Office of the
Privacy Commissioner
of Canada

Wearable Computing

Challenges and opportunities for privacy protection

Report prepared by the Research Group of the Office of the Privacy Commissioner of Canada

Table of Contents

Abstract

The purpose of the research report is to provide the OPC with a better understanding of the privacy implications of wearable computing technologies as a foundation for the OPC's advice to Parliament, policy position development and future compliance activities. Rapid technological innovation, consumer demand and dropping costs are fueling the development and adoption of a new generation of wearable devices. These devices, worn on the user's body and sometimes tethered to the individual's smart phone, can amplify the tracking and profiling risks that are characteristic of the current mobile ecosystem. The report provides an overview of wearable computing and some of its privacy implications. Following a discussion of the application of federal privacy laws in this environment, the report sets out some wearable computing design considerations to enhance built-in privacy protections and concludes with some potential next steps.

Introduction

While only some wearable products are currently available on the consumer market, many more will likely launch in the near future. Wearable computing is set to become a much more prominent feature of our lives. When the OPC addressed the issue of device sensors in our guidance to mobile application developers, we talked about sensors permitting location awareness which, when combined with data on what we do and what we think, create a portrait of who we are. Wearable computing brings this portrait *to life*.[1]

While this research report focuses on body-worn cameras and technologies, the OPC has also examined the surveillance potential of other mobile technologies, such as drones,[2] that are becoming part of our environment. The wearable era compounds and amplifies privacy risks in the mobile environment by gathering additional, and intimate, personal information. The differences between a smart phone and many wearable computing devices are more of degree than in kind, but they are important differences from the point of view of privacy protection. Many are an extension of the current capabilities of smart phones. The user can actively contribute data and, when combined with other data, the result is a rich resource. There are many types of sensors with different capabilities. For example, sensors have the ability to collect, in real time, information about:

- the user's body: mood, habits, physical activities, health status, speed, mobility and
- the user's environment: images, sounds, temperature, humidity, location, social environment as well as computer-generated data to mediate the user's experience of the world around them.

Though a camera would only capture some of these elements, the camera feature is the focus of many current privacy concerns.[3] It is the ability of these devices to record, perhaps constantly, and perhaps covertly, that leads to many concerns. Interestingly, wearable camera devices that always face away from the device wearer may not actually capture images of the wearer at all, unlike smart phones with reversible cameras that make it easy for the user to include themselves in images.

Recent and widespread availability of a number of appealing wearable computing products on the consumer market at an accessible price point have increased the urgency in our developing a more nuanced understanding of the privacy implications of this issue. A number of important barriers to the adoption of early wearable computing devices such as battery life, aesthetics and ease of use[4] are being overcome and we may anticipate that the development cycles in this area will be as rapid as those in the mobile app ecosystem.

We know that conveying meaningful information about privacy choices remains a challenge in the mobile space, with a small screen and intermittent user attention. As we explored in our guidance to mobile

application developers,[5] these design characteristics add to the difficulty in reaching users with the right information about their privacy rights, in a form they can understand and at the right time for them to make informed choices.

Wearable computing further compounds the challenge of reaching users. More importantly perhaps, it also amplifies the challenge of protecting the privacy of non-users, who may be the subject of audio and video recordings. This paper will deal primarily with devices containing cameras as they are the current focus of public debate. This research is based on our knowledge of the environment and wearable technologies at this time. It may be updated as required to reflect changes in the wearable computing ecosystem and the broader technological and social environment.

1. What is wearable computing?


Source: Shutterstock

Wearable computing is the use of a miniature, body-borne computer or sensory device worn on, over, under or integrated within, clothing.[6] Constant interaction between the user and the computer, where the computer "learns" what the user is experiencing, at the time he or she is experiencing it, and super-imposes on that experience additional information, is an objective of current wearable computing design.

According to a 2013 market research report,[7] there are currently four main segments in the wearable technology marketplace:

- fitness, wellness and life tracking applications (e.g. smart clothing and smart sports glasses, activity monitors, sleep sensors) which are gaining popular appeal for those inclined to track many aspects of their lives; [8]
- infotainment (smart watches, augmented reality headsets, smart glasses);
- healthcare and medical (e.g. continuous glucose monitors, wearable biosensor patches[9]) and
- industrial, police and military (e.g. hand worn terminals, body-mounted cameras, augmented reality headsets).

While categorizing wearable computing devices in this way can be helpful, it also creates the risk of overlooking creative ways in which the devices could be applied in different fields. There is a wide spectrum of capabilities among the devices. Innovations abound in different aspects of wearable computing and we can only cover a select few here.

a) Some characteristics of wearable computing

Many wearable technologies currently under development, or on the market, have appealing characteristics[10] that could contribute to broad consumer adoption. For example, they:

- have a visual appeal;[11]
- can be seamlessly integrated with the wearer's clothing, body or linked to a smart phone;
- can be customized and adapted to the needs of the user and provide feedback;
- can supplement the user's own physical or mental abilities;
- are relatively low cost for the benefit derived;
- are versatile and have a wide variety of personal and workplace applications; and
- are relatively simple for a consumer to set up and operate.

