Sensors and In-Home Collection of Health Data:

A *Privacy by Design* Approach

www.privacybydesign.ca

August 2010

IATSL
Intelligent Assistive Technology and Systems Lab

Information and Privacy Commissioner,
Ontario, Canada

Acknowledgements

The authors wish to gratefully acknowledge the work of Michelle Chibba and Vance Lockton, Policy Department staff at the Information and Privacy Commissioner's Office, Ontario, Canada, for their input on this paper, as well as all of the researchers, graduate students, and collaborators of the University of Toronto's Intelligent Assistive Technology and Systems Lab who have been a part of the research presented in this paper.

Information and Privacy Commissioner,
Ontario, Canada

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

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca

Table of Contents

Commissioner's Foreword

In-home health care monitoring devices are gaining in prominence. *The Economist* recently carried a story about the "coming convergence of wireless communications, social networking and medicine [that will] transform health care" ("When your carpet calls your doctor", 2010). The sensor technologies required for applications in this field are becoming smaller and more efficient, and may be easily integrated into an individual's environment – or an individual's body. While there are clear benefits that will arise from these developments (better health monitoring capabilities, the ability for seniors to 'age with choice', etc.), the potentially detailed collection of personal data about an individual's physical state and behaviours will require careful examination with regard to possible privacy implications.

As the Information and Privacy Commissioner of Ontario, Canada, my mandate includes conducting research into privacy-related issues involved in emerging technologies or new programs that may impact privacy. In this white paper, I am pleased to have partnered with Dr. Alex Mihailidis and his research team from the Intelligent Assistive Technology and Systems Lab (IATSL) at the University of Toronto and the Toronto Rehabilitation Institute. Through their work, Dr. Mihailidis and his research team have demonstrated an understanding of the importance of privacy in home health care systems. It is critical that privacy be designed directly into technologies, at an early stage – and who better than the academic and research communities to achieve this task?

Our message for the application of sensors within health care is the same as that for any emerging technology: privacy cannot be sacrificed for other anticipated benefits (zero sum). However, nor do I propose stifling innovation or denying the benefits that technologies can bring to our lives. Instead, I support adopting a positive-sum paradigm: allowing for both privacy *and* functionality, instead of a trade-off between the two, representing a false dichotomy. Considering privacy from the outset and building in appropriate protections at the design phase can allow this to occur. Privacy protections are likely to be a major key to the adoption of in-home sensor technologies – individuals must feel comfortable that their privacy will not be violated within their own homes. Following the 7 Foundational Principles of *Privacy by Design* can help to achieve this goal. We advance the view that *Privacy by Design* is the *sine qua non* or the essential element that must be embedded in advances made in technology, data management and application of sensor technologies within the home health care environment. Let's make it a reality!

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

1 Introduction

Technological improvements in networking, wireless communications, and the miniaturization of electronics have resulted in a suite of emerging technologies that rely on the collection of information from within the home, from an individual's body, or both. In-home health monitoring[1] is a growing field that involves the in-home (or on-body) measurement of various physiological (heart rate, blood pressure, etc.) or behavioural characteristics (fall detection, dementia warning signs). This new technology brings with it significant potential benefits for both society as a whole and individual citizens, such as reducing strain on health care systems through a more preventative (rather than reactive) approach to potential health care problems, which generally improves an individual's clinical outcomes and/or independence (we discuss these benefits further in Section 3). In order to create these benefits, however, significant and continuous data collection about the individual is required. Until now, these data have not been accessible, as technologies were not sufficiently advanced to collect necessary information accurately, reliably, and securely. It is important to recognise that these data tend to be of a highly sensitive nature, as they are collected either directly about the individual or about actions taken within his or her home (traditionally the most privacy protected location in one's daily life). As such, people's privacy must be at the forefront of these activities and be strongly protected.

Privacy concerns should not prevent the potential benefits of innovation as seen through the development and application of new technologies. At the same time, though, privacy cannot be sacrificed in order to bring about other benefits. To do so would represent a 'zero-sum' trade-off, where the potential benefits of using a technology were negated by a loss of privacy. Instead, the 'positive-sum' must be achieved, in which all relevant objectives – privacy, functionality, usability, security, etc. – are respected and maintained. The manner in which this outcome can be achieved is becoming widely agreed upon: privacy and data security must be integrated at the design stage. (IPC, 2009; OECD, 2009)

In this white paper, we describe a general technology that is commonly used to collect data for in-home health care monitoring systems – sensors and sensor networks. We then identify the points of interest within such a system with regard to privacy, and describe some of the considerations that might be made when determining appropriate privacy protections. To demonstrate this approach, we will describe examples of devices being developed by the Intelligent Assistive Technology and Systems Lab (IATSL) at the University of Toronto and Toronto Rehabilitation Institute, and the lab's application of the *Privacy by Design* (*PbD*) principles [which are listed in Appendix A] to the technologies they create.

2 Overview of Sensor Technology

In the simplest terms, a sensor is an instrument that detects or measures a physical or environmental characteristic or state, and transmits and/or records the reading in some form (e.g., a visual display, audio signal, digital transmission, etc). Sensors appear in a nearly endless array of applications,

[1] See the IPC's white paper *Remote Home Health Care Technologies: How to Ensure Privacy? Build It In: Privacy by Design,* (http://www.ipc.on.ca/images/Resources/pbd-remotehomehealthcarew_Intel_GE.pdf)

some hundreds of years old. They range from the simple, such as thermometers that use mercury or alcohol to display a temperature reading or gym equipment (stationary bikes, etc.) that uses sensors embedded in handles to measure heart rate (and display this data to the user on-screen), to the complex, such as powerful telescopes that can detect immensely distant galaxies. Sensors are designed to detect and measure a particular feature of interest, such as a thermometer to measure temperature, a heart rate monitor to measure one's pulse, and a telescope to measure faint and distant energy sources. In many situations, multiple sensors will be used to jointly measure or detect particular states – this is referred to as a 'sensor network.' The scope of technologies that can be integrated into sensor-based systems is broad and constantly expanding.

