. Ann Cavoukian, August 2009 (available online at www.ipc.on.ca).

Conclusion

The above represents a small sampling of the technologies we have examined from a privacy and security perspective, as it relates to the growing connectivity of consumer devices. We have further research posted on our website (www.privacybydesign.ca) in the areas of Smart Meters and the Smart Grid, de-identification of data, near field communication (i.e. smart cards, tap n' go systems), geo-location data and mobile devices, and wireless technology, that may be helpful as the FTC examines the privacy and security implications of the Internet of Things.

I thank the FTC for the opportunity to provide input. My Office will be following future developments that flow from this important initiative – we are available to provide any further information as requested.

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

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

www.ipc.on.ca
www.privacybydesign.ca