Office of the
Privacy Commissioner
of Canada

The Internet of Things

An introduction to privacy issues with a focus on the retail and home environments

Research paper prepared by the Policy and Research Group of the Office of the Privacy Commissioner of Canada

February 2016

Table of Contents

Abstract

This research paper is intended to help individuals understand how their privacy will be affected by the online networking of a multitude of uniquely identified, everyday objects, which has come to be known as the Internet of Things. Attention to these issues is needed now: rapid technological innovation, consumer demand and dropping costs are fueling the development and adoption of a new generation of low-energy sensors. These sensors, integrated in consumer items and infrastructure, can amplify the tracking and profiling risks that are characteristic of the mobile and wearable computing environment. Without adequate protections, these developments may pose significant risks to our privacy.

This research paper provides an overview of the Internet of Things technologies generally, and with special application in the retail and home context. It then goes on to examine some of the challenges that this new environment creates through the lens of specific privacy issues: customer profiling, accountability, transparency, ethics of data collection, access and correction rights, the existing consent model, as well as the challenges of device and information security.

Introduction

The Internet of Things has been compared to electricity,[1] or a nervous system for the planet,[2] to illustrate phenomena that are at once pervasive, unseen and will become crucially integrated within the fabric of our society.

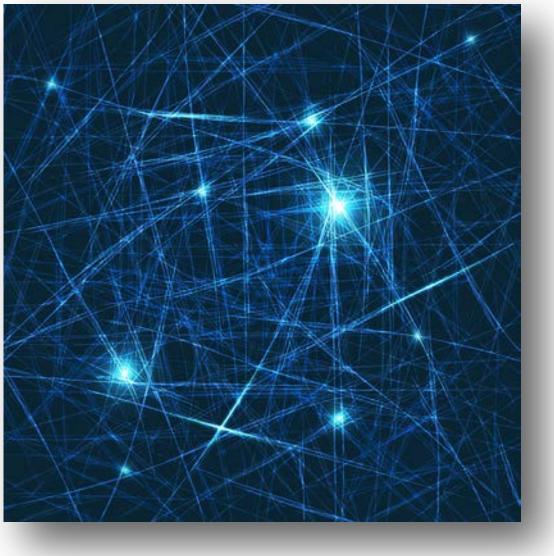
In general, the “Internet of Things” is the networking of physical objects connecting through the Internet. The Internet of Things is not a new concept, as devices have been communicating with each other for a number of years. The difference now is that:

- electronic devices and everyday objects, especially consumer products, are increasingly being built to facilitate interoperable communication through sensors and Internet connectivity;
- sensors are becoming more sophisticated;
- objects and devices have the ability to seamlessly connect and communicate a wide range of online and offline information (including location, biometrics, purchases, and online browsing history);
- Internet of Things computing devices are becoming affordable and accessible for individuals and organizations of all sizes, including small- and medium-sized enterprises (SMEs); and
- cloud computing and Big Data analytics are available for all organizations to store information, share it, and make inferences about their clientele.

Governments, businesses and data protection authorities around the world are trying to anticipate the possible impacts of the Internet of Things and with good reason. Several international experts, thinkers and technology builders are forecasting[3] profound political, social and economic transformations; concerns about privacy and surveillance are chief among them. Governments in Europe[4] and the US[5] have undertaken public consultations to probe into anticipated impacts. A number of industry associations are working on Internet of Things-related projects.[6] As well, the European Commission’s Article 29 Data Protection Working Party, which includes representatives from European data protection offices, adopted an opinion on the Internet of Things,[7] where it set out a number of serious privacy risks and detailed recommendations for addressing them.

Echoing several of the messages in the Article 29 Working Party opinion, international data protection authorities adopted the Mauritius Declaration on the Internet of Things.[8] In this declaration, regulators made several observations, concluding that sensor data are so high in quantity, quality and sensitivity, that such data should be regarded and treated as personal data. They commented on the business models that they anticipate to be spawned by the Internet of Things, recognizing that the value is not in the devices themselves, but rather in new services related to the Internet of Things and in the data they can amass and combine. The regulators also highlighted transparency as a key concern, arguing that consent obtained on the basis of existing privacy policies—lengthy and complex as they are—is not likely to be informed. As well, the regulators expressed deep concern about the security challenges posed by the Internet of Things.

Ultimately, today's profiling, tracking and targeting of individuals or groups by organizations of all kinds are expected to become more nuanced, specific and accurate with the Internet of Things. If a device becomes linked to us in some way, it becomes a data point that can be tracked and mined for patterns in our behaviour.[9] Companies will be looking to exploit these data to develop new business models and transition from selling us just "things" at one point in time, such as a battery operated fire detector, to value-added, for-fee services, such as remote fire detection monitoring.



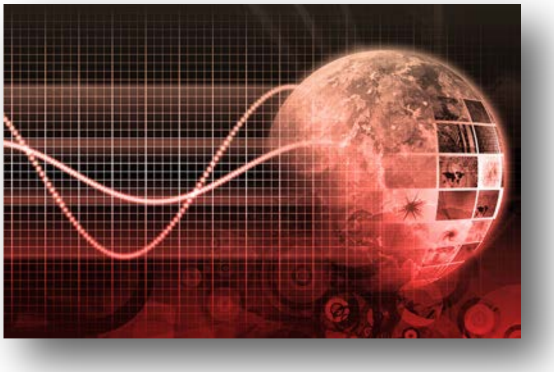
The data generated by these devices, their interactions and their ability to reveal contiguous information about our daily activities will be a crucial element of Big Data analytics conducted by governments and the private sector. These developments will pose profound challenges to the legislative frameworks protecting the privacy and security of personal information and create the real potential for seamless cyber and physical surveillance.

Conveying meaningful information about privacy risks in order to inform user choice remains a challenge in the mobile space, particularly with a small screen and intermittent user attention, as we described in our guidance to mobile application developers.[10] Wearable computing, which we examined in a separate research paper,[11] further compounds the challenge of reaching users with relevant information at the right time and in a form and format that they can access and understand. But the Internet of Things, where computing power may become entirely invisible to the user, renders privacy risk information even more opaque and adds to the difficultly of enabling informed consent.

1. What is the Internet of Things?

There are a variety of definitions and graphical representations[12] of the Internet of Things, most of which include the following elements:

- cheap, ubiquitous and uniquely identifiable sensors, devices or “things;”
- the means to react or carry out a command;
- integration into a dynamic global network infrastructure or “network of networks;”
- use of standard and interoperable communication protocols;
- connection of the physical world with the cyber world;
- both physical and virtual “things” that have “identities, physical attributes, and virtual personalities”;
- devices that communicate without human intervention and are “self-configuring;” and
- devices that generate data stored in the cloud and involve data processing, aggregation and analytics.[13]



The Internet of Things has components that range in complexity, from simple identification tags to complex machine-to-machine communication.[14] Objects are becoming enhanced with computing and communication powers capable of reproducing and replacing human observations and senses in the virtual world.[15] Networked traffic cameras and radio-frequency identification tagging of shipments in the supply chain are well-established examples. Location tracking devices are now available to find our car keys,[16] pets[17] and even our children and our elderly parents or grandparents.[18] Remote monitoring of temperature and activity in our homes is also becoming more common. We are starting to wear technologies that monitor, track and report our fitness levels. Smart electric meters are helping us monitor our home energy use. Connected cars are self-diagnosing problems as well, capable of feeding in location information about traffic congestion and providing information about our driving habits to insurance companies that can affect our premiums.

Some of the technologies involved

There are several technologies involved in the Internet of Things, such as radio-frequency identification (RFID), near-field communications (NFC), machine-to-machine communication (M2M) as well as wireless sensor and actuator networks.

- RFID is an important enabling technology for the Internet of Things and is used mainly for tracking and tracing objects. We have written[19] and funded several resources on the privacy implications of RFID over the last decade. It provides the ability to link all manner of inanimate objects from our daily life.[20]
- NFC can be understood as having evolved from RFID and is a short-range, low-power wireless way to transfer small amounts of data between devices.[21]

- M2M communication generally refers to the Internet of Things for industrial, business and commercial applications, while the Internet of Things is discussed more in the context of consumer applications.[22]
- Wireless sensors are different from RFID technologies in that they measure features of our physical environment, such as pressure, heat and humidity.[23]
- Actuators convert information or energy from sensors into action by transmitting it to another power mechanism or system, such as heating or cooling a room.[24] No human intervention need be involved in the decision-making process.[25]

Selected resources on the history[26] and technical workings of the Internet of Things have been included in the notes to this paper.[27]

> "The massive amount of data present in the IoT means there is no question that the IoT, en masse, is personal. It simply is. If you can access, correlate, and associate identity and activity in the IoT, you will pretty much be able to write a biography that will shock mothers and end marriages. Every time."
>
> The Privacy Engineer's Manifesto, 2014

Even though the term "Internet" is part of the Internet of Things, the structures of the networks that are meant to be described by this term are much more diverse. For example, a mesh network can be an Internet of Things, in that each connection point, or node, in the network is connected to other nodes around it, rather than going through a central router.[28] In a home, however, the router is likely to be the way Internet-connected devices link to the outside world.[29]

Data processing in the Internet of Things can take place in a variety of ways ranging from locally, on the device itself, to remotely, with information being sent for processing to centralized servers elsewhere. When machines communicate directly with other machines, a device collects information by means of a sensor. The sensor then uses a radio transmitter to send the data over a network. The network can be either wired or wireless. Wireless networks can be cellular, satellite, Wi-Fi for wide range communication, or Bluetooth, ZigBee and RFID for short range communication.[30] Once the data arrives at its destination, it can be analyzed and acted upon by either another device or a human being.[31]

Market growth forecasts

Market growth forecasts for the Internet of Things are highly optimistic. According to the International Data Corporation's research into 36 use cases in select industries in Canada, those use cases alone will result in an investment of $6.5 billion in 2018.[32] BI Intelligence forecasts that 1.9 billion once-inert everyday and enterprise devices are already connected to the Internet, from parking meters to home thermostats, and by 2018 that number will top 9 billion.[33] ABI Research reports that there are more than 10 billion wirelessly connected devices in the market today; with over 30 billion devices expected by 2020.[34] Cisco Systems is forecasting that there will be 50 billion such devices by 2020, representing a $15 billion market,[35] while Gartner predicts that the total economic value generated through the Internet of Things will be $1.9 trillion dollars by 2020.[36] McKinsey Global Institute reports that The Internet of Things has the potential to create economic impact of $2.7 trillion to $6.2 trillion annually by 2025[37] and that the sales of sensors have grown by 70 percent annually since 2010.[38]
These forecasts depend on a variety of innovations and changes[39]:

- emergence of standardized, small, ultra-low power wireless technologies;
- affordable access to mobile computing;
- the trend of app developers to push intelligence from the app layer to the network layer, or the cloud;
- improvements in machine-to-machine communication;
- the growth of Big Data and analytics, burgeoning health and fitness monitoring using wearable devices[40];
- ever-increasing network capacity at higher speeds and ever-cheaper rates;
- the consumerization of enriched experiences with things; and
- enough addresses for all of the devices to connect, through the implementation of IPv6[41].