When considering issues such as privacy in sensor-based systems, it is not sufficient to focus on only the sensors themselves. Instead, the entire end-to-end flow of data generated by the sensor system must be examined. As shown in Figure 1, there are four primary points at which privacy should be considered in sensor-based systems: the monitored individual, the sensors, the processing/display device, and the people/organizations that are able to access the data at any point (including those who may attempt to access the data without a legitimate purpose).

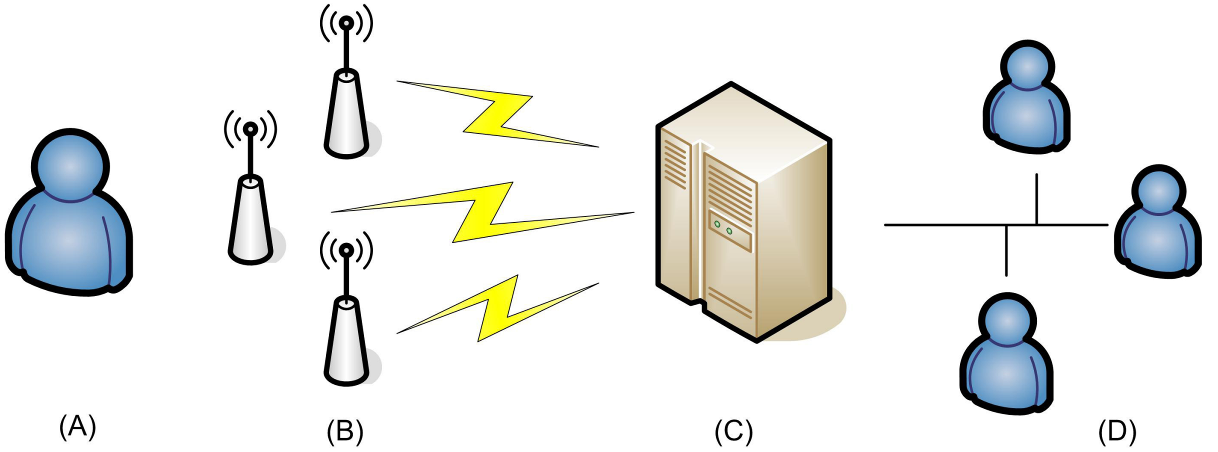

Figure 1 – In a sensor-based system, data about an individual (A) is collected by one or more sensors (B). These sensors transmit data to a server or other computing device (C) for processing and/or storage. This data may then be transmitted to, or accessed by, third parties (D).

A sensor system with which many will be familiar is Radio Frequency Identification (RFID), in which 'readers' are able to sense the presence of 'tags', and a communication protocol allows the sensed tag to transmit any data stored in its memory back to the reader for processing. There are numerous privacy guidelines that have been produced with respect to implementing RFID-based technologies.[2] However, though these resources may be considered a starting point for sensor technology privacy measures in general (particularly in regard to data processing, storage and access considerations), privacy and data security concerns are different (and often unique) across the various types of sensors – and thus in each instance, an appropriate approach to addressing these concerns must be identified.

[2] See, for instance, the IPC's white paper *RFID and Privacy: Guidance for Health-Care Providers*, available online at: http://www.ipc.on.ca/images/Resources/up-1rfid_HealthCare.pdf, or the IPC's earlier work *Privacy Guidelines for RFID Information Systems*, available online at: http://www.ipc.on.ca/images/Resources/rfid-guides&tips.pdf

In an RFID-based system, there are two particular considerations that set the technology apart from many other sensor-based systems with regard to privacy concerns. First, the point at which the user is engaged in the privacy protection process must be considered. With an RFID-based system, a user can be given control over the *distribution* point of information – that is, they may be allowed control of the device that pushes out data (i.e. the RFID tag), through on-off switches, shielding mechanisms or simply not carrying the tag (or item in which it is embedded). Many other sensor-based systems, on the other hand, give individuals control over the *collection* point of information, through options regarding what sensors are installed, where they are installed, and when they are active.

A second difference between RFID and many other sensor-based systems is seen in the *static* data of an RFID-based system, as opposed to the *dynamic* data generated by various other sensors. RFID tags are generally read-only; that is, the data stored in the tag's memory (a tag identification number or other information, depending on the application) is written once and subsequently transmitted in response to each query from a reader. Information can be inferred from multiple readings based on the time and place of each, but the tag itself will generally not introduce new information. Other sensors, though, will often be dynamic – each reading representing a different measurement of a particular characteristic (e.g., changes in temperature). Aggregation of these measurements over time may indicate significant trends and information beyond what can be deduced from any individual measurement. Thus, while for each technology a similar examination must be made of the data made available via a single transmission, different considerations will need to be made with regard to the potential aggregation of multiple readings.

Though the above represents only a sampling of the considerations that must be made when designing a sensor system based on a particular technology (RFID), it illustrates the importance of determining and addressing the privacy and data security concerns specific to each sensor-based application.

3 Sensors and In-Home Health Care

Sensors, for in-home health care applications, can be divided into two broad categories: behavioural and characteristic. *Behavioural sensors* are meant to observe actions: motion detectors to record entering/exiting a room, pedometers to count steps taken, cameras to detect motion patterns (such as potential falls), etc. Data regarding actions can be translated into behavioural information, with irregular or worrisome behaviours handled as required (alerts raised for fall detection, health care providers notified in case of potentially significant behavioural changes, etc). *Characteristic sensors*, on the other hand, measure the physiological attributes of an individual – body temperature, blood pressure, stress levels, blood-glucose levels, etc. – with the sensor system storing or reacting to this data as required by the particular reading and application.