Given these potential characteristics, even a casual observer would conclude that there is potential for broad appeal of wearable devices.

b) How wearable computing differs from mobile computing

Many wearable devices can be out and operating all the time, whereas smart phones are often either in your hand, in a pocket or a bag. This distinction may be fleeting with new ways to mount smart phones on the body. However, for the moment, some wearable devices can amplify privacy risks in the mobile environment by collecting images, audio and video in unobtrusive, or covert, ways and by creating the potential to gather this personal information in situations where a more obvious camera device would not be socially acceptable.

c) Market growth forecasts and some drivers in the adoption of wearable computing

Current market adoption forecasts for wearable computing devices vary but they all suggest significant growth. Juniper Research has identified 2014 to be the watershed year for wearable devices.[12] IMS Research suggested in 2012 that 171 million wearable devices would be shipped by 2016.[13] ABI Research forecasted that the wearable computing device market will grow to an astounding 485 million annual device shipments by 2018.[14] BI Intelligence suggested more limited adoption, forecasting 100 million wearable devices being shipped in 2014, and reaching 300 million units five years from now.[15]

Sports and activity trackers are the areas with the most growth potential at this time, but the market for wearable computing may not reach its potential until the technology is fully integrated into our clothing, becoming seamless and invisible,[16] and we no longer have to reach for our phones. Market speculation about Apple offering other highly disruptive wearable technology, like its introduction of the iPhone in 2007,[17] is building, fueled by various reports of "iWatch" patent filings[18] and its recent hiring of an expert in luxury fashion.F[19] Widespread smart phone adoption is another factor that will improve the likelihood of individuals buying wearable computing devices that are tethered to those phones.

Emerging business models driving the adoption of wearable computing will be important to monitor and understand. For example, companies selling wearable fitness tracking devices may be focused on selling the fitness enhancing product to the consumer, but they may also be interested in using the information to target and customize advertising.

Source: Shutterstock

d) From visual aids to mediated reality

Historically, examples of wearable computing, such as the evolution of timekeeping with pocket and wristwatches,[20] show how the relationship between people and machines has evolved to answer certain questions or solve particular problems. As well, wearable *assistive* technologies have been with us for centuries. Assistive technologies for vision have evolved from magnifying glasses, to eyeglasses, to contact lenses.[21] The US Federal Drug Administration has recently approved retinal implants[22] that, when used with glasses and a computer to send a signal to the implant, can help some blind patients experience some degree of sight.

Some wearable devices overlay sound, video, graphics or location information on what the user sees. For example, the OrCam device[23] is a commercially available vision aid which can identify both objects and people pointed to by the user and then uses bone-conduction technology to communicate this information to the user, all at a cost similar to that of a hearing aid.[24] Innovega has developed an augmented reality system called

iOptik which projects a heads-up display on contact lenses from specialized eyeglasses.[25] Augmented reality wearable computing devices can super-impose sound, video, graphics or GPS data.[26] Canadian inventor and wearable computing pioneer Steve Mann has also developed several "diminished" reality visual wearable devices which can selectively *decrease* or simplify information that is made visible to the user. A commercial application of this technology is a real-time video helmet for use by welders to get detailed and accurate information about the flame while protecting their eyes.[27] Filtering light is one application but there are other ways that wearable devices could filter the user's experience that will be explored further in the conclusion to this report.

e) Some wearable computing applications

Wearable computing has the potential to revolutionize several sectors by reducing the physical barriers to interacting with the digital world.[28] Below are some products from the current technology marketplace that have received media attention over the last year. There are interesting commonalities in the applications of the technology for divergent markets such as consumer leisure activities, industrial workplaces and patient care. For example, a speech-driven digital assistant being developed by Kopin, called Golden-i, which helps to prioritize activities and filter information could have many diverse applications.[29] New generations of intelligent digital assistants, such as IBM's question-answering Watson supercomputer technology, that are now coming to smart phones,[30] will be developed for wearable devices in the future.