However, some significant barriers to implementing the Internet of Things have been identified by industry watchers[42]:

- the cost of sensors and actuators must fall to levels that will spark widespread use;
- interoperability and security standards need to be established for sensors, computers, and actuators[43]; and
- privacy and security concerns must be addressed in a meaningful way.

The following sections provide specific examples of the Internet of Things in the retail and home environments.

2. Special Application in the Retail Sector

The practice of retail analytics continues to evolve. At the time of writing, consumer behaviour can be analyzed automatically, efficiently and unobtrusively. The main enablers of this development are the electronic devices (smart phones, tablets, etc.) that many of us carry when we go shopping. These devices frequently transmit information by means of their radio interfaces (e.g., cellular, Wi-Fi, Bluetooth), often without the knowledge or involvement of the person carrying them. This information is very useful for retailers looking to track and recognize customers as they move about the store environment, and make repeated visits over time.

Retail stores have traditionally used some form of analytics to gather data about customers as they shop. Practices have included in-store observations, review of video analytics, deployment of mystery shoppers, combined with information that a consumer may willingly submit, such as customer satisfaction surveys. With advances in technology, however, the methods have evolved to facilitate analytics from large, automatically collected data sets such as purchase histories, loyalty card information and consumer profiles from data brokers.

Tracking within the Internet of Things can help a business with asset management, inventory control and store layout efficiencies. More detailed information obtained can be used for sophisticated analytics for marketing and profiling of individuals. Tracking of personal mobile devices (such as a smartphone) also provides bricks-and-mortar business establishments with an enhanced means to "know" the customers in their physical stores, similar to what virtual/online operators have through cookies and other technologies. Sophisticated tracking and profiling can occur in a seemingly invisible manner, involve third parties that individuals may not be aware of, and result in a combination of online and offline information such as location patterns (inside a store or across a city), online browsing, purchase history and social media activity. What is important for individuals to be made aware of is the degree to which their movements, location and seemingly normal everyday interactions are monitored as they move in and out of bricks-and-mortar stores.

Consumer devices and "things" that can continuously "talk" to a business can convey information that is of a personal and potentially sensitive nature about an individual. The value for retailers lies in the data that these things emit, and also the interaction between consumers and retailers that can take place using the things. This information can be used in multiple ways to expand analysis on customer behaviour and improve business practices. According to a 2014 Canadian retail study by Deloitte commissioned by the Retail Council of Canada:

The store is no longer just a store, but instead a space where opinions, reviews, social media, mobile, expectations, experience, technology and attitude combine to create connections.[44]

The convergence of technologies is what enables omni-channel operations, and at that core of that is master data. Whether the data pertains to items, customers, or vendors, it needs to be structured, analyzed, and available in order to provide value.[45]

While a retailer may have multiple channels to reach individuals—such as a physical location, an online store, or social media sites—having each of these operate in a silo may not offer consistent prices, deals, and content to customers. The Internet of Things provides a means to generate detailed analytics derived from consumer interaction with all of these channels, and offer consistent promotions and marketing campaigns across these platforms. The combination of online and offline data though, including information from mobile app activity, has the ability to paint a detailed background of where a device has traveled, what stores or locations it frequents, and what online activity it, and the individual behind it, has engaged in.

The detailed level of real time analytics that results from the Internet of Things contributes to its commercial and economic value, but it also raises significant privacy considerations that must be addressed to comply with privacy rules and best practices, and to support consumer trust.

Pointing to the potential privacy implications of the Internet of Things in the retail environment does not mean that, as a concept, it lacks merit. Rather, such attention serves as a means of identifying basic elements of consumer trust that are essential for novel commercial applications to be successful. It also serves to sensitize businesses to the reality that certain data elements in the Internet of Things ecosystem can become personal information even though, on the surface, they may not appear to fit traditional understanding of personal information.

Tracking and Profiling by Retail Establishments

There are a number of technologies that can be used to track and interact with devices in retail environments and they differ in the range of operation and the accuracy of location information. The following chart below is an overview of such technologies:

Technology	Description
Cellular	▪ Cellular radio provides very wide signal coverage, typically at the scale of neighbourhoods. ▪ Devices have unique identifiers that identify them to the telecommunications network.
Wi-Fi	▪ Wi-Fi generally involves medium-range communications, for example within or around a building. ▪ If a device has Wi-Fi turned on, it is always looking for a Wi-Fi network to connect with. ▪ When that device comes in range of a Wi-Fi network that a store (or third-party) has placed in a physical establishment, the Media Access Control (MAC) address, which is a unique number associated to that device, can be captured. ▪ Therefore, if a device is Wi-Fi enabled, observations can be made that reveal which devices are in a store. ▪ Wi-Fi networks can also be located in more public spaces such as streets or malls and can be used to analyze which stores a device is near or often frequents. Information about a device gathered from a number of Wi-Fi networks could offer detailed observations or patterns related to geolocation, date and time.
Bluetooth	▪ Bluetooth generally involves short-range communications at the level of rooms. While Bluetooth's range is smaller than Wi-Fi and it requires less hardware than Wi-Fi tracking, it also uses less bandwidth and can transmit data faster than Wi-Fi.[46] ▪ Similar to Wi-Fi tracking, beacons (which are sensors) can be placed in a store or in public spaces and can gather observations via Bluetooth about a device within or outside of the store. ▪ In order for a business to engage in 2-way communication with a device via Bluetooth, an individual must have undertaken an action, such as downloading a store's app. ▪ Bluetooth Low Energy (BLE) uses Bluetooth connectivity, but it can connect faster and is more energy efficient than Bluetooth. BLE is only active when a connection to a device is made and is therefore optimal for sending small amounts of data periodically.[47] BLE devices can be powered for long periods of time, so devices do not have to be charged for up to a year.[48] ▪ This type of low-energy transmission can be used in equipment, appliances, and fixtures.
Near Field	▪ RFID uses radio signals to transmit information from a tag on a device to a

Communication (NFC) and Radio-Frequency Identification (RFID)	RFID reader.[49] ▪ NFC evolved from RFID to provide a low-power method to transfer small amounts of data between devices. ▪ Both NFC and RFID require close proximity to communicate. ▪ NFC can be used for a number of applications, including receiving coupons or deals by tapping a device at a digital sign/kiosk. It is also used for mobile payments, where an individual with an NFC enabled device can simply tap their device at a merchant's point of sale system to complete a payment transaction.

Retail analytics can be performed from *observations* gathered in a store by devices and sensors placed in or around the environment. With an individual doing nothing more than passing through or near a store, information about their device can be captured for the purposes of tracking or marketing. Additionally, if individuals perform some type of *interaction*, such as downloading an app or connecting to a store's free Wi-Fi, richer information from devices can be obtained. The following are some examples of retail analytics involving passive and interactive modes both in-store and across stores:

	In-store	**Outside of Store**
Passive Observation	▪ Location tracking via short-range radio. ▪ Short-term behaviour analysis. ▪ Video cameras used to analyze customer traffic flows. ▪ Facial detection and analysis to customize digital signs and ads.	▪ Location tracking via medium- and long-range radio. ▪ Neighbourhood-level tracking. ▪ Long-term behaviour analysis.
Active Interaction	▪ Downloading an app to receive coupons when in the store. ▪ Connecting to a "free" Wi-Fi service. ▪ Completing a NFC-enabled transaction (for example, a mobile payment on a smartphone).	▪ Creating a digital perimeter around a store so coupons can be delivered when a potential customer approaches. ▪ When an individual walks by a competitor's store, providing them with a coupon to draw them in to their store instead.

Internet of Things in the Retail Context: Use Cases

This section explores some of the Internet of Things applications that consumers may encounter when they visit local businesses. These examples illustrate how profiling, surveillance and monitoring are key components that add value for marketing, product promotion, customer engagement and consumer experiences.

This section also illustrates how retailers and other businesses can derive insights from the full range of customer behaviour—from walking by a store, to walking through it, to browsing products on a shelf or on a smartphone and eventually making purchases.[50]

A. Passive In-Store Tracking

Organizations can install radio base stations and sensors that can capture the unique identifiers associated with the cellular, Wi-Fi, and Bluetooth features of consumer devices. These identifiers can be used for tracking the sections of a store where the device has been located and what products or goods it has been near. This type of tracking can be done by either the store itself, or by a third-party that is unfamiliar to the individual.