Measurements from sensors may be constant, as in the case of sensors either implanted or worn directly on the skin, or may be occur only when the user takes a particular action. The sensor device may also be capable of automatically signalling a need for action to other devices; for example, a blood-glucose monitor which is capable of wirelessly signalling an implanted insulin pump (Wireless Incorporated, 2007). However, more commonly, sensor readings will either alert the individual (or a health care provider) about a current or potential problem, or be stored for future evaluation.

Recently, many applications of sensors and sensor networks to new intelligent home systems have been developed. These technologies can monitor people during common health-related activities (e.g. self-care activities, medication management), provide assistance to the user (e.g. providing prompts and reminders), and/or provide health status reports to the user, care providers, clinicians, caregivers, and family members. As the percentage of people in North America and Europe over the age of 65 continues to grow dramatically, there has been a significant increase in the number of systems that have been developed specifically to support older adult users. For example, Autominder is a device that uses sensors and artificial intelligence planning to schedule events (e.g., medication taking) at times when they will not interfere with a person's daily schedule, such as favourite television programs or daily walks (Pollack, 2006). Autominder uses environmental sensors to detect the status of activities, and if required, provides the user with context-aware reminders regarding unattended activities. The Gator Tech Smart House is an example of a smart home designed with older adults in mind (Helal et al., 2005). A sensor network distributed throughout the house takes into account context when performing actions to support the occupants. For example, if it is a sunny day outside and an occupant has the television on, the Gator Tech Smart House will automatically close the blinds to reduce glare. Other features include medication reminders that can appear on the bathroom mirror and automatic sensing and ordering for soap and toilet paper refills. Pigot et al. developed Archipel, a cognitive modeling system for cooking tasks that recognizes the user's intended plan and adapts prompting to a pre-determined cognitive impairment level (Pigot et al., 2008). Sensors placed in the kitchen environment, such as RFID tags and readers, detect which objects have been used and provide cues (audio, video and strategic lighting) to help users through each step in the task. As with Autominder, Archipel will not give reminders for tasks the person has already accomplished.

There are significant benefits to be had through remote home health care technologies (that is, technologies that can provide support without having a clinical professional present). Health care costs, for both providers and individuals, are reduced by decreasing the cost and time requirements associated with in-person monitoring and office visits, as well as through a general cost-saving focus on prevention and early detection of adverse health events (Noel et al., 2004; Stankovic et al., 2005; Pekka Raatikainen et al, 2008). Appropriate technologies may also be able to alert caregivers to changes in behaviour or physical state that may go unreported or unnoticed by the patient, but which represent important symptoms for proper diagnosis and treatment (Stankovic et al., 2005). Patients may also see better clinical outcomes with monitoring devices installed in their homes (Noel et al., 2004; Meyer et al., 2002), without significant restriction on their daily activities (Meingast, Roosta and Sastry, 2006).

4 Building In Privacy – *Privacy by Design*

The application of remote sensors to the provision of health care – particularly as sensors and data collection enter the home – brings additional factors to the already complex issue of health information privacy. Kotz et al. (2009), for instance, identify three particular features of remote home health care that have implications for privacy. Applied to sensor technologies, these features are as follows:

1. **More medical data** may be collected about a patient, as sensors allow continual monitoring of health characteristics over an extended period;

2. **Broader health data** may be collected about the patient; in addition to physiological data, information about an individual's lifestyle and activities may be recorded.

3. A **broader range of applications** may be enabled by the range of data made available through the use of sensor technologies.

The ability to maintain the privacy and security of patient information will be a key determinant of the success of remote home health care systems (see, for instance, the findings of Mihailidis et al., 2008). Of course, in ensuring privacy, the ability of these systems to aid in the provision of care cannot be compromised. What then, is the best manner of achieving these dual goals? The answer lies with *Privacy by Design* and the positive-sum paradigm.

4.1 Privacy by Design

Privacy by Design (*PbD*) is a concept developed in the mid-nineties that entails embedding privacy into the design specifications of technologies. This may be achieved by building the principles of Fair Information Practices into the design, operation and management of information processing technologies and systems (IPC 2010). While *PbD* has information technology as its primary area of application, it has also expanded in scope to also include accountable business practices and physical design and infrastructures. With the current near-exponential growth in the creation, dissemination, use and retention of personally identifiable information it is more critical now than ever to embrace the *PbD* approach if the concept of privacy is to be maintained in the 21st century.

4.2 The Positive-Sum Paradigm

Rather than following the conventional zero-sum mindset that sees privacy being attained at the expense of functionality or some other business objective, organizations must recognize that a positive-sum model is far more desirable. A win-win scenario, whereby privacy, the individual's well-being, and business interests may all be served, can and must be achieved. This positive-sum model can be attained if privacy safeguards are proactively built into a system at the outset. Privacy is essential to creating an environment that fosters trusting, long-term relationships with existing customers or users, while attracting opportunity and facilitating the development of new relationships. In a world of increasingly savvy and privacy-aware individuals, an organization's approach to privacy may offer precisely the competitive advantage needed in order to succeed.

Researchers in the remote home health care field have been very clear about the necessity of creating positive-sum technologies. Coughlin et al. (2007) found that the concerns of older adults with regard to Smart Home technologies, which must be addressed to promote acceptance thereof, included usability, reliability, privacy and trust, among others. Kotz et al. (2009) described the technology goal for remote health care technologies as being the development of "*usable* devices that respect patient *privacy* while also retaining data *quality* and *accessibility* required for the medical uses of the data" [original emphasis]. This positive-sum approach can and must be the end-goal for the designers and developers of sensor applications in health care for society to benefit fully from this new technology.