Fitness, wellness and life trackers

If individuals were once considered passive data subjects, wearable computing provides an opportunity for them to be actively involved in the collection, use and disclosure of great volumes of data about themselves, and others around them. For example, the tiny Narrative Clip "lifelogging" camera, hangs around the user's neck and takes a picture every 30 seconds to document the user's activities throughout the day.[31]

Source: Shutterstock

One estimate suggests that the market for wearable sports and health wireless monitoring devices will reach nearly 170 million devices by 2017.[32] Under the fitness and wellness category, there are a whole host of so-called "lifebands," such as Nike+ FuelBand,[33] Fitbit,[34] Bodymedia [35] and Jawbone[36] that measure daily activity levels and calculate calories burned. More importantly, the device uses the wearer's smart phone to link to a cloud application which evaluates the data and provides advice to follow and gives the user an ability to share the results with his or her community. There is also a new generation of ear buds that deliver music as they measure real-time biometric and physiological data and send this data to the user's smart phone.[37] As well, the Shine activity tracker is a good example of a small, light, and attractive wearable device that pairs with the user's smart phone. There are also a variety of smart watches, such as Pebble[38] and Samsung's Galaxy Gear,[39] that wirelessly connect to the user's smart phone.

Infotainment (and related) wearable devices

GoPro cameras have become widely popular with sports enthusiasts to capture video and pictures of themselves, but the camera's convenience, functionality and relatively low cost is also leading to adoption in other activities and fields.[40]

Google Glass[41] is a head-mounted computer that has received attention[42] from international data protection authorities. It is only one of several wearable devices with similar capabilities, distinguished perhaps by the vast potential of integration with Google's other holdings and the creativity of wearable application developers. For example, the Vuzix Smart Glasses M100[43] are a hands-free smart phone display with integrated sensors and Internet connectivity, which became available in December 2013. Another eyeglasses product, Recon Jet, produced by Vancouver-based Recon Instruments, has been designed for athletic activities and functions independent of a smart phone. It is slated to ship in March 2014.[44]

The promise of virtual reality experiences is also approaching with developments in the field of immersive visualization. The ongoing development of Oculus Rift,[45] a virtual reality visor for immersive gaming, also has applications for training in a number of high risk fields. Muscle stimulation technology, currently used in the treatment of paralysis, could also make gaming on a smartphone a more intense experience.[46] Researchers have linked their device through a mobile phone to electrodes that are placed on a user's forearm. These electrodes cause the gamer's muscles to contract, thereby giving a sense of force being exerted in connection with the game.[47]

Advances in gesture control address the challenge of having to rely on voice commands and cameras. Waterloo's Thalmic Labs has developed the MYO Bluetooth armband motion control device, which uses sensors to detect movements in the user's forearm muscles and translate them into digital commands.[48] Twenty-five thousand MYO armbands have been pre-ordered for $149 US each and are set to be shipped in 2014.[49] As well, a portable version of Microsoft's motion-sensing device for the Xbox Kinect, called Digits, is being developed.[50] Digits can replicate arm and finger movements on screen or allow control of a complex computer game.[51] Leap Motion has already launched a motion-controlled sensor, along with a variety of applications, to let the user interact with computers using hand gestures.[52]

Healthcare and medical

In a recent study conducted by PricewaterhouseCoopers, more than a third of Canadians conveyed that mobile health apps will make health care more convenient in the next three years and nearly 80% of respondents said they would be comfortable using a virtual monitoring service for a chronic condition.[53] This feedback complements the findings of the 2013 Canadian Telehealth Report, which explained that provincial governments recognize the potential of medical peripherals, such as digital stethoscopes and cameras, and are looking at either introducing or increasing their use in telemedicine in the coming years.[54]

In addition to devices that monitor a user's blood pressure for signs of heart attack and stroke, there are some more revolutionary developments in the health sector. For example, the Google X lab is in the process of developing a contact lens to help diabetics monitor their blood sugar levels.[55] Proteus Digital Health[56] is developing a new category of products and services it calls "digital medicines." Already approved for certain uses in the US,[57] a digestible microchip the size of a grain of sand can be added to medication. When it reacts with stomach juices, it sends a signal to a patch on the patient's skin, which relays the information to a smart phone which in turn relays the information to the doctor's office.[58] This provides the capability to report back to patients, health providers, family members and researchers on whether patients take their medicine and how it affects them.[59]

Industrial, police and military applications

Ratheyon's Aviation Warrior system is a pilot's helmet with a flip-down monocle display screen to show mapping, location readings and other sensor data from the cockpit indicators when the pilot is away from the

aircraft to provide accurate and timely situational awareness.[60] The helmet is integrated with a body-worn computer and a smart phone strapped to the pilot's wrist.
Kopin's Golden-i[61] device is being developed to provide live video streaming, mobile internet access, GPS navigation and hands-free control for maintenance workers, police, paramedics and firefighters. As well, Motorola's HC1[62] headset computer was designed for use in the field by industrial and military mechanics, utility technicians, manufacturing workers and engineers.[63]
Some police forces in Canada have undertaken pilot projects with various body worn video cameras, such as in Victoria in 2009[64] and Edmonton in 2012.[65]