One organization involved in providing such analytic services to stores is Euclid Analytics, which promotes its Wi-Fi tracking products on its website:

> *Because shoppers don't need to actually connect to your Wi-Fi network or install a mobile app, you can measure their activity without interrupting their shopping experience.*[51]
>
> *Using Wi-Fi enables Euclid clients to measure their store visits, shopping time, and repeat visits and pinpoint what marketing and operations practices are most effectively driving revenue.*[52]

Toronto-based Aislelabs[53] provides similar passive Wi-Fi tracking services[54] and states that they provide insights on individuals inside or outside of stores, identification of first time and repeat customers, walking paths and dwell times.[55]

B. Interactive In-Store Tracking

Many stores offer customers the ability to connect to a free Wi-Fi network or interact with Bluetooth stations located in the store. If a consumer has installed and enabled the store's app on a mobile device, they can also receive deals or promotions.

For example, Philips now sells intelligent light bulbs that can be placed in stores to connect to users' smartphones via beacons.[56] By downloading a store's app, light bulbs in the store can send information and deals to an individual's smartphone based on which aisle a device is in, and allow stores to "…keep track of their habits and preferences in-store…"[57]

Information about an individual's device and its movements could be tracked by a store, or third-parties the store partners with, that offers the free Wi-Fi service. This tracking could also involve combining location information with information about online search activity,[58] shopping carts[59] and loyalty programs.[60] Even more information can be gleaned if a social network site authenticator (like a social network account) is used to sign-in to the Wi-Fi services.[61]

Another method of active tracking involves the use of beacons. Beacons are sensors that communicate via Bluetooth to a device that is Bluetooth-enabled. Beacons can be used to track how many times a customer visits a shop and the areas and departments where they spend the most time, thereby determining which displays may be most effective and the number of promotions or vouchers that are redeemed.[62] Beacon services often require an individual to download a mobile app, either the store's own app or one from a third-party.

Shopkick, a company which provides a beacon to retailers called “shopBeacon,”[63] notes on its website:

> *ShopBeacon can welcome a shopper when she enters a store and show her location-specific deals, discounts, recommendations, and rewards, without her having to remember to open the app. It can also tie at-home browsing to in-store benefit—if she “likes” a specific product in the app, shopBeacon can remind her when she enters the store that sells it. It can also deliver department-specific offers throughout the store—so the boots she liked show up at the most useful time—in the Shoe department.*[64]

Media reports have indicated that Canadian retailer Hudson’s Bay began piloting beacon technology in some stores across Canada. According to a statement from the executive vice-president and chief marketing officer for Hudson’s Bay the beacons are “…to detect and interact with shoppers who have downloaded a compatible smartphone app.”[65]

In addition, mannequins in stores can be equipped with Bluetooth to interact with a passerby’s mobile device.[66] With an app, an individual can interact with the mannequin and receive information about the clothes the mannequin is wearing, directed to make a purchase, share information with friends, or receive related offers.[67]

Digital signs in the retail environment are also being used in conjunction with beacons, which allows for devices that have a store’s app to provide “…targeted content to in-store digital signage while simultaneously presenting a tailored offer to the shopper's mobile devices.”[68] These can also be designed to include content based on the habits and preferences of a particular user[69] and purchase history.[70]

Dressing room mirrors or monitors can allow individuals to virtually try on different clothes and compare different outfits, side-by-side. The virtual images are not only used to help an individual with a purchasing decision, but can be shared through social media or other operating channels of the physical store.[71] The founder of MeMomi, which has a product called MemoryMirror, was reported as saying: “Since MemoryMirror ‘remembers’ each customer interaction, it not only allows fashion retailers to provide an exciting in-store, web, and mobile shopping experience, but to collect valuable data on customer behaviors and preferences.”[72]

Mobile payments can also tie-in the whole consumer experience in a store. Take for example a restaurant that combines mobile payments with electronic reservations and ordering. All of these interactions can be tied together, logged, and tracked.[73,74]

C. Tracking Physical Location Anywhere

Consumer activity and location tracking can also take place outside of a store, perhaps in the larger shopping mall, the local neighbourhood, or around the city. If data from multiple participating stores is combined, a more detailed profile of consumer behaviour and travel can be derived. Third-party services are emerging that offer in-store tracking at a number of locations and provide an ability to combine and aggregate the data into more general profiles.

For example, media reports have noted that a company called Turnstyle placed a few hundred sensors in businesses around Toronto and provided their clients with insights as to what other businesses and services their customers frequented, which then allowed those businesses to develop targeted marketing campaigns based on that information.[75] While Turnstyle suggests that the information is not tied to a specific name, it is tied to a hashed MAC address.[76]

Media reports also indicate that this form of tracking by Turnstyle can include *any* device that is Wi-Fi or Bluetooth enabled.[77] Turnstyle provides an opt-out link on their website and requires individuals to enter their device MAC address in order to opt-out.[78] Turnstyle also provides physical businesses with free Wi-Fi for their customers, and if individuals sign in with a social media account, it allows them to "…collect the names, ages, genders, and social media profiles."[79]

Another Toronto-based company, Via Interactive, uses information from cellular carriers to conduct "on the street" tracking. Its website states: "We are data people, we believe in the prospect of uncovering 'invisible' data to help make sense of all of the consuming, driving, walking, running, watching, eating and buying that is going on in the 'real-world'."[80]

Reports suggest that Via Interactive has roughly 50 million pieces of location data to generate location profiles that are combined with data from social networks.[81] It has also been reported that the company can use cellular data to track location to the square meter.[82] Its website notes that its services include aggregated, geo-stamped public posts from social networks, aggregated location and contextual data from wearables and "anonymized" point of sale data. The website also makes claims about "rich, real-time and unbelievably insightful location data."[83]

SkyHooks, a data analytics company, offers a business solution that its website states: "delivers anonymized contextual data on each user's location-based behavior for you to personalize content, create real-time experiences or target advertising."[84] Its website further states that this information can be gleaned as users move throughout their everyday lives, whether they interact with a business's app or not.[85] SkyHooks uses Wi-Fi, cellular and GPS data for its location service offerings.[86]

"Geo-fencing," with respect to mobile marketing, is a term used to describe a device's ability to receive notifications based on a defined area.[87] The practice could involve an individual having downloaded an app and allowing that app to access geolocation data from their device[88] and could even include using other information such as real-time search history.[89] For example, an individual walking by a flower shop could receive an advertisement or coupons for flowers, or if an individual walks by a participating store, it could receive ads for complementary products.[90] Geolocation could even be used to serve ads to sway people from entering competitors' shops.[91]

Geo-fencing could also be used to influence individuals in a particular area given certain environmental factors. A case study from an advertising industry association outlines a geo-location test by Wal-Mart in Canada that was based on not only location, but other factors, such as weather and time.[92]

3. Special Application in the Home

Internet of Things technologies are now being made available to consumers who are willingly bringing these technologies into their homes. “Smart,” Internet-connected devices for use in the home are being touted as providing safety, security and convenience. Smart fridges can prevent food spoilage, saving consumers money; smart meters can control energy consumption; smart home monitoring can ensure security. However, all of these devices come with a privacy cost which may not be immediately apparent to those who choose to use them.

There is considerable – and understandable – enthusiasm for deployment of smart technologies within the home since this is where the Internet of Things can have the most profound impact on our daily lives. The capacity for an array of sensors ensuring our personal security and ensuring our homes operate efficiently is certainly appealing. However, as the Supreme Court of Canada has recognized, “[t]here is no place on earth where persons can have a greater expectation of privacy than within their ‘dwelling-house.’”[93]

Many analysts consider 2014 the year that the connected home came to be: “home automation is not a very new market, but the mass awareness of home automation is relatively new, primarily driven by initiatives from security companies and more recently telecom and cable companies.”[94] A “smart home” is fitted or equipped with a range of interconnected sensors to read external elements such as light, temperature, motion, moisture of systems such as heating, lighting, security; and of devices such as media devices and appliances, which can be automated, monitored and controlled through a computer or smart phone, including from outside the home, or via the Internet. Smart homes can either be the result of integrated design, or the accumulation of interconnected components over time, perhaps in response to changing needs or availability of technology. The intent is to provide the occupants with sophisticated information about the state of their home, and to allow them to control the connected devices.[95]

The European Union Agency for Network and Information Security anticipates three likely patterns in the development of smart home technology:

- a fully decentralized smart home where each device is autonomous and which makes use of the existing home network to the Internet and transmits data to the service provider in the cloud;
- a home with an enabled local connectivity between smart devices, without the use of connection to cloud services and without a central getaway; and
- a home with a central hub where a central software system—and accessible from one central device—coordinates all the smart devices and integrates their services to create added-value.[96]

Current developments display a combination of these three patterns to varying degrees and, while smart homes may still be in their infancy, the market is forecast to grow exponentially within the next five years. The global smart home and buildings market is expected to grow at a compound annual growth rate of 29.5% between 2012 and 2020.[97] Canadian consumers are projected to spend $0.79 billion on smart home systems, devices and software in 2015. As of June 2014, Canadian households had, overall, 63 million Internet connected devices. By the end of 2015, this figure was projected to increase to 86 million.[98]

A number of households already have components of a smart home in operation. It may not be considered as such, and the devices may not be intrinsically and seamlessly connected to their users and to one another, but for the most part, the first stepping stones leading to a home-connected environment are already set. It is also expected that smart appliances will create a significant shift in how consumers acquire, manage, prepare and consume food and analysts forecast a global market growth from $613 million in 2012 to about $35 billion in 2020.

Internet of Things in the Home: Use Cases

A. Smart Meters: connecting homes to the wider grids

Many homes in Canada, are currently equipped with smart electricity meters which can better manage consumption and find efficiencies. Smart meters measure and record consumption times and levels and transmit this information automatically to the power authority. They make it possible to introduce time-of-use pricing to encourage ratepayers to shift their electricity use to times of lower demand[99] and are growing in popularity largely to address the challenges of an aging electrical grid.[100] An added advantage is that billing can be much more accurate when use is measured and transmitted in small increments – usually hourly but sometimes as small as every 10 minutes.