5 IATSL's COACH and HELPER systems

To demonstrate the integration of *Privacy by Design* into sensor-based home health care technologies, we will describe the work of the Intelligent Assistive Technology and Systems Lab (IATSL) at the University of Toronto and Toronto Rehabilitation Institute. IATSL is considered to be an international leader in the development of intelligent home systems, with a focus on aging-with-choice (meaning the freedom to choose where one would like to live) and older adults with dementia. The lab brings together a unique team of researchers from several disciplines such as engineering, computer sciences, occupational therapy, speech language pathology, medical sciences, and theatre and drama. This allows for a highly interdisciplinary approach in the development of new technologies, which is crucial in ensuring that a holistic approach is taken throughout the design process. Through the use of advanced computer science concepts, such as artificial intelligence, IATSL is developing *zero-effort technologies* that automatically learn about and react to the user of the device, thus requiring minimal interaction between different users (e.g., people with dementia, caregivers, family members, doctors, etc.) and the device itself. The rationale behind this approach is that health care monitoring devices should be reliable and intuitive to use with minimal opportunities for data to be misreported or tampered with.

Most of the assistive technologies developed at IATSL use computer vision as their primary sensor. Computer vision uses cameras (both still and video) to capture images that are then analysed by computers to extract and compile data of interest[3]. IATSL has chosen computer vision for the majority of their intelligent home systems as it has the potential to provide a much richer data set than other sensors (e.g., motion detectors, RFID tags, switches), can be used across different applications and tasks without the need for extensive reinstrumentation of an environment, requires much less hardware (and potentially lower costs) than other types of sensing systems, and provides very interesting research and theoretical challenges.

One example of a computer vision-based technology being developed by IATSL is COACH (**C**ognitive **O**rthosis for **A**ssisting a**C**tivities in the **H**ome). COACH is a system that employs various computer vision and artificial intelligence techniques to autonomously provide cues to an older adult with dementia to guide him or her through common activities of daily living (ADL), such as handwashing (Mihailidis, 2009). Handwashing was chosen as the first ADL to assist as it is a relatively safe activity that older adults with dementia have difficulties completing because of the planning and initiation skills required. In addition, using handwashing has allowed for the in-depth exploration of issues related to privacy through a low-risk context due to the ADL's relatively non-private nature.

COACH uses an overhead video camera to follow handwashing using a computer vision technique known as flocking (Hoey, 2010). Flocking uses colour to track the locations of the user's hands and artificial intelligence is applied to recognise when he or she is interacting with objects of interest, such as the soap and towel. This method of tracking is quite robust and able to dependably follow the location of the user's hands and the position of the towel, even after occlusion by an object or after leaving and returning to the camera's field of view (Hoey, 2010). Furthermore, the user does not have to wear any type of marker, such as a patterned bracelet, which is required by many other

[3] As a sensor is a device that detects or measures an environmental characteristic, this includes cameras, which detect and record light patterns.

similar tracking techniques. Artificial intelligence methods are employed to learn characteristics about each individual over time, such as what his or her level of independence is, what type of prompts are most effective with him or her, and the average amount of time it takes him or her to complete each step in handwashing. Not only does this approach enable COACH to customise guidance to each individual's needs, but also allows the system to adapt over time to changes in individuals' responsiveness and capabilities. If the system determines that the person requires assistance (e.g., he or she performs a step in the handwashing activity out of sequence, gets sidetracked, or is not sure what to do next), COACH is able to give different levels of audio/video guidance and is able to summon a caregiver to intervene if the user does not respond to prompts from COACH. The different levels of prompts available to COACH enable the system to select the most appropriate support for each individual's dementia particulars and his or her overall responsiveness (Mihailidis, 2009). Additionally, COACH has the potential to share information regarding assistance and user performance with interested parties, such as family, caregivers and clinicians. While a video camera is used as the sensor for COACH, it is important to understand that no images are recorded or stored in any way; each incoming frame is analysed and discarded so that only the coordinates of the hands and towel are transmitted to the artificially intelligent planning device. Additionally, clinicians are only able to view higher-level trends about patient data and performance, such as estimated level of dementia, the average number of prompts needed to get a patient to wash his or her hands, and with what step(s) of the task the patient may be having trouble.

A second example of a computer-vision based intelligent home system being developed by IATSL is HELPER (**H**ealth **E**valuation and **L**ogging and **P**ersonal **E**mergency **R**esponse). HELPER is designed to automatically detect when an adverse event, such as a fall, occurs and to work with the user to procure appropriate assistance. HELPER uses an overhead video camera to capture images of the environment (e.g., the individual's home) to track the people in it. A computer autonomously extracts a silhouette of the person and determines if the location of the silhouette is in a pre-defined "inactivity zone", such as a bed or chair, where a fall is unlikely and extended periods of inactivity are expected. If the silhouette is outside an inactivity zone then geometric and temporal features of the silhouette are calculated by the computer and are input into a classification algorithm to determine if the occupant is behaving normally or if an adverse event has occurred. As with the COACH, this capture and analysis is completed without any human intervention and the user does not wear any kind of markers or devices.

HELPER uses a dialogue module and automatic speech recognition (ASR) to ask a series of 'yes' and 'no' questions that determine: 1) if the person is injured and requires help; 2) if the person would like external assistance to be called; and 3) if help is required, who the system should call. This approach provides the user with control over his or her health by allowing him or her to choose who is notified, such as a neighbour, family member, a live call centre, or 911. If the system does not understand the user, or if there is no response at all, then the system will connect to a live call centre in order for a human operator to further assess the situation. If the person does not require or want assistance, the system will not place a call for assistance, but will continue to monitor the person. As with COACH, no images are recorded or stored and the user is in control of what data (if any) is seen by third parties.