2. Overview of implications for privacy

In a recent industry-funded opinion survey on the social implications of wearable computing in the UK and US, 51% of respondents cited privacy as a barrier to adoption and 62% thought Google Glass and other wearable devices should be regulated in some form, while 20% called for these devices to be banned entirely.[66]
Forrester Research has concluded that fulfilling the promise of wearable computing is dependent on putting users in control of their own data, such as being able to choose whether to share it or not.[67]

a) Challenges to the existing consent model

Information collected by sensors within objects that are connected to each other, whether those objects are worn by individuals or simply carried with them, can yield a tremendous amount of data that can be combined, analyzed and acted upon without adequate transparency, accountability or meaningful consent.
These developments pose profound challenges to the existing privacy frameworks around the world. For example, the purpose limitation principle intended to limit the collection of personal information, subject to consent being given for those specific purposes, is becoming increasingly difficult to apply in a world of ubiquitous computing and mobile devices. Moreover, as the OPC set out in its guidance to mobile app developers, it remains a challenge to obtain meaningful consent through mobile devices.[68] More needs to be done to show users, in a creative and meaningful way, what is actually happening with their personal information.

b) New surveillance options

As we have seen, some wearable computing devices gather photos, videos, sounds, locations and record the general environment around the device, including nearby people and other devices. The camera in several of these devices is the source of many privacy concerns.[69] Inexpensive, versatile, everyday items, such as baseball caps,[70] MP3 music players[71] and shirt buttons,[72] are available in Canada with James Bond-style hidden cameras.[73] Many of these devices have the ability to record constantly and covertly.

Beyond the camera however, the new generation of fitness tracking technology is set to provide health insurance companies and employers with new insights into our health and behaviours. For example, the Heart & Stroke Foundation has partnered with Desjardins Insurance to launch a suite of digital tools designed to help users reduce their risk of stroke.[74] In the workplace, wearable computing products are being marketed to employers as a way to curb costs related to employee mental and physical health. The Canadian company Sprout cites several Canadian clients for its employee activity tracking program in support of corporate occupational health and wellness initiatives.[75] In the US, Empatica's[76] advertising video explains that its emotion-monitoring product is being used in corporate wellness programs in the US: a wristband gathers information about blood pressure, skin conductivity, body temperature, and body movement in real time.[77]

The data is to be collected through the user's smartphone and then analyzed to show which activities lead to stress and the locations where the stress is generated.

We can expect more developments of this nature. The emerging field of "physiolytics" will link wearable devices with big data analytics to provide feedback and a suggestion system for behavioural change.[78]

c) Aggregating data from wearable computing devices

As we saw with the OPC's research on predictive analytics,[79] 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. It is already challenging for individuals to make informed judgments about whether to disclose personal information, as they are not in a position to fully understand how their information may be combined and used in the future. Wearable computing devices that are constantly collecting, processing and sending data are likely to compound this problem.[80]


Source: Shutterstock

Wearable computing devices may also change the ways organizations approach the expansion of their customer base. For example, Forrester Research advises that marketers should avoid using wearable devices to reach new customers and focus instead on using them to deepen engagement with their existing customers. Forrester cautions that marketers need to make responsible use of information collected from sensors in their ongoing efforts to anticipate and respond to customer moods and needs even before they are expressed.[81]

d) Accelerating "context collapse"

Individuals try to maintain distinctions between different spheres of their lives, whether it is among different social circles that they inhabit or simply between work and home life. Social media and the online environment generally have been undermining our ability to maintain tidy distinctions between the spheres. The dissolving of these distinctions, which social scientists have referred to as "context collapse,"[82] may be exaggerated and accelerated as a result of sensors that are always on and always interacting with the user's body and other devices in the user's environment.

e) Opportunities to increase autonomy and control

There are some promising developments in the wearable computing landscape that may serve to enhance autonomy if they are championed as part of the design process. For example, the opportunity to filter out parts of the user's environment as experienced through the device could enhance user autonomy.[83] By filtering advertising to only those advertisements that the user wishes to be shown, in the way they want to receive them, wearable computing devices could create a more comfortable environment that the user can design and control. For example, programs to "delete" on-camera objects in real-time could be used to remove advertising from the information that we are shown through the device.[84] Eyeglasses could filter out unwanted advertising, overwriting that space with data that is useful and desirable to the individual, such as directions.[85]

f) New authentication methods, new personal information

Wearable computing may be configured to manage personal information in a way that protects privacy and security. For example, research is underway to combine data generated by sensors within the current

generation of smart phones so as to identify and authenticate individuals, just by having the smart phone in a pocket as those individuals go about their daily activities.[86]

This means that simply walking, jogging, climbing and going down stairs with a smart phone in a pocket all have the potential to create biometric signatures of the user. While this creates the potential to improve security by means of authenticating the user, it also creates new privacy risks.