Early versions of smart meters communicated only one way: from the meter to the utility company. Newer models also allow the users to learn about their energy consumption. The Green Button Initiative pilot launched in 2013 in Ontario enables users to share their electricity data with a third party through an app to help them monitor their consumption and find efficiencies.[101] This common data standard is being implemented in other North American jurisdictions.[102] A feature related to smart meters is the utility company installing, with the consent of the user, a device which allows the utility to remotely adjust home energy consumption during peak consumption periods, such as setting a higher thermostat temperature during a heat wave, to ease pressure on the electrical grid.[103]

B. Smart entertainment systems, towards an integrated infotainment structure

A smart TV is any television that can be connected to the Internet to access streaming media services and that can run entertainment apps, such as on-demand video-rental services, Internet music stations or Web browsers. Higher-end models have built-in video cameras, microphones, and voice and gesture recognition. Smart TVs can be inherently smart if they have an internal microprocessor and Internet access capability, or they can be regular TVs made smart by being connected to a set-top box like Roku, Apple TV or Fire TV, which enables Internet access and streaming. In 2013, it was estimated that 25% of Canadian households, a full one in four, already had a smart TV; this number was projected to increase to 40% by 2015.[104] The level of market penetration for these new smart TVs or smart options has accelerated to the point where fewer and fewer “dumb” TVs are even available anymore.

The fact that smart TVs can connect to many other devices wirelessly, such as laptops, wireless keyboards, mice, smartphones and tablets to facilitate text entry, navigation, web browsing and content sharing is considered a major step towards a convergence of computing and entertainment. It also provides the consumer with the capacity to have content literally at the touch of his or her many devices — for instance, seamlessly moving from watching a movie on one device to another, starting from where the user left off, or wirelessly displaying pictures from a smartphone onto the TV screen.

As smart TV interconnectivity continues to develop, a smart TV could potentially take content from any source (TV, movie, podcast, social media), observe consumption and viewing habits and make intelligent recommendations or serve ads based on the analysis of the content being consumed across media and platforms.[105]

C. Home monitoring at the touch of your smartphone

Another smart home technology that is gaining a significant foothold in consumers' homes is security systems. While established home security companies are updating their products, new entrants, such as local telecommunications providers, independent developers and giants such as Google and (soon) Apple,[106] are all leveling the playing field and competing for a share of this growing market.

In years past, surveillance systems were limited to commercial enterprises such as banks, warehouses and airports.[107] As technology evolved and prices dropped, it became feasible to set up a network of real-time, high-definition surveillance cameras in the home to be monitored either by third parties (including security firms and telecommunications companies) or by homeowners themselves by means of smartphone apps. Notwithstanding the selected device or system, they usually provide features such as: smart door locks; garage openers; video cameras; night vision; door and window sensors; and movement, fire and temperature sensors. Security systems can be self-monitored or monitored by a third party—for instance, by a telecommunication or home security company. Self-monitored systems have a two-way communication between the system and the user and the data being collected can also be stored in the cloud. Monitored systems, on the other hand, are installed by a security or telecommunication company and will additionally stream back certain data to the company. Certain companies are teaming up with data analytics providers to offer more tailored advice or solutions to a given user.

In the US, those who opt to install such systems can be rewarded with lower home insurance rates as a reward for minimizing the attractiveness of their home to criminals.[108] This presupposes that it is made overt, either through visible cameras on the exterior of the home, or through promotional lawn signs and window stickers, that a surveillance system is in place. However, small, covert cameras can also be used to monitor people and their activities within or near the home without their knowledge. An obvious example is the so-called "nanny-cam," a small camera typically installed inside a doll, named for monitoring child care providers. Another is the "peep-hole camera," which can photograph anyone who comes within a certain distance, be they visitors, couriers, vandals or thieves. Newer cameras can be motion activated, and set to send an e-mail or text alert to a smartphone upon activation.[109]

D. Smart appliances: chattering electronics

The smart appliance market is still embryonic. With energy efficiency increasingly being an innovation driver, there is a significant focus on having smart appliances connected to the smart meter grid to optimize household energy consumption, so that heavy users of electricity, such as the washer or dryer, could be remotely operated during off-peak hours.[110]

Some smart appliances, such as refrigerators, are equipped with sensors to detect the freshness of food items and then keep users informed by means of text messages to help with food items management and purchasing.[111] Another scenario, which calls for a seamless device integration, suggests for instance that a user watching a cooking show could send information about an interesting recipe to the refrigerator, by means of the smart TV. The refrigerator would log the recipe and verify whether the required groceries are available. If the user had everything that was required to make the dish, the user could remotely connect to the oven to preheat.[112] If not, the refrigerator could also send the list of missing ingredients to an online grocery store.

Yet another technology making its entrance in high-end homes is the digital backsplash. The digital backsplash replaces the traditional backsplash in the kitchen and allows the user to connect to its camera system, display photos and artwork or connect to the Internet through touch screens.[113]

Widespread adoption of smart appliances and kitchens is most likely some years away as appliance choices are limited, prices remain prohibitive for the average consumer and, most importantly, their added value is yet to be well defined and marketed to the consumer.

E. The Smart and "Safe" Home for Independent Living

While home surveillance systems have obvious security uses, aging populations and pressures on health care systems are making surveillance a viable alternative to ensure that people at risk, such as the disabled and elderly, can remain in their homes safely. The concept of "aging in place," that is, growing old in one's home rather than in institutional facilities, is made more feasible notably through home monitoring systems that can connect the elderly with health care services or caregivers electronically;[114] these systems and sensors can monitor behaviour patterns to detect falls, determine if dementia is present or progressing, and track sleep patterns. Given that wait times for assisted living facilities are increasing,[115] there is a growing uptake of monitoring systems in Canada, particularly those which are sensor driven, that may be viewed as less intrusive than camera-based systems.[116]

Connected appliances can be a "potential game-changer for the disabled."[117] Deployment of wireless sensor networks or voice-activated appliances inside the home can perform a variety of functions to afford a measure of independence in daily living. Those with restricted mobility can benefit from controlling appliances, checking who's at the front door and adjusting the thermostat from their smartphones. Sensors worn on the body can interact with environmental sensors in the home to report falls or other mishaps to a caregiver, to activate air conditioning if the core body temperature is over a certain threshold, or remind patients to take certain medications.[118] As the cost for these systems and devices drops, their implementation can be expected to spread.

4. Privacy Implications

As individuals will have their daily activities and behaviours measured, recorded and analyzed, there is a pressing need for developers and policy-makers to turn their minds to informing consumers and citizens as to who collects what kind of personal information, how it is then stored, used and disclosed to whom and for what purposes. Privacy principles dictate that users should be able to keep control of their data as well as to be able to opt out of the "smart" environment without incurring negative consequences. How will this unfold, and will traditional privacy principles be addressed?

Before we too readily endorse smart devices and sensors that can send into the cloud information about many personal aspects of our daily lives, it is essential to have an informed discussion about the implications of the Internet of Things and to plan the integration of privacy principles and safeguards into the conception and implementation of the many smart environment components.

Information collected by sensors within objects that are connected to each other can yield a tremendous amount of data that can be combined, analyzed and acted upon, all potentially without adequate accountability, transparency, security or meaningful consent.

Identifiability of Internet of Things Data

In some instances, device tracking is said to involve aggregate, anonymized, or de-identified information.[119] Broadly speaking, aggregate information can be thought of as "complied or statistical information that is not personally identifiable."[120] Even aggregate information, however, could lead to an identifiable individual, as research has shown.[121] While some have argued that the information at issue in the Internet of Things environment is anonymized or pseudonymized, there are difficulties with anonymizing information in this context.[122] As the Article 29 Working Party has noted, even pseudonymized, or anonymized data, may have to be considered personal information.[123]

While tracking in the Internet of Things involves the tracking of a device, the motivation is to understand the behaviour of the individual behind the device. Indeed, value is derived from the rich information about the individual, their activities, their movements, and their preferences. When inferences are made about the owner of a device, it raises the question whether it is the device being tracked or the individual. A report from the European Commission found that objects in the Internet of Things can become like extensions to the human body and mind with enhancements such as embedded intelligence and knowledge.[124] As well, long-term patterns of location data attributed to a particular device can potentially reveal information about where a device is located at certain times of the day or night, which could potentially identify work or home locations.[125]

In 2013, the U.S.-based Future of Privacy Forum released a code of conduct for Mobile Location Analytics (MLA) Companies that offer consumer tracking analytics to businesses.[126] The code states "MLA Companies shall not collect personal information or unique device information, unless it is promptly de-identified or de-personalized, or unless the consumer has provided affirmative consent."[127] While the code notes that MAC address that are hashed could be considered de-personalized data,[128] the Future of Privacy Forum noted that "… it is important to understand, that Code does **NOT** take the position that hashing MAC addresses amounts to a de-identification process that fully resolves privacy concerns"(bold and uppercase emphasis in original).[129]

Hashing is a process that converts a number into a new unique number, referred to as a "hash value."[130] As the U.S.-based Electronic Frontier Foundation (EFF) has noted, one of the limitations with hashing, is "by definition, hashing the same value always produces the same result."[131] Therefore, hashing a unique number, such as a MAC address, may not necessarily make information truly anonymous, or remove the risk of re-identification, which has been noted in findings from the OPC[132] and technology experts.[133] According to TRUSTe, a privacy trust mark company, in some cases, "the entire reason for keeping the hashed data is to be able to identify a discrete user the next time they return to the site."[134]

There are a number of court decisions that address when information can be about an identifiable individual, and therefore, be considered as personal information. For example, the Federal Court has ruled[135] that information will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information.