6 Applying *Privacy by Design* to In-Home Health Care Sensors

One's health status affects virtually every aspect of his or her life. As such, people generally (and rightfully) wish to understand and have control over who has access to information regarding their well-being and how this information is used. With respect to sensor systems for health care, *Privacy by Design* (outlined in Appendix A) can be used to ensure users' privacy is implicitly protected through the design and functionality of devices. Below we describe three areas that are integral to sensor systems: the user, the sensor system, and the data. We show how *PbD* can be implemented to ensure privacy without compromising device performance and provide an example of how the intelligent home systems being developed by IATSL incorporate the principles being discussed.

6.1 Focus on the User – Keep it User-Centric

Key Privacy by Design Principles:

- Respect for user privacy
- Visibility and transparency
- Full-Functionality – Positive-Sum, not Zero-Sum

A focus on the user begins with respect. Privacy-friendly defaults, appropriate notice, and user-friendly options and interfaces are important to ensure that the user can fully engage in the protection and control of his or her own personal information. Systems' functionality should be transparent and their components visible, particularly in the application of sensors to home health care scenarios – monitored individuals should always be able to easily discern where the sensors are installed, what data is being collected and who can access it. This knowledge should be available to users (and any designated representatives) at all phases of the relationship with the device provider, which includes prior to installation when the potential user is evaluating the technology.

Of course, engagement with users can and should begin earlier than the point of (potential) deployment. Identifying potential privacy concerns at a *conceptual* stage of design allows *PbD* to be applied even earlier than the technical design phase of a technology, creating the possibility for discussions during the development of user requirements. The design practices used by IATSL, for instance, look to build complete visibility and transparency into systems by having representative users involved throughout the design process and testing of the final technologies, and by providing education sessions on how the system operates. This approach ensures that the system's users have an understanding of how the system operates and that reasonable and appropriate measures to protect privacy have in fact been incorporated into the final design. For example, in designing the COACH system, caregivers expressed concerns about how the system used the video data that were captured, especially if the caregiver was captured on the video as well. After they were shown exactly how the system's algorithms processed the videos and that the images were then deleted automatically after processing was completed, they were re-assured and gained trust in the technology. Users of any technology should always be given the opportunity to ask any questions they have about the technology and must be given honest answers communicated in a way they can understand.

Early engagement with the user also allows the designer to understand any unanticipated sensitivities with regard to the data being collected. Dr. L. Jean Camp of Indiana University, for instance, tells audiences of an intelligent home system designed to aid seniors which takes images of visitors at their front door, and then either provides memory cues or stores this data as specified by the user. In interviewing one senior, Dr. Camp found that there was a sensitivity to this information that researchers had overlooked – specifically, the individual did not want others to have a record of when her boyfriend came to visit (Camp, 2010). Due to this, it was determined that this particular system should have three phases: on, off, and mute, the latter being the case when a system remains on, but is not transmitting any data.

As discussed above, attention to identifying and addressing privacy concerns before and during the design phase of a technology supports the notion that privacy should be considered as an essential part of the feature set of sensor technologies. If the user does not feel that his or her privacy is being respected, then he or she will be much less likely to adopt the technology. Therefore, when the practice of focusing on user and involving them in all phases of development is embraced at an organizational level, the positive-sum paradigm – designing to maximize both privacy and functionality – will necessarily follow.

6.2 Focus on the Sensor System

Key Privacy by Design Principles:

- Proactive not Reactive; Preventative not Remedial
- Privacy Embedded into Design

Once the user's ongoing privacy requirements and desires have been determined, a second focal point emerges – the design of the sensor system itself. This requires a number of privacy protections appropriate to the sensitivity and identifiability of the data, which should be developed and proactively incorporated into systems. Given the remote installation and (often) limited computing power and connectivity of the sensors themselves (as opposed to the connected and quite powerful back-end systems), it is important and far more effective – both in terms of cost and functionality – to address all foreseeable privacy issues before they occur, as a breach in privacy would require the updating or re-instrumentation of a system after installation. Where possible, protections should also be embedded deeply into system components, that is, made part of the sensors themselves. For instance, much of the data processing can usually be done within the sensor device itself, or on a local (in-home) processor to which the sensor is directly connected via a cable. Transmitted data can also be formatted to contain only the reading and a sensor ID and not transmit any information about the user, the type of sensor, or any kind of index that might indicate that readings from multiple sensors refer to the same individual (this information being added, as necessary, at the processing stage). Sensor systems can be designed in a manner such that data is only transmitted after authentication of the receiver (particularly in the case where multiple readings are collected or identifiers need to be added prior to transmission). Sensors should also be designed to respect the principle of data minimization, collecting only information that is required for the specified purpose; data should not be collected, for instance, based on an undefined potential future usage. Finally, it should be clearly understood that each sensor represents a potential point of failure in a sensor network. For example, Chan and Perrig (2003) suggest that sensor networks may require the capability of ensuring secure operation even in the presence of a small number of malicious or compromised nodes. It is important that sensor systems are able to recognise if they are being compromised and alert the user and/or provider. Failures in a sensor's ability to transmit or a processor not receiving expected data must raise appropriate warnings in a timely manner.