3. Canada's privacy laws and wearable computing

Real-time information about someone's mood, physical fitness and health status are likely to be captured by the definition of personal information. We know that combining disparate bits of information, derived from multiple sources, can lead to detailed profiles that could identify individuals. The Federal Court has ruled[87] 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. The OPC has also made the case that powerful insights about an individual can be gleaned from subscriber information[88] and this analysis provides some important points to reflect upon in considering the wearable environment.

a) Wearable computing and the *Privacy Act*

Under the *Privacy Act*, federal government institutions can only collect personal information if it relates directly to an operating program or activity. They can only use personal information for the purpose for which the information was collected or for a use consistent with that purpose. Apart from some limited and specific exceptions, the consent of the individual must be obtained for any other use of the information collected by means of a wearable device.

Wherever federal departments intend to make use of wearable computing devices to collect personal information, they will need to ensure that their program activities are carried out in accordance with the *Privacy Act,* undertake Privacy Impact Assessments (PIAs) and establish privacy protocols for conducting research, audits and evaluations, in accordance with Treasury Board directives and policies.[89]

A recent Parliamentary Committee report

In 2012, the Standing Committee on Public Safety and National Security released a report[90] on the effectiveness, cost efficiency, and implementation readiness of electronic monitoring in the context of specific offender and immigrant populations. Witnesses before the Committee advised of electronic monitoring in these settings using biometric devices as well as bracelets fitted with radio frequency transmitters.
In its response[91] to the Committee's report, the government advised that Correctional Service of Canada planned to implement a second, expanded, electronic monitoring pilot project in 2013. The project description and the privacy risk mitigation measures for this phase of the project are now available online.[92]

The government's response to the Committee's report also explained that electronic monitoring was in use for several individuals subject to long-term security certificates and that the Immigration and Refugee Board had in the past also ordered electronic monitoring in a few cases as a condition of release. The government's response also noted that Canada Border Service Agency would be undertaking a study of the risks and benefits of implementing broader electronic monitoring programs in the context of immigration by examining the experience of the United States and United Kingdom in this area. Aspects of this project have been discussed in the media.[93]

The regulation of medical devices

It is worth noting that Health Canada already regulates many types of medical devices, such as automatic blood pressure monitors, blood glucose monitors and hearing aids, which currently must have a Canadian medical device license before they can legally be sold in Canada.[94] New wearable computing devices that feature software, advanced materials, microelectronics and biotechnology[95] could be captured by aspects of the existing regulatory regime of the *Medical Devices Regulations* under the *Food and Drugs Act.* The scope of wearable devices that could be subject to these regulations could broaden as the line between health monitoring and interventionist medical devices becomes less defined. Health Canada may also need to collect personal information in, for example, reporting of adverse events and problems with such medical devices.[96]

b) Wearable Computing and the *Personal Information Protection and Electronic Documents Act (PIPEDA)*

Wearable computing may pose challenges to *PIPEDA*'s privacy framework that are very similar to those already being faced in the mobile and online environment generally. A central feature of the debate on this issue seems to be the very small cameras that some wearable devices offer and, in particular, with respect to information collected by individual users about other individuals for personal purposes. Under these specific circumstances, *PIPEDA* may not have much to say.

PIPEDA specifically does not apply to "any individual in respect of personal information that the individual collects, uses or discloses for personal or domestic purposes and does not collect, use or disclose for any other purpose."[97] By virtue of this exception, *PIPEDA* may not apply to audio and video recordings made by individuals about other individuals and posted online.[98] The federal government has recently proposed measures to address an aspect of this issue, the non-consensual distribution of intimate images.[99] *PIPEDA* could be engaged where personal information from the user's device is sent on to organizations that collect, use and disclose personal information in the course of commercial activities. For example, in the recent letter[100] to Google on Glass, data protection authorities asked what information Google collects by means of the device when it is used by individual users and with whom that information would be shared. Google's reply focused on selected issues of user control and a commitment not to deploy facial recognition applications for Glass at this time.[101]

Employees of federally-regulated organizations may be in a position to use head-mounted wearable devices in their daily work. Employers who collect or use this employee-generated data could potentially contravene *PIPEDA*'s consent and transparency requirements if they capture personal information of individuals or customers too broadly, without appropriate knowledge and consent.[102] Perhaps these devices will also be configured to monitor and report on employee stress levels and emotions, as the Empatica product would do. Such information would likely capture personal information and engage several *PIPEDA*-related obligations. Fundamentally, the question to consider is whether such a collection would only be for purposes that a reasonable person would consider appropriate in the circumstances.

A recent technical study by the US-based Privacy Rights Clearinghouse on 43 popular health and fitness mobile apps drew some interesting conclusions about privacy and business models that are relevant to the application of *PIPEDA*. The study found that 72% of the apps studied were a moderate or high risk to privacy, concluding that "the apps which presented the lowest privacy risk to users were paid apps. This is primarily due to the fact that they don't rely solely on advertising to make money, which means the data is *(sic)* less likely to be available to other parties."[103] This dynamic underpins a number of the privacy issues in the mobile

and online environments and will extend to challenges that we can expect with wearable devices. Many of the recommendations OPC makes in its guidance for mobile application developers,[104] its fact sheet on gaming consoles,[105] and in its policy position on online behavioural advertising[106] are relevant in the context of wearable computing as well.