More recently, the Supreme Court of Canada has ruled[136] that there is a reasonable expectation of privacy in subscriber information linked to Internet activity, as this information can be the key to unlocking sensitive details about a user's online activities and is worthy of constitutional protection. This decision affirms that it is not enough to look at specific pieces of data in isolation, but rather one must also look at what the data can reveal, including the potentially intimate details about lifestyles and personal choices that can be inferred from the data.[137]

The OPC has demonstrated elsewhere that powerful insights about an individual can be gleaned from information such as IP addresses.[138] Another research paper entitled *Metadata and Privacy - A Technical and Legal Overview*[139] concluded that metadata (data that provides information about other data) can reveal much about an individual and deserves privacy protection, while recognizing that context matters. And, as we saw with the OPC's research on predictive analytics[140], we are witnessing a new generation of privacy challenges arising from the combination of seemingly innocuous and non-sensitive bits of personal information to derive insights into personal behaviour.[141] This work will inform our understanding of the appropriate checks, balances and processes that may be required in the Internet of Things environment.

The question as to what constitutes personal information becomes even more important when there are combinations of online and offline tracking. There are some cases where organizations may advise that they are not collecting personal information such as names and addresses, but they do collect MAC addresses or other identifiers which could be considered personal information depending on the context and what other information is being collected.[142]

Further to this, there are business models in the retail environment that combine and aggregate online and offline information to create customer profiles. While this may be done with aggregate or de-identified information, the amount of detailed information that can be obtained from ubiquitous, always-on devices expands the scope, scale and potential sensitivity of information. Combining location data with offline and online information related to purchase histories and online browsing can potentially reveal a detailed portrait of an individual including sensitive information related to finances, purchases, or interests.

For example, the Wall Street Journal reported on a study by the Massachusetts Institute of Technology (MIT), which used de-identified information from credit card purchases of 1.1 million people, and found it could re-identify the unique purchase habits in 90% of cases by matching activity against other publicly available information on LinkedIn, Facebook, Twitter and Foursquare.[143]

Accountability in the land of machines

Accountability is a key principle in privacy law. To be accountable, an organization needs to be able to demonstrate what it is doing, and what it has done, with personal information and explain why. This may be easier said than done in the Internet of Things environment when there is a multitude of stakeholders, such as device manufacturers, social platforms, third-party applications and others.[144] Some of these players may collect, use or disclose data, and can have a greater or lesser role in its protection at various points, though where to draw the line between them can be challenging at the best of times. For example, who is ultimately responsible for the data which the smart meter broadcasts? The homeowner who benefits from using the device, the manufacturers or power company which provided it, the third-party company storing the data, the data processor who crunches the numbers, all of the above, or some combination thereof? And to whom would a privacy-sensitive consumer complain? Should privacy be breached, where does the responsibility of one party end and another begin? Mapping dynamic data flows and setting out the responsibilities and relationships between various actors could help clarify how information flows among the parties and can help inform the basis of an organization's privacy management program.

In the case of "machine-made" decisions, developers and owners of the underlying algorithms, systems and products may find it even more challenging to demonstrate accountability.[145] In addition to this vexing issue, the legal and ethical responsibilities in the case of errors or accidents are far from clear.[146] The scope of privacy management programs, and the level of accountability organizations are expected to demonstrate, will be complex in the Internet of Things environment.

Transparency and the ethics of data collection

Devices in the Internet of Things may often be designed to operate quietly as part of our environment so that we may never know they are there. As a result, we may have difficulty knowing what information about us is being collected, used and disclosed by devices in a sensor network. It is also likely to be difficult for us to learn about the parties that benefit from the information collected by these devices. While business models for the Internet of Things are in their infancy, industry commentators see opportunity in developing services built around the *data* collected from devices, rather than sales of the devices themselves.

Consider, for example, the issues around transparency of data collection within our homes. Homes are where we spend most of our time when we are not working or at school. They are also the places we consider to be the most private. Yet, the introduction of connected devices is bound to fundamentally alter how we live our private lives. Some of the risks stem from the widespread use of devices and networks with weak security postures. Others relate to the information that is being collected, who will have access to it and for what purposes.

In the retail environment, passive in-store tracking and profiling raises questions as to how individuals are made aware of the purposes of the collection of their personal information, how transparent the information management practices of all the stakeholders involved are, how individuals are notified about such practices, and how these communications are presented to them in order for them to give meaningful consent. Given the use of small portable electronic devices, *how* information is communicated to individuals is also an important consideration.

The Future of Privacy Forum's code on Mobile Location Analytics calls for the use of conspicuous in-store signage to advise individuals of such practices and information for how individuals can choose to participate—or not. It also notes that such signage need not be restricted to just physical signage.[147] Companies shall provide a link to a central industry website that has a central opt-out service and their websites can also provide a link to a company-specific opt-out.[148] Given the passive nature of this type of monitoring, however, it is important that such an opt-out option be made prominent and easy to find. The current industry approach to opt-out requires users to manually enter a complicated URL or a long and complex MAC address, which may not be a simple or easy process for all individuals.

In the United States, the Federal Trade Commission (FTC) undertook action against Nomi Technologies Inc. (Nomi), an organization that places sensors in client's physical establishments to track individuals who entered or passed by those stores.[149] While the FTC noted that Nomi did provide an opt-out option on its website, it did not provide an in-store opt-out or otherwise inform individuals that the tracking was taking place at the stores. The FTC also noted that even though Nomi does hash MAC addresses, the process "…still results in an identifier that is unique to a consumer's mobile device and can be tracked over time."[150] In April 2015 Nomi settled the FTC charges and committed to provide an in-store opt-out and to inform individuals when locations were using Nomi's tracking technologies.[151]

Guidance from the OPC has noted that while there are challenges to the consent model in an age of ubiquitous computing and mobile devices, "more needs to be done to show users, in a creative and meaningful way, what is actually happening with their personal information."[152]

He said, she said, "it" said: access and correction rights

Access and correction rights are squarely related to accountability and transparency. How will an individual know to ask for their information and challenge its accuracy, if they never become aware that it was ever collected? Similarly, how will individuals determine what organization they should seek out to gain access to and, where necessary, correct their personal information?

Canada's privacy laws in both the public and private sectors are heavily reliant on the complaint process as a mechanism for helping individuals challenge organizational decisions made about them. This model works well when there is an obvious organization to contact or a list of information banks,[153] but breaks down when the collecting organization is difficult to pinpoint. What would be an effective way to map dynamic data flows and make them explicit and transparent for all to see so that individuals could more meaningfully exercise their access and correction rights?

Challenges to the existing consent model

Data collection by devices in the Internet of Things context may often be invisible to us and, because we may not be aware, we are unlikely to be in a position to understand it or weigh in on the manner in which it is done. This has obvious implications for achieving meaningful consent.

Binary, one-time consent and traditional definitions of personal information are increasingly perceived as outdated because they reflect a decision at a moment in time in the past, under specific circumstances and are tied to the original context for the decision. Simplistic, "on/off" personal data management policies may be neither flexible, nor appropriate, in the fast-developing online environment.[154]

The OPC has identified challenges with the consent model as an issue under its Economics of Privacy priority and has adopted a strategy to identify, explore and validate enhancements to the consent model so that concerns raised both by individuals and organizations are addressed.

There are many interesting options to deal with the challenges of consent in the Internet of Things environment. Many of these, such as setting machine-based rules for proxy-decision making[155] or having a device "learn" what actions are acceptable (or not) to users at certain times and places,[156] will be considered in the OPC's future work on consent.

D. Information collection, use and disclosure within the home

Smart home devices can also be very telling about the number of people who live in a home, details about their daily habits as well as changes in their routines. In the case of smart meters, there is concern that widespread deployment has focused on energy conservation at the expense of privacy. In the absence of a framework clearly providing choice and control to the consumer and establishing strict collection, use and disclosure rules, the information revealed could be used for data mining, insurance claims or litigation purposes, to name a few potential secondary uses. The Information and Privacy Commissioner for British Columbia and the Office of the Information and Privacy Commissioner of Ontario have issued reports which discuss the privacy issues of smart meters in some detail.

As for smart appliances, home entertainment and surveillance systems, a number of privacy issues are already emerging from the early adopter experience. When connected to the smart meter and grid, smart appliances will provide even more granular information about the identity of the individuals using them, the usage of specific appliances, entertainment habits and presence or absence of people in the home. Smart home devices and their related apps also relay information back to their manufacturers and it is not entirely clear how manufacturers intend to use it and with whom it may be shared. In the case of voice activated devices, if set in "activation mode," they could transmit users conversations to manufacturers. If information is sent via smartphones, Internet service providers will have access to data, which could be shared with law enforcement through lawful access requests. Finally, it should be noted that as smart devices and appliances become more and more normalized, there is an increasing "erosion of choice" for individuals who would have preferred their "non-smart" versions.

Hacking the Internet of Things

As consumers and organizations begin to use Internet-enabled devices and sensors, more and more points are open to attack. An attack on one of these interconnected devices could provide an opportunity for a hacker to not only gain control of a device, but leverage it as a gateway to gain access to all kinds of personal information. It is not just databases that need to be safeguarded, but the Internet-enabled devices like the sensors, light bulbs, video cameras and Wi-Fi routers that facilitate these communications.

Given this, the Internet of Things is likely to require a new security model. The limitations on power, computing capacity and other factors, will require significant changes in the way that these devices are protected, as traditional concepts of firewalls and anti-malware are unlikely to translate well to their capabilities. Routers are becoming an attractive target for hackers in that they are generally always on and they can contain outdated software that may be difficult to upgrade or patch.[157] Every connected device is a potential security weakness that could attack or co-opt other devices connected to it[158] and, as well, many of the connected devices may not be capable of strong encryption because they lack both the necessary computing and battery power.[159] As the common metaphor goes, a chain is only as strong as its weakest link.

How can we trust a device without knowing whether it has been tampered with? An innovative attack method may deprive sensors or devices of power.[160] A compromised device can put the individual's personal information and reputation at risk. It can also compromise their health or even their life if, for example, someone instructs a medical device to deliver an overdose of medication to a patient.[161] Although work is being done to ensure the various parties in the Internet of Things ecosystem implement security measures proportional to the risks posed by these devices,[162] reliable and robust protections need to be built in if we are to develop a secure Internet of Things ecosystem.