The operation of any privacy features should also require no or minimal effort of the part of the user – after initial set-up, the user should not have to actively enforce his or her privacy choices. This is particularly true for sensor applications in the health care domain. The designs of 'always-on' sensor-based home health care systems are intended to be, in most cases, minimally intrusive. Users are not necessarily meant to be consciously aware of these systems at all points of interaction; individuals are instead meant to be able to go about their normal lives, with devices providing assistance only when required or taking readings inconspicuously. Other sensor applications might be engaged only at critical moments, when the individual keenly requires the service provided by the device. If a system is continually running or being used during an emergency, data privacy is likely not to be at the forefront of the individual's mind throughout the point of data collection. Privacy – via embedded and by-default protections – must thus be something that the individual can *expect* to be present, much as they expect any other functionality of the sensor device to be available when required.

By way of example, IATSL's COACH and HELPER systems are proactive in ensuring privacy through intrinsic features. The application of artificial intelligence and other advanced computer science concepts allow these systems to operate autonomously. A processor wired to the video camera analyses each image frame the moment it is captured then deletes it before the next frame is captured. No images are broadcast over a network – and thus no images can be intercepted and/or viewed by a human or other computer. This key design feature eliminates many potential privacy concerns while simultaneously significantly reducing the amount of data that needs to be transferred to fully support the user. If COACH summons a caregiver to help a man wash his hands or a user of HELPER wishes to place a call to her daughter, the connection will be made over existing LAN and/or phone networks in the same fashion as a call is placed now. In the case of the user consenting to allow a third party (e.g., family members, caregivers, and clinicians) to view data regarding his or her person, IATSL's approach attempts to deliver a maximized level of privacy by having the system itself keep any personal data collected in its operation, while a third party would only see a "boiled down" report of key statistics and indicators. Using artificially intelligent systems to collect and analyse data not only helps to ensure the privacy of the users, but also enables these technologies to be more usable as they do not require complex interfaces or input devices for a user to operate them. Not requiring users to enter information also avoids the possibility of incorrectly inputted data.

6.3 Focus on the Data

Key Privacy by Design Principles:

- End-to-end Lifecycle Protection
- Privacy as the Default

At some point, collected data must be processed for a sensor application to serve a function. It is the handling of these data – and particularly, the need for end-to-end data protection – that is the third focal point for ensuring privacy in sensor applications for health care.

End-to-end lifecycle protection of data requires analysis and protection of each stage of information management. In some applications, such as IATSL's COACH system, this can be accomplished by automatically processing data as fast as it is collected by the sensors and translating it into more general results (e.g., an alert to a caregiver, a diagnosis, etc.), so long as these results are also given appropriate protections. Of course, it is not always the case that sensor data can be immediately deleted. For instance, in many medical systems the long-term collection of sensor readings may be part of a crucial diagnostic tool, such as trends in blood pressure or glucose levels. It is here that end-to-end protections must be especially clearly defined and implemented. Data must be given "cradle-to-grave" protections, including secure collection, transmission, storage, and destruction protocols, as well as methods to ensure the information being used is kept as accurate and up-to-date as possible. Users should have access to their own data and be able to define and control who has access to it. This control can generally be understood by answering the question, 'Who can see what data, and under what circumstances?' Furthermore, data protections appropriate to the application should be enabled by default – even if the user were to take no action, his or her privacy should remain intact.

In IATSL's HELPER system, the use of automated dialogue and speech recognition allows a user to maintain control over the decision of whether or not personal health data should be transmitted outside of the home. If the user is capable of making this decision (i.e., conscious and responsive), the system respects the person's choice. Moreover, during the initial set-up of the system, the user can select the level of privacy that best suits him or her (e.g., whether or not an image is automatically broadcast to emergency response services if there is a bad accident). There remains, of course, the question of 'What constitutes a "bad accident"?' Are there instances when the system should overrule a user's decision in the interests of his/her wellbeing? It is important that developers of health care technologies work closely with experts in health care, ethics, and privacy as well as representative end-users, to answers to questions such as these and determine if and when system actions are acceptable and appropriate.

6.4 Overall Privacy by Design Considerations

Privacy by Design offers a potential method to integrate and address privacy concerns at the design stage. With respect to sensor-based health care technologies, this requires organisations, health care providers, and device developers to work with end-users and experts in the fields such as medicine and ethics to ensure that the privacy of end-users is respected and maintained.

IATSL's focus on the use of computer vision techniques is a clear example of both the need for, and power of, *PbD*. As with many home health care technologies, the privacy issues in IATSL's systems revolve around the collection of potentially sensitive data. In the case of the computer vision-based systems developed by IATSL, this collection creates particularly rich datasets regarding the user's actions within his or her home. COACH and HELPER use images of the user to augment or generate health data and indicators – sensitive information that must be protected accordingly. However, as is the case when applying sensors to any home health care application, IATSL researchers are able to avoid potential privacy issues through the design and implementation of features that adhere to the *PbD* principles.

7 Conclusions

Sensors act as "the interface between the physical world and the world of electrical devices," (Wilson, 2008) creating opportunities for innovative new means of monitoring, detecting and preventing health-related conditions in one's home. However, in order to achieve the full benefits of this new application of sensor technologies to health care, it is essential that appropriate privacy measures be developed to protect the large amounts of potentially very sensitive data that are gathered by these systems. These protections should be both user-focused and user-friendly, beginning with the physical design of the sensor system and continuing throughout the lifespan of the data.

With their intelligent home systems, IATSL's devices demonstrate how privacy may be strongly maintained, without compromising the user's well-being. By focusing on the individual, working with target users to determine what data collection is necessary and acceptable, and developing clear communications strategies that explain how the devices operate, many privacy concerns are implicitly incorporated or avoided. These protections are active by default, embedded into the system, and are "zero-effort" for the user – each an important factor in assuring a potentially vulnerable population that collected data will not be put to unexpected use. Most importantly, these protections did not 'simply happen'; the culture of privacy and consideration for the end-user must itself be embedded into the Lab environment, and each of its developers.