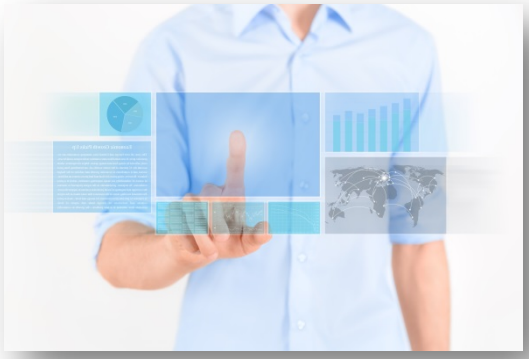
4. Some design considerations for wearable computing devices

Certain fair information principles stand out as deserving of special attention for protecting privacy in the wearable computing environment. Maintaining a technology-neutral approach to privacy protection will be important as the characteristics of today's wearable computing devices evolve in tandem with the Internet of Things.

a) Dynamic User Control

Binary, one-time consent and traditional definitions of personal information are increasingly perceived as outdated. For example, the International Institute of Communications undertook a qualitative research study[107] in 2012 to establish mental models on personal data management. The study, which included some Canadian participants, concluded that simplistic, "on/off" personal data management policies are neither flexible, nor appropriate, in the fast-developing online environment.[108] This study also found that the current approach to looking at information as falling inside or outside the ambit of data protection law, depending on whether it meets the test of personal information, was seen as too simplistic and, rather, a graduated or progressive system of control should be provided to the user.[109]

Current thinking on the concept of privacy suggests that it should be thought of as a dynamic condition because the individual's social and cultural environment is constantly changing.[110] A constellation of creative options needs to be explored to make consent more meaningful, appropriate to changing circumstances and preferences and to minimize decision overload in the wearable computing environment. The options outlined here extrapolate from the work of privacy experts such as Solove,[111] Calo,[112] Nissenbaum,[113] Tene,[114] Bailey,[115] Kerr,[116] and Sweeney.[117] For example, work should be done to:



Source: Shutterstock

- develop dynamically calibrated privacy rules to meet individuals' privacy needs and expectations;
- integrate simple design features so that the wearable device can reflect individual privacy preferences, and
- call on organizations to enhance their privacy policies with dynamic and interactive data maps[118] and infographics to show relationships in the wearable computing device ecosystem.

Another feature of wearable computing is that it may be able to selectively *decrease* or simplify the information the user receives, in a way of the user's choosing. Concepts like this one have the potential to be a real opportunity for privacy protection, in a way applying concepts from the "do not track" online privacy debate to the wearable computing environment. The example that was mentioned earlier, of programs that can "delete" on-camera objects in real-time, could be used to remove advertising from the information that individuals are shown through the device and could also limit the information otherwise destined for third parties.[119]

Some other models for enhancing user control over facial recognition features are being explored at this time. For example, the Article 29 Data Protection Working Party has recommended that an organization may collect someone's digital image to determine whether that individual has already granted the organization the permission to collect it and, if no such consent has been granted, the organization must delete the image.[120]

The design requirements for interacting with the wearable device will impact on the user's privacy. For example, a wearable device that relies on voice commands creates a similar privacy issue to holding a phone conversation in public. The individual's ability to modify behaviour, perhaps switching the conversation from audio to text would be an interesting design adaptation to enhance privacy.

b) Evolving transparency models

There are opportunities and challenges for transparency in the wearable computing context. For example, wearable devices that use vision, hearing or other senses may be more tightly integrated with the user, so it may be easier in some ways to get the user's immediate attention. In this way, making consent and notice "visceral"[121] in the design of a wearable device may be easier than on a smart phone. The design of some wearable computing devices do not require screens at all, so new models for negotiating privacy with users will need to be developed.

User privacy is one issue but the privacy of those around the user is another, and perhaps more vexing, problem. It is already difficult to know when someone is using a smart phone or other device to capture audio or video. With wearable computing devices, where the computers become more seamlessly integrated into unremarkable items, such as frames for everyday eyeglasses, this greatly diminish others' ability to know and control the collection of information about them.

c) Access to data and challenging accuracy in automated decision-making

Squarely related to transparency is the issue of access to personal information. It is not obvious how individuals will be able to determine what is collected by a wearable device and know what is being used and disclosed. Users will need a way to challenge the personal information gathered and used by organizations as a foundation for their decisions, as accuracy is not guaranteed.