Many smart home devices lack secure design or implementation. This may be the result of developers' lack of experience with security, of wanting to keep costs low so as to ensure affordability or the inherent limits of miniaturized devices.[163] A 2014 HP study reveals that about 70% of Internet of Things devices, including sensors and connected infrastructure, have vulnerabilities that could be exploited. These devices included TVs, webcams, thermostats, remote power outlets, sprinklers, door locks, home alarms, scales and garage openers. Among the key findings: 80% of devices, including cloud and mobile apps, failed to require strong passwords, 70% of devices did not encrypt communications, 60% lacked encryption for software updates and another 60% had insecure web interfaces.[164]

A follow-up study released in February 2015 looked at 10 of the newest home security systems. It revealed that none of the systems required strong passwords and that only one asked for two-factor authentication.[165] Of the seven systems with cameras, four gave access to additional users. Most systems also lacked the ability to lock out accounts after a certain number of failed attempts. Other issues included weaknesses in the encryption configuration, making these systems vulnerable to unauthorized access.[166]

Concerns about the use of Internet connected cameras came to light when a website began livestreaming footage from unsecured web cameras around the world. In November 2014, our Office, together with several other Data Protection Commissioners in Canada and around the world, wrote to the website operator and subsequently to several webcam makers to highlight concerns related to Internet-connected cameras and urge them to ensure that appropriate security measures are in place to protect their customers' privacy.[167]

An attacker could use vulnerabilities such as weak passwords, insecure password recovery mechanisms and poorly protected credentials to gain access to a system. These issues can all lead to account "harvesting," where an attacker could determine login credentials and gain access to the overall system. The addition of accounts using weak passwords with access to video cameras could provide an attacker a gateway to identifying an account to use for access to the rest of the system and ultimately to the home. Furthermore, the increasing popularity of wearable devices that track mood, physical fitness and health status, presents new privacy and security challenges, which are discussed in more detail in a separate paper.[168]

Conclusion

Sensors and actuators that are always on, and always interacting with the user's body, and other devices in the user's environment, will make it more difficult for individuals to maintain distinctions between different spheres of their lives. There will also need to be real world accountability for the results of decisions that so-called smart machines make about us.

As individuals' activities and behaviours are measured, recorded and analyzed, there is a pressing need for developers and policy-makers to turn their minds to informing consumers and citizens as to who collects what kind of personal information, how it is then stored, used and disclosed to whom and for what purposes.

If transparency with respect to tracking by devices in the world of the Internet of Things is significant for our relationship with the private sector, it is equally important in our relationship with government. It should not be surprising that the richness of information gleaned from the Internet of Things collected for commercial purposes might attract the interest of law enforcement agencies and governments.

Technological development in the context of the Internet of Things has not been matched by an equivalent evolution of overarching privacy governance models. Not much consideration has been given as of yet to the many privacy implications of having an extraordinary amount of data points that could be collected, aggregated across devices and analyzed not only by the device owners, but also by other third parties unknown to the individual.

One key challenge is that, as these technologies become ubiquitous, we may have little or no warning or awareness that they are even in place;[169] they simply become part of the backdrop of our daily lives. How, then, can citizens who may or may not want to use this technology ensure that someone is held accountable for its use? How will they be able to challenge how the information is used, and how will they be able to give any kind of meaningful consent?

The full impact of the Internet of Things for our privacy may become more evident when its capabilities are combined with other innovations shaping our world today that track not only our activities, movements, behaviours and preferences, but our emotions and our thoughts.

Notes

[1] Digital Life in 2025, Pew Research Internet Project, March 11, 2014. Retrieved: May 12, 2015.
[2] Eric Savitz, "How The Internet Of Things Will Change Almost Everything," *Forbes*, December 17, 2012, Retrieved: May 12, 2015.
[3] See the Pew Research Internet Project, Digital Life in 2025, March 11, 2014. Retrieved: May 12, 2015.
[4] For example, the European Commission has posted the results of public consultations and output of working groups on the Internet of Things, February 2013. Retrieved: May 12, 2015.
[5] See the US Federal Trade Commission Staff Report, Internet of Things: Privacy and Security in a Connected World, January 2015. Retrieved: May 12, 2015.
[6] For example, the IPSO Alliance and ZigBee Alliance.
[7] Opinion 8/2014 on the on [sic] Recent Developments on the Internet of Things. 14/EN WP 223. Article 29 Data Protection Working Party, September 16, 2014. (This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.)
[8] Mauritius Declaration on the Internet of Things. 36th International Conference of Data Protection and Privacy Commissioners, October 2014. Retrieved: May 12, 2015.
[9] Comments of The Electronic Privacy Information Center to the Federal Trade Commission On the Privacy and Security Implications of the Internet of Things, June 1, 2013. Retrieved: May 12, 2015.
[10] Office of the Privacy Commissioner of Canada. "Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps." October 2012.
[11] Wearable Computing - Challenges and opportunities for privacy protection. OPC Research report, January 2014.
[12] See the European Research Cluster on the Internet of Things web site.
[13] See, for example, the Internet of Things: From Research and Innovation to Market Deployment report of the European Research Cluster on the Internet of Things (IERC), 2014. Retrieved: May 12, 2015.
[14] Jeremy Crump, "Time for debate about the societal impact of the Internet of Things," The Policy and Internet Blog, University of Oxford, April 22, 2013. Retrieved: May 12, 2015.
[15] Hakima, Chaochi. (ed.) *The Internet of Things: Connecting Objects to the Web*, 2010, p.252.
[16] "Finding the Best Lost-Item Trackers: Tile, TrackR and Duet Reviewed: Thanks to New Bluetooth Tags, Your Keys, Wallet and Purse Should Never Go Missing Again." *Wall Street Journal Online*, June 17, 2014, Retrieved: May 12, 2015.
[17] See PetHub.
[18] See BuddyTag.
[19] See OPC's fact sheet on RFID, our consultation paper *Radio Frequency Identification (RFID) in the Workplace: Recommendations for Good Practices* (2008) and the consultation results.
[20] For more detail, see Hakima, Chaochi. (ed.) *The Internet of Things: Connecting Objects to the Web*. Wiley-ISTE, 2010, p.18: mechanical (e.g. position, force, pressure, etc), thermal (e.g. temperature), electrostatic or magnetic fields, radiation (e.g. electromagnetic, nuclear), chemical (e.g. humidity, ion, gas concentration), biological (e.g toxicity), military (enemy tracking or battlefield surveillance).
[21] Jamie Carter, "What is NFC? Everything you need to know" *Tech Radar*, January 16, 2013. Retrieved: May 12, 2015.
[22] For more detail, see Alain Louchez, "The Internet of things — Machines, businesses, people, everything." *ITU News*, No. 6, 2013. Retrieved: May 12, 2015.

[23] For more detail, see Hakima, Chaochi. (ed.) *The Internet of Things: Connecting Objects to the Web*. Wiley-ISTE, 2010, p.18.: mechanical (e.g. position, force, pressure, etc.), thermal (e.g. temperature), electrostatic or magnetic fields, radiation (e.g. electromagnetic, nuclear), chemical (e.g. humidity, ion, gas concentration), biological (e.g. toxicity), military (enemy tracking or battlefield surveillance).

[24] Ángel Asensio, Álvaro Marco, Rubén Blasco, and Roberto Casas. Protocol and Architecture to Bring Things into Internet of Things, *International Journal of Distributed Sensor Networks*, 13 April 2014. Retrieved: May 12, 2015.

[25] Melanie Swan, Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0. *Journal of Sensors and Actuator Networks*, 2012, 1(3), 217-253. Retrieved: May 12, 2015.

[26] See, for example, the International Telecommunication Union, ITU Internet Report: The Internet of Things, 2005. Retrieved: May 12, 2015.

[27] Some recent published resources for further reading on the technology, history and Internet of Things: see "Machine-to-Machine Communications: Connecting Billions of Devices," *OECD Digital Economy Papers*, No. 192, OECD (2012), D. Uckelmann et al. (eds.), "An Architectural Approach Towards the Future Internet of Things," *Architecting the Internet of Things*, 2011 and Hakima, Chaochi. (ed.) *The Internet of Things: Connecting Objects to the Web*, 2010.

[28] For some visual representations of different network configurations see National Institute of Standards and Technology Catalogue of Network Connectivity Models, 2001.

[29] Seth Rosenblatt, "'Internet of Things,' not privacy, to dominate at Black Hat." *CNet*, August 6, 2014, Retrieved: May 12, 2015.

[30] Daniel Kellmereit and Daniel Obodovski, *The Silent Intelligence: The Internet of Things*. 2013, pp.30-31.

[31] For the quotation in the adjacent text box, see Michelle Finneran Dennedy, Jonathan Fox, Thomas R. Finneran. The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value. 2014. Retrieved on April 4, 2015.

[32] "New IDC Research Forecasts Canadian Spending on Internet of Things to be Largest in Manufacturing, Healthcare and Transportation Industries," International Data Corporation Press release: April 23, 2015. Retrieved: May 12, 2015.

[33] Emily Alder, "The 'Internet Of Things' Will Soon Be A Truly Huge Market, Dwarfing All Other Consumer Electronics Categories," *Business Insider*, July 17, 2014. Retrieved: May 12, 2015.

[34] "More Than 30 Billion Devices Will Wirelessly Connect to the Internet of Everything in 2020," ABI Research, May 9, 2013. Retrieved: May 12, 2015.

[35] "Privacy integral to future of the Internet of Things," *USA Today*, July 11, 2014. Retrieved: May 12, 2015.

[36] "Gartner Says It's the Beginning of a New Era: The Digital Industrial Economy," Gartner Press release, October 7, 2013. Retrieved: May 12, 2015.

[37] James Manyika, Michael Chui, Jacques Bughin, Richard Dobbs, Peter Bisson, Alex Marrs. "Disruptive technologies: Advances that will transform life, business, and the global economy."p.51, McKinsey Global Institute. May 2013. Retrieved: May 12, 2015.