The integration of sensors into home health care technologies can present new challenges for privacy. However, these challenges may be addressed through the application of *Privacy by Design* – proactively building safeguards into the design of sensor systems.

References

Axisa, F. et al. (2005) Flexible Technologies and Smart Clothing for Citizen Medicine, Home Healthcare, and Disease Prevention. *IEEE Transactions on Information Technology in Biomedicine,* 9(3), 325 – 336.

Camp, L. Jean. (2010) Respect by design. As presented at *Privacy by Design: The Gold Standard – The Information and Privacy Commissioner of Ontario's Second Annual Privacy by Design Challenge.* January 28, 2010, Toronto, Ontario.

Chan, H. and Perrig, A. (2003) Security and Privacy in Sensor Networks. *IEEE Computer,* 36(10), 103-105.

Coughlin, J.F. et al. (2007) Older Adult Perceptions of Smart Home Technologies: Implications for Research, Policy & Market Innovations in Healthcare. *IEEE Proceedings of the Engineering in Medicine & Biology Conference*, Lyon, France, August 2007.

Finkelstein, S., Speedie, S., and Potthoff, S. (2006) Home Telehealth Improves Clinical Outcomes at Lower Cost for Home Healthcare. *Telemedicine and Health*, 12(2), 128-136.

Helal, S., Mann, W., El-Zabadani, H., King, J., Kaddoura, Y., & Jansen, E. (2005). The Gator Tech Smart House: A Programmable Pervasive Space. *IEEE Computer,* 38(3), 50-60.

Hoey, J., Poupart, P., Von Bertoldi, A., Craig, T., Boutilier, C., Mihailidis, A. (2010). Automated Handwashing Assistance For Persons With Dementia Using Video and A Partially Observable Markov Decision Process. Journal of Computer Vision and Image Understanding - Special Issue on Computer Vision Systems, 114(5), 503-519

IPC (2010). The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices. Available online at: http://www.privacybydesign.ca/docs/pbd-implementation-7found-prin.pdf

IPC (2009). Transformative Technologies Deliver Both Security and Privacy: Think Positive-Sum, not Zero-Sum. Available online at: http://www.ipc.on.ca/images/Resources/trans-tech.pdf

IPC (2009a). Remote Home Health Care Technologies: How to Ensure Privacy? Build It In: Privacy by Design. Available online at: http://www.ipc.on.ca/images/Resources/pbd-remotehomehealthcarew_Intel_GE.pdf

IPC (2008) RFID and Privacy: Guidance for Health-Care Providers. Available online at: http://www.ipc.on.ca/images/Resources/up-1rfid_HealthCare.pdf

IPC (2006) Privacy Guidelines for RFID Information Systems. Available online at: http://www.ipc.on.ca/images/Resources/rfid-guides&tips.pdf

Kotz, D., Avancha, S., and Baxi, A. (2009) A Privacy Framework for Mobile Health and Homecare Systems. *SPIMACS'09*, November 13, 2009, Chicago, Ill, USA

Lin, X. et al. (2009) SAGE: A Strong Privacy-Preserving Scheme Against Global Eavesdropping for eHealth Systems. *IEEE Journal on Selected Areas in Communications*, 27(4), 365-378.

Meingast, M., Roosta, T., & Sastry, S. (2006) Security and Privacy Issues with Health Care Information Technology. Conference proceedings of the *IEEE Engineering in Medicine and Biology Society*, 1, 5453-5458.

Meyer, M. et al. (2002) Virtually Health: Chronic Disease Management in the Home. *Disease Management*, 5(2), 87-94.

Mihailidis, A., et al. (2008) The Acceptability of Home Monitoring Technology Among Community-Dwelling Older Adults and Baby Boomers. *Assistive Technology*, 20(1), 1-12.

Noel, H. et al. (2004) Home Telehealth Reduces Healthcare Costs. *Telemedicine Journal and e-Health*, 10(2), 170 – 183.

Mihailidis, A. and Boger, J, (2009). How engineers are helping seniors with dementia stay at home. Journal of Policy Engagement, 1(4), 2-8.

OECD (2009). OECD Experts Conference: *Using Sensor-Based Networks to Address Global Issues*: *Policy Opportunities and Challenges*. Lisbon, Portugal, June 8-9, 2009. Summary available at: http://www.oecd.org/sti/ict/sensors

Pigot, H., Lussier-Desrochers, D., Bauchet, J., Giroux, S., & Lachapelle, Y. (Eds.). (2008). *A Smart Home to Assist in Recipe Completion*. Amsterdam, The Netherlands: IOS Press.

Pollack, M. E. (2006). Autominder: A Case Study of Assistive Technology for Elders with Cognitive Impairment. *Generations*, 30(2), 67-79.

Pekka Raatikainen, M.J. et al. (2008) Remote monitoring of implantable cardioverter defibrillator patients: a safe, time-saving, and cost-effective means for follow-up. *Europace*, 10(10), 1145-1151.

Stankovic, J. A. et al. (2005) Wireless Sensor Networks for In-Home Healthcare: Potential and Challenges, in *High Confidence Medical Device Software and Systems (HCMDSS) Workshop*, Philadelphia, PA, June 2-3, 2005 (position paper).

When your carpet calls your doctor. (2010, April). *The Economist,* 394, 65-66.

Wilson, J. (2008) *Sensor Technology Handbook, Newnes/Elsevier, Oxford.* As cited in: OECD (2009) *Sensors, Sensor Networks, and the Environment: Technologies, Applications and Impacts.*

Appendix A – The *Privacy by Design* Principles

Available online at: http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

Privacy by Design is a concept developed by Dr. Ann Cavoukian in the 1990's, to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems.

Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.