A recent study of some fitness-related wearable devices questioned the reliability of tracking the energy costs of light-intensity activities like standing or cleaning.[122] Inaccuracies in capturing these kinds of data could have real implications for individuals using these devices. For example, inaccurate readings from a new early detection method for Alzheimer's disease, involving the assessment of patient movements by means of an accelerometer,[123] could impact patient diagnosis and care. Inaccurate readings could also create issues in the workplace if an employer were to rely on these devices to monitor aspects of employee productivity. Ensuring individuals have a way to launch a meaningful challenge to the accuracy of the data generated, or the analysis that is done, would be an important design feature based on data collected by a wearable device.

d) Security vulnerabilities

Wearable computing devices without proper security and authentication systems in place are vulnerable to attack.[124] Compromised wearable computing devices can put not only the individual's personal information and reputation at risk but their health as well. For example, eavesdropping and impersonation of a wearable device charged with regulating insulin could result in dire consequences for the individual's health.[125] As one commentator expressed it, "your personal data security is only as strong as the weakest link in your quantified self ecosystem."[126]

Conclusion

There is little debate that wearable computing will become a much more prominent feature of our daily lives. In McKinsey Global Institute's May 2013 report on disruptive technologies,[127] six of the twelve identified technologies are already clearly part of the wearable computing landscape: inexpensive mobile computing, intelligent software systems, low-cost sensors, cloud technology, advanced energy storage and advance materials.

Wearable computing is a significant development in its own right; however, it would be a mistake to study it in isolation. Its true significance for the privacy landscape will be revealed when its capabilities are combined with other innovations shaping our world today that also track our activities, movements, behaviours and preferences. This trend may well affect our private lives, but our workplaces as well. For example, Hitachi's Business Microscope[128] identity badge, which contains embedded infrared sensors, an accelerometer and a microphone sensor, purports to capture the interaction patterns in the workplace but also the *quality* of employee collaboration. Monitoring of our emotions, health status and the quality of our human interactions strikes at the very core of our most intimate selves.

Once the stuff of science fiction, integration of cameras and sensors *within* the body also seems likely, particularly where there is a need to supplement or augment human functions. For example, researchers at Princeton University have used 3-D printing tools to merge electronics with tissue to create a functional ear that can "hear" radio frequencies far beyond the range of normal human capability.[129] In the field of epidermal electronics,[130] health-monitoring devices mounted onto human skin, like temporary tattoos, are being developed to diagnose and monitor conditions like heart arrhythmia or sleep disorders noninvasively. The US Navy is looking at next-generation bio-monitors, in the form of temporary tattoos, to track soldiers' stress indicators such as heart-rate, temperature or bio-electric response during various training situations.[131]

Examples like these demonstrate just how deeply integrated wearable technologies can become with our bodies and minds. They pose profound changes for the ways we can be tracked and evaluated by others. While wearable computing technologies have the potential to improve the lives of many people, the potential for social upheaval and surveillance remains profound.

Addressing the privacy challenges posed by wearable technology

Given the pervasive yet nearly imperceptible potential for surveillance, the need for transparency has never been greater. Individuals can ask questions and challenge surveillance when they know or suspect that it is taking place. However, when wearable sensors are tiny, silent and embedded in everyday items such as clothing,[132] there is no obvious trigger for inquiry or challenge.

If transparency with respect to tracking by wearable computing devices is significant for our relationship with the private sector, it is equally important in our relationship with government. Revelations on the national security front[133] show that the personal information collected by the private sector plays a crucial role in the surveillance ecosystem. It should not be surprising that the richness of information gleaned from wearable devices might attract intelligence agencies and governments.

While wearable computing ushers in a whole new generation of privacy risks, it also offers a tremendous opportunity for enhancing privacy protection and user autonomy. Creative ways of engaging more of our senses could provide users with new ways to provide feedback and choice about privacy preferences; it would be beneficial to minimize the decision overload, which typifies today's text-based privacy policies and binary, static consent practices.

Challenges to privacy originating from both the public and private sectors will only intensify in years to come. These technologies all have the potential to benefit society but the privacy risks remain challenging and difficult to predict, even in the short term. Market assessments all point to increased consumer adoption. Greater transparency, innovative technological solutions and active public engagement on these issues are necessary if privacy protection is to keep pace with, and become an integral part of, the wearable computing revolution.

Notes

[1] The scope of this research report is limited to wearable devices worn on the outside of the body, and not implants, as they pose a host of additional privacy challenges. Selected tags: anticipatory marketing, assistive technology, BodyMedia FIT, context collapse, digital medicines, Digits, Empatica, epidermal electronics, FitBit, FuelBand, Google Glass, HC1, implantable telescope, Innovega iOptik, intelligent digital assistants, iWatch, Jawbone UP, Kopin Golden-I, GoPro, Leap Motion, lifebands, LifeBoard, Memoto, MYO armband, Oculus Rift, OrCam, Pebble, physiolytics, Proteus Digital Health, Raytheon Aviation Warrior, Recon Jet, Shine, Steve Mann, Thalmic Labs, Tieex spy watch DVR, Vital Connect HealthPatch, Vuzix Smart Glasses M100, wearable computing.