[38] James Manyika, Michael Chui, Jacques Bughin, Richard Dobbs, Peter Bisson, Alex Marrs. "Disruptive technologies: Advances that will transform life, business, and the global economy."p.53. McKinsey Global Institute. May 2013. Retrieved on May 12, 2015.

[39] See, for example: Thomas Ohnemus, "The Internet Of Things: Enabler Of The Fourth Industrial Revolution," SAP guest blog post, May 21, 2014. Retrieved: May 12, 2015.

[40] Lou Frenzel, "The Connected World Awaits," *Electronic Design*, March 10, 2014. Retrieved: May 12, 2015.

[41] See *Network World* reference of Irish Telecom's Infographic comparing IPv6 and IPv4. October 7, 2014. Retrieved: May 12, 2015.

[42] "Gartner Says the Internet of Things Will Transform the Data Center," Gartner Inc., March 18, 2014. Retrieved: May 12, 2015.

[43] See, for example, the agenda and list of multi-disciplinary selection of expert participants at the ITU workshop, "Internet of Things: Trends and challenges in standardization," held in Geneva, 18 February 2014. Retrieved: May 12, 2015.

[44] Deloitte and the Retail Council of Canada, "Omni-channel: Rethink, reshape, and revalue." Retail Study 2014, pg. 12.

[45] Deloitte and the Retail Council of Canada, "Omni-channel: Rethink, reshape, and revalue." Retail Study 2014, pg. 16.

[46]ProximitySky - Wi-Fi vs. Bluetooth webpage.

[47] LinkLabs - Bluetooth Vs. Bluetooth Low Energy: What's The Difference?, November 1, 2015.

[48] Bluetooth – Bluetooth Low Energy (also called Bluetooth Smart), November 1, 2015.

[49] Office of the Privacy Commissioner of Canada, "RFID Technology."

[50] For additional information, please refer to The Office of the Privacy Commissioner of Canada's "Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing."

[51] Euclid Analytics webpage.

[52] Euclid Analytics blog post "Why Wi-Fi is the right approach for retail analytics." July 23rd, 2014.

[53] Darrell Etherington, "Aislelabs Raises $1.5M To Bring Full Cycle Visitor Analytics To Brick-And-Mortar Retail." TechCrunch, March 19th 2014.

[54] Chantal Tode, "Location tracking opt-out could land big blow to retail technology." *Mobile Marketer*, February 19th 2014.

[55] Aislelabs AisleFlow webpage, "Cloud based in-store analytics to understand the behavior of your customers" *AislelabsFlow*.

[56] Jacob Kastrenakes, "Philips takes on Apple's iBeacon with lights that send deals to your smartphone" *The Verge*, February 27th 2014.

[57] Phillips – Lighting systems for retail & hospitality webpage.

[58] Nestor E. Arellano, "New Fortinet solution offers retail analytics." IT World Canada, January 13, 2014.

[59] Retail Technology, "Modern retailing and omnichannel challenge." August 14th 2014.

[60] Cisco, "Wi-Fi: New Business Models Create Real Value for Service Providers." June 1st 2013, pg. 8.

[61] Lee Badman, "Social WiFi Sign-In: Benefits With A Dark Side." *Information Week*, May 7th 2014.

[62] Steven Skinner, "Beacon technology offers plenty of opportunities for retailers." *The Guardian*, September 4th 2014.

[63] Shopkick webpage -what is shopBeacon™?

[64] Shopkick webpage -what is shopBeacon™?

[65] Armina Ligaya, "Hudson's Bay keeps closer tabs on shoppers with new in-store mobile marketing." *Financial Post*, July 28th 2014.

[66] Claire Swedberg, "Iconeme Launches Bluetooth Beacon Solution for Mannequins." *RFID Journal*, April 21st 2014.

[67] Iconeme – "How it Works" webpage.

[68] DigitalSignageToday, “Digital signage leveraging beacon tech to boost shopper loyalty.” January 7th, 2015.
[69] intel, “Intelligent Mobile Advertising Solution Delivers Targeted Messages.” pg.2.
[70]Ms Smith, “Digital Signage: Privacy in a 'One-Way Mirror Society.'” *NetworkWorld*, February 15th, 2011.
[71] Ally Orlando, “Digital Mirrors Could Create Virtual Fitting Rooms In Retail Stores.” *Integrated Solutions For Retailers*, May 13th 2014.
[72]Ally Orlando, “Digital Mirrors Could Create Virtual Fitting Rooms In Retail Stores.” *Integrated Solutions For Retailers*, May 13th 2014.
[73] Mike Elgan, “How apps are changing fast food.” *Computerworld*, February 15th 2014.
[74]Natalie Gagliordi, “Internet of Things, Big Data fuels latest batch of POS tech.” *ZDNet*, May 19th 2014.
[75] Shane Dingman, “Why your smartphone is telling this Toronto tech firm all about you.” *The Globe and Mail*, January 14th 2014.
[76] Armina Ligaya, “‘It’s creepy': Location based marketing is following you, whether you like it or not.” *Financial Post*, February 1st, 2014.
[77] Armina Ligaya, “‘It’s creepy': Location based marketing is following you, whether you like it or not.” *Financial Post*, February 1st, 2014; and Elizabeth Dwoskin, “What Secrets Your Phone Is Sharing About You.” *The Wall Street Journal*, January 13th 2014.
[78]Turnstyle – Privacy webpage.
[79] Elizabeth Dwoskin, “What Secrets Your Phone Is Sharing About You.” *The Wall Street Journal*, January 13th 2014.
[80] Via Informatics homepage.
[81] Ivor Tossell, “Using 'remarkable' source of data, startup builds rich customer profiles.” *The Globe and Mail*, January 6th 2014.
[82] Elizabeth Dwoskin, “What Secrets Your Phone Is Sharing About You.” *The Wall Street Journal*, January 13th 2014.
[83] Via Informatics homepage.
[84] Skyhook – Personas webpage.
[85] Skyhook – Personas webpage.
[86] Skyhook – Homepage.
[87] Mobile Marketing Association, “Mobile Location Based Services Marketing Whitepaper.” October 2011, pg. 19.
[88] Lauren Brousell, “5 Things You Need to Know About Geofencing.” *CIO Magazine*, August 28th 2013.
[89] Interactive Advertising Bureau, *“*Mobile Location Use Cases and Case Studies.” March 2014, pg. 18.
[90] Lauren Brousell, “5 Things You Need to Know About Geofencing.” *CIO Magazine*, August 28th 2013.
[91] Benjamin Spiegel, “Geo-Location, Geo-Fencing & Creep Factor: The Future of Location Data and Mobile Advertising.” *ClickZ*, October 11th 2013.
[92] Interactive Advertising Bureau, “Mobile Location Use Cases and Case Studies.” March 2014, pgs. 14-16.
[93] Cory J. in *R* v. *Silveira*, [1995] 2 SCR 297, 1995 CanLII 89 (SCC).
[94] Adarsh Krishnan, Research senior analyst with ABI, a technology market intelligence company, quoted by Morgan Brennan, “House of the Future: How Automation Tech Is Transforming The Home,” *Forbes Magazine*, October 10, 2013, Retrieved: April 1, 2015.
[95] ENISA, “Threat Landscape and Good Practice Guide for Smart Home and Converged Media,” p.5, December 1, 2014, Retrieved: April 1, 2015.

[96] ENISA, "Threat Landscape and Good Practice Guide for Smart Home and Converged Media," p.5-6, December 1, 2014, Retrieved: April 1, 2015.
[97] Mellissa Tolentino, "Smart Home market to boom in 2020 : New trends in smart elevators + smoke detectors," *Silicon Angle Blog*, January 27, 2014, Retrieved: April 1, 2015.
[98] ETS Insights, "U.K. and Canada Smart Home Market Brief," June 18, 2014, Retrieved: April 1, 2015.
[99] 2014 Report of the Office of the Auditor General of Ontario, p.362, Retrieved: April 1, 2015. The Report also concludes that estimated benefits related to smart meter implementation were higher than those of the actual current results.
[100] More information is available from Hydro One's Smart Meter site, Retrieved: April 2015.
[101] "Ontario's Green Button: Providing You with Access to Your Energy Data," Retrieved: April 1, 2015.
[102] "Green Button: Helping You Find and Use Your Energy Data," Retrieved April 1, 2015.
[103] "Save on Energy," Retrieved: April 1, 2015.
[104] "Connected TVs Reach One in Four Homes," eMarketer, January 3, 2013, Retrieved: April 1, 2015.
[105] Dan Shust, Vice President of the RI Lab at Resource Interactive, quoted by Jay Donovan in "Smart TVs: How Do They Work?," *TechCrunch*, January 13, 2012, Retrieved: April 2, 2015.
[106] Google and Apple are both positioning themselves to be key leaders in smart home security; Google is acquiring startups such as Nest, a smart thermostat and Dropcom, a closed circuit camera developer so as to combine the two devices. Apple has launched HomeKit, a software framework that can be used by app and hardware developers for communicating with and controlling connected accessories in a user's home. For more details, see "Smart homes: 'My home, my comfort', say readers," Open Roboethics Initiative, October 28, 2014, Retrieved: April 2, 2015.
[107] Rick Delgado, "From Edison to Internet: A History of Video Surveillance," August 14, 2013, Retrieved: April 2, 2015.
[108] Richard Davis, "How surveillance systems save money on insurance," January 24, 2014, Retrieved: April 2, 2015. While it is unclear whether this is currently the case in Canada, it is highly likely Canadian Insurance companies will be following suite. See also the Financial Services Commission of Ontario's Fact Sheet on Home Insurance Tips, Retrieved: April 2, 2015.
[109] This capacity is increasingly available in many cameras including Vue Zone, Belkin's netcams, and others.
[110] Smart from Sunrise to Sunset: A Primer on Ontario's Evolving Electricity Grid, Environmental Commissioner of Ontario, October 15, 2014. Retrieved: January 21, 2015.
[111] Megan Wollerton, "Smart appliances, connected homes at CES 2014," *CNET*, January 10, 2014, Retrieved: April 1, 2015 and "Out of Milk? LG's New Smart Fridge Will Let You Know," *NBC News*, May 7, 2014, Retrieved: May 12, 2015.
[112] Yohana Desta, "Why You're Not Seeing More Smart Home Appliances," April 26, 2014, Retrieved: April 1, 2015.
[113] Morgan Brennan, "House Of The Future: How Automation Tech Is Transforming The Home," October 10, 2013, retrieved April 1, 2015. View these related images.
[114] Alison Marie Kenner, "Securing the Elderly Body: Dementia, Surveillance, and the Politics of 'Aging in Place'," in Vol. 5, No 3 (2008), *Surveillance and Society*, Queen's University, Kingston, Ontario, Retrieved: April 2, 2015. Smart home monitoring is an element of the "aging in place" initiative.
[115] Canadian Association of Retired Persons, "Nursing Home Woes," June 2011, Retrieved: April 2, 2015.
[116] Victoria Stunt, "Use of surveillance tech to monitor seniors at home on rise," March 9, 2014, Retrieved: April 2, 2015.