Initially, deploying Privacy-Enhancing Technologies (PETs) was seen as the solution. Today, we realize that a more substantial approach is required — extending the use of PETs to PETS *Plus* — taking a positive-sum (full functionality) approach, not zero-sum. That's the "*Plus*" in PETS *Plus*: positive-sum, not the either/or of zero-sum (a false dichotomy).

Privacy by Design extends to a "Trilogy" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and networked infrastructure.

Principles of *Privacy by Design* may be applied to all types of personal information, but should be applied with special vigour to sensitive data such as medical information and financial data. The strength of privacy measures tends to be commensurate with the sensitivity of the data.

The objectives of *Privacy by Design* – ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage – may be accomplished by practicing the following 7 Foundational Principles:

1. ***Proactive*** not Reactive; ***Preventative*** not Remedial

The *Privacy by Design* (*PbD*) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. *PbD* does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to prevent them from occurring. In short, *Privacy by Design* comes before-the-fact, not after.

2. Privacy as the ***Default***

We can all be certain of one thing — the default rules! *Privacy by Design* seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, by default.

3. Privacy ***Embedded*** into Design

Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

4. *Full* Functionality – Positive-Sum, not Zero-Sum

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. *Privacy by Design* avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.

5. End-to-End Lifecycle Protection

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, in a timely fashion. Thus, *Privacy by Design* ensures cradle to grave, lifecycle management of information, end-to-end.

6. Visibility and Transparency

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

7. Respect for User Privacy

Above all, *Privacy by Design* requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

About the Authors

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

Dr. Ann Cavoukian is recognized as one of the leading privacy experts in the world. Noted for her seminal work on Privacy Enhancing Technologies (PETs) in 1995, her concept of Privacy by Design seeks to embed privacy into the design specifications of technology, thereby achieving the strongest protection. An avowed believer in the role that technology can play in protecting privacy, Dr. Cavoukian's leadership has seen her office develop a number of tools and procedures to ensure that privacy is strongly protected, not only in Canada, but around the world. She has been involved in a number of international committees focused on privacy, security, technology and business, and endeavours to focus on strengthening trust and confidence in emerging technological applications. Dr. Cavoukian also serves as the Chair of the Identity, Privacy and Security Institute at the University of Toronto, Canada and is a member of the Future of Privacy Advisory Board. Recently reappointed as Commissioner for an unprecedented third term, Dr. Cavoukian intends to grow Privacy by Design and hopes to make it go "viral."

Alex Mihailidis, Ph.D., P.Eng., Associate Professor, University of Toronto; Barbara G. Stymiest Research Chair in Rehabilitation Technology, Toronto Rehabilitation Institute

Dr. Alex Mihailidis is an Associate Professor in the Department of Occupational Science and Occupational Therapy (University of Toronto), with cross appointments in the Institute of Biomaterials and Biomedical Engineering (U of T) and the Department of Computer Science (U of T). He is also the Barbara G. Stymiest Research Chair in Rehabilitation Technology at Toronto Rehabilitation Institute. He has been conducting research in the field of pervasive computing and intelligent systems in health for the past 13 years, having published over 80 journal papers, conference papers, and abstracts in this field. He has specifically focused on the development of intelligent home systems for elder care and wellness, technology for children with autism, and adaptive tools for nurses and clinical applications. He currently holds several major research grants from internationally recognized funding agencies to support this work (including both the Canadian and American Alzheimer Associations, NSERC, and Intel Corporation). He is also a CIHR New Investigator. His research has been completed through collaborations with other researchers in this field from Canada, the United Kingdom, and the United States, and with various industrial partners. Dr. Mihailidis has also co-edited two books: one from CRC Press entitled "Pervasive computing in healthcare", and the other from IOS Press entitled "Technology and Aging", which resulted from him being the conference chair for the 2nd International Conference on Technology and Aging.

Jennifer Boger, M.A.Sc., P.Eng., Research Manager, University of Toronto; Toronto Rehabilitation Institute

Jennifer Boger has been an active member in the field of computerised assistive technology for enhancing safety and independence for older adults and people with disabilities for more than eight years. Examples of projects Jennifer is involved in include: using an artificially intelligent system to assist people with dementia complete activities of daily living; a pervasive system for detecting and responding to emergencies in the home, such as falls; investigating the impact of design on product usability for older adults with dementia; surveying the current usage of high and low tech technologies in the community; and an anti-collision and navigation system for powered wheelchairs. Apart from advancing the technological capabilities of computer-bases assistive technologies, Jennifer's interests include the application of user-centred design to the assistive technology development process, the advancement of zero-effort technologies, and actively perusing collaboration between the diverse spectrum of stakeholders involved in the field of assistive technologies. Jennifer holds a Master of Applied Science in Biomedical Engineering and is a Professional Engineer. She is an author on numerous peer reviewed journal and conference publications regarding artificially intelligent assistive technology, including co-editing the book "Technology and Aging" (IOS Press).

PbD

www.privacybydesign.ca

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8
Telephone: (416) 326-3333
Fax: (416) 325-9195
E-mail: info@ipc.on.ca
Website: www.ipc.on.ca

Intelligent Assistive Technology and Systems Lab
160-500 University Avenue
Toronto, Ontario
Canada M5G 1V7
Telephone: (416) 946-8573
Fax: (416) 946-8570
E-mail: iatsl@utoronto.ca

The information contained herein is subject to change without notice. IATSL, University of Toronto, Toronto Rehabilitation Institute, and the IPC shall not be liable for technical or editorial errors or omissions contained herein.

August 2010

http://www.iatsl.org | http://www.privacybydesign.ca

IATSL
Intelligent Assistive Technology and Systems Lab

Information and Privacy Commissioner,
Ontario, Canada