[117] Shalene Gupta, "For the disabled, smart homes are home sweet home,"*Fortune Magazine*, February 1, 2015, Retrieved April 29, 2015.

[118] Basma M. Mohammad El-Basioni, Sherine Mohamed Abd El-Kader, and Hussein S. Eissa, "Independent Living for Persons with Disabilities and Elderly People Using Smart Home Technology," *International Journal of Application or Innovation in Engineering and Management*, April 2014, Retrieved: April 29, 2015.

[119] Future of Privacy Forum, "The Future of Privacy Forum Announces New Group to Develop Best Practices for Retail Location Analytics Companies." July 16, 2013.

[120] International Association of Privacy Professionals Information Privacy Certification – Glossary of Common Privacy Terminology.

[121] Tech@FTC, "Is aggregate data always private?" May 21st 2012.

[122] Article 29 Data Protection Working Party, "Opinion 8/2014 on the on Recent Developments on the Internet of Things." September 16th 2014, pg.11.

[123] Article 29 Data Protection Working Party, "Opinion 8/2014 on the on Recent Developments on the Internet of Things." September 16th 2014, pg.8.

[124] Ângela Guimarães Pereira, Alice Benessia, Paula Curvelo, "Agency in the Internet of Things." Joint Research Centre – Institute for the Protection and Security of the Citizen; European Commission. 2013, p.9.

[125]Article 29 Data Protection Working Party, "Opinion 13/2011 on Geolocation services on smart mobile devices." May 16th 2011, p.6.

[126] Future of Privacy Forum, "Mobile Location Analytics Code of Conduct." October 22nd 2013.

[127] Future of Privacy Forum, "Mobile Location Analytics Code of Conduct." October 22nd 2013, pg. 3.

[128] Future of Privacy Forum, "Mobile Location Analytics Code of Conduct." October 22nd 2013 pg. 6.

[129] Future of Privacy Forum, "MAC address and de-identification." March 27th 2014.

[130] Office of the Privacy Commissioner of Canada, "Leading by Example: Key Developments in the First Seven Years of the Personal Information Protection and Electronic Documents Act (PIPEDA)." May 23rd 2008, pg. 28.

[131] Electronic Frontier Foundation, "Mobile Tracking Code of Conduct Falls Short of Protecting Consumers." October 26th 2013.

[132] Office of the Privacy Commissioner of Canada. PIPEDA Report of Findings #2013-001.

[133]Ed Felten,"Does Hashing Make Data "Anonymous"?" *Tech@FTC Blog,* April 22nd 2012.

[134] Truste Blog, "Data Anonymization." April 16th 2013.

[135] Gordon v. Canada (Health), 2008 FC 258 (CanLII), Retrieved: May 12, 2015.

[136] The Privacy Commissioner of Canada issued the following statement regarding the Supreme Court of Canada's decision in R. v. Spencer, June 13, 2014.

[137] Speech by Patricia Kosseim, Senior General Counsel, Office of the Privacy Commissioner of Canada, Should we Adopt a Digital Bill of Rights? Remarks at the Canadian Bar Association Legal Conference. August 15, 2014.

[138] What an IP Address Can Reveal About You: A report prepared by the Technology Analysis Branch of the Office of the Privacy Commissioner of Canada. May 2013.

[139] Metadata and Privacy: A Technical and Legal Overview. Office of the Privacy Commissioner of Canada. October 2014.

[140] The Age of Predictive Analytics: From Patterns to Predictions, A report prepared by the Research Group at the Office of the Privacy Commissioner of Canada, August 2012.

[141] Comments of The Electronic Privacy Information Center to the Federal Trade Commission On the Privacy and Security Implications of the Internet of Things, June 1, 2013. Retrieved: May 12, 2015.
[142] The Office of the Privacy Commissioner of Canada. PIPEDA Report of Findings #2013-017.
[143] Robert Lee Hotz, "Metadata Can Expose Person's Identity Even Without Name." *The Wall Street Journal*, January 29th 2015.
[144] In its opinion on the Internet of Things, the Article 29 Working Party made recommendations in this area by setting out some specific responsibilities for these stakeholders. Opinion 8/2014 on the on Recent Developments on the Internet of Things. 14/EN WP 223. Article 29 Data Protection Working Party, September 16, 2014. Retrieved: May 12, 2015.
[145] See, for example, the Electronic Privacy Information Center's resources on "algorithmic transparency."Retrieved: July 15, 2015 and See Getting Accountability Right with a Privacy Management Program, joint guidance developed by The Office of the Privacy Commissioner of Canada (OPC), and the Offices of the Information and Privacy Commissioners (OIPCs) of Alberta and British Columbia. April 2012.
[146] See, for example, David S. Kemp, "Autonomous Cars and Surgical Robots: A Discussion of Ethical and Legal Responsibility," *Verdict*, November 19, 2012 and James Manyika, Michael Chui, Jacques Bughin, Richard Dobbs, Peter Bisson, Alex Marrs. "Disruptive technologies: Advances that will transform life, business, and the global economy." McKinsey Global Institute, p.59. May 2013. Retrieved: April 14, 2015.
[147] Future of Privacy Forum, "Mobile Location Analytics Code of Conduct." October 22nd 2013, pgs. 1-2.
[148] Future of Privacy Forum, "Mobile Location Analytics Code of Conduct." October 22nd 2013.
[149] Federal Trade Commission Press Release, "Retail Tracking Firm Settles FTC Charges it Misled Consumers About Opt Out Choices." April 23, 2015.
[150] Federal Trade Commission Press Release, "Retail Tracking Firm Settles FTC Charges it Misled Consumers About Opt Out Choices." April 23, 2015.
[151] Federal Trade Commission Press Release, "Retail Tracking Firm Settles FTC Charges it Misled Consumers About Opt Out Choices." April 23, 2015.
[152] Office of the Privacy Commissioner of Canada, "Wearable Computing - Challenges and opportunities for privacy protection." January 2015.
[153] Government of Canada List of Personal Information Banks Info Source. Retrieved on April 13, 2015.
[154] Personal Data Management: The User's Perspective. *International Institute of Communications*. November 22, 2012, p.9.
[155] If machines can learn and enforce the automated rules we set about what sharing we feel is appropriate in a particular circumstance, place and time – and then turn off the tap – this has potential to enhance privacy. See Jared Allen, Quang Duong, Craig Thompson, "Natural Language Service for Controlling Robots and Other Agents," KIMAS 2005, April 18-21, 2005, Retrieved: May 12, 2015.
[156] Gestural Interfaces: Controlling Computers with our Bodies, *MIT Technology Review*, May/June 2011. Retrieved: May 12, 2015.
[157] Bruce Schneier, "The Internet of Things Is Wildly Insecure—And Often Unpatchable," *Wired*, January 6, 2014, Retrieved April 14, 2015.
[158] Stacey Higginbotham, "The internet of things needs a new security model. Which one will win?" Gigaom, January 22, 2014, Retrieved: May 12, 2015.
[159] Wade Trappe, Richard Howard, Robert S. Moore, "Low-Energy Security: Limits and Opportunities in the Internet of Things", *IEEE Security & Privacy*, vol.13, no. 1, pp. 14-21, Jan.-Feb. 2015.

[160] Earl Perkins (Gartner Research VP), Securing The Internet of Things– Some Not-So-Obvious Concerns, January 20, 2014, Retrieved: May 12, 2015.

[161] Possible cybersecurity flaws in medical devices probed. CBC News, October 22, 2014. Retrieved: May 12, 2015.

[162] See, for example, recommendations on "security by design" in Opening Remarks of FTC Chairwoman Edith Ramirez, "Privacy and the IoT: Navigating Policy Issues," International Consumer Electronics Show, January 6, 2015, Retrieved: April 14, 2015.

[163] *Supra*, note 4, pp. 17-18.

[164] "Internet of things big security worry, says HP," Larry Dignan, *ZDNet*, July 29, 204, Retrieved: April 2, 2015.

[165] Two-factor authentication is a security process in which the user provides two means of identification, one of which is typically a physical token, such as a card, and the other of which is typically something memorized, such as a security code. The two factors involved are sometimes spoken of as *something you have* and *something you know*. See TechTarget, Retrieved: June 29, 2015.

[166] "HP Study Finds Alarming Vulnerabilities with Internet of Things (IoT) Home Security Systems," February 10, 2015, Retrieved: April 2, 2015.

[167] These letters are available on the OPC website: Letter to 10 webcam manufacturers in Canada and the United States and Letter to operators of webcam website.

[168] Office of the Privacy Commissioner of Canada, "Wearable Computing - Challenges and opportunities for privacy protection," published January 2014.

[169] Chris Baraniuk, "Surveillance: The hidden ways you're tracked," BBC. October 27, 2014, Retrieved: April 2, 2015.