[2] Office of the Privacy Commissioner of Canada. "Drones in Canada: Will the proliferation of domestic drone use in Canada raise new concerns for privacy?" March 2013.

[3] Donald Melanson and Michael Gorman, "Our augmented selves: The promise of wearable computing." Engadget. December 12, 2012. Retrieved on July 8, 2013.

[4] Marcelo Ballvé, Wearable Computing: From Fitness Bands To Smart Eyewear, A New Mobile Market Takes Shape, *BI Intelligence*, 2013.

[5] Office of the Privacy Commissioner of Canada. "Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps."October 2012

[6] Steve Mann, (1996a): Smart Clothing: The Shift to Wearable Computing. In Communications of the ACM, 39 (8) pp. 23-24. See Mann, Steve (2013): Wearable Computing. In: Soegaard, Mads and Dam, Rikke Friis (eds.). *The Encyclopedia of Human-Computer Interaction*, 2nd Ed. Aarhus, Denmark: The Interaction Design Foundation. Retrieved on June 14, 2013.

[7] "Wearable Technology Market - Global Scenario, Trends, Industry Analysis, Size, Share And Forecast, 2012 – 2018." *Market Research Reports Biz*. January 2013. Retrieved June 13, 2013.

[8] Emily Waltz, "How I Quantified Myself: Can self-measurement gadgets help us live healthier and better lives?" IEEE Spectrum, August 30, 2012. As referenced in Steve Mann. "Steve Mann: My "Augmediated" Life." *IEEE Spectrum*. March 1, 2013. Retrieved on June 14, 2013.

[9] See Vital Connect's HealthPatch. Viewed on January 6, 2014.

[10] Tom Ryan, "Will tech wearables go mainstream?" *RetailWire*, January 14, 2014. Retrieved April 22, 2014.

[11] For example, see Misfit Wearables as referenced by Jennifer Darmour in"3 Ways To Make Wearable Tech Actually Wearable." *Fast Company*, March 15, 2013. Retrieved on June 12, 2013.

[12] Smart Glasses and Other Wearable Devices to be worth over $1.5bn by 2014, finds Juniper. Juniper Research Press Release, October 31, 2012. Retrieved on July 17, 2013.

[13] *World Market for Wearable Technology – A Quantitative Market Assessment – 2012,* IMS Research, August 2012 as discussed in Wearable Computing Devices, Like Apple's iWatch, Will Exceed 485 Million Annual Shipments by 2018, ABI Research, February 21, 2013. Retrieved on July 10, 2013.
[14] Wearable Computing Devices, Like Apple's iWatch, Will Exceed 485 Million Annual Shipments by 2018, ABI Research, February 21, 2013. Retrieved on July 10, 2013.
[15] Marcelo Ballvé, Wearable Computing: From Fitness Bands To Smart Eyewear, A New Mobile Market Takes Shape, BI Intelligence, April 2013. Retrieved on July 10, 2013.
[16] Donald Melanson and Michael Gorman, "Our augmented selves: The promise of wearable computing." Engadget. December 12, 2012. Retrieved on July 8, 2013.
[17] Christina Warren. "Why the iPhone Was Truly a Disruptive Product," *Mashable*, June 29, 2012. Retrieved on July 16, 2013.
[18] Charles Arthur, "Apple applies for iWatch trademark." *The Guardian*. July 1, 2013. Retrieved on July 16, 2013.
[19] "Apple hires Yves Saint Laurent CEO, stoking rumours of wearable device." *CBC News*. July 3, 2013. Retrieved on July 16, 2013.
[20] Steve Mann, (2013): Wearable Computing. In: Soegaard, Mads and Dam, Rikke Friis (eds.). *The Encyclopedia of Human-Computer Interaction*, 2nd Ed. Aarhus, Denmark: The Interaction Design Foundation.
[21] While commercially available implantable vision aids, such as the "implantable telescope" for people with age-related macular degeneration, are beyond the scope of this paper, it is important to recognize the much broader reach of advances in other forms of assistive technology for vision impairments. "Implantable Telescope Lens to Treat Macular Degeneration Available at Johns Hopkins." News Release. *Johns Hopkins Medicine*. March 21, 2013. Retrieved June 12, 2013.
[22] Sunir Garg, "Retinal Prostheses Offer Hope to Blind Patients." *Review of Ophthalmology*. March 15, 2013. Retrieved on June 14, 2013.
[23] Orcam device web site.
[24] John Markoff, "Device From Israeli Start-Up Gives the Visually Impaired a Way to Read." *The New York Times*. June 3, 2013, Retrieved on June 13, 2013.
[25] "iOptik augmented reality contact lens prototype to be unveiled at CES," *Gizmag*, January 6, 2014. Retrieved January 7, 2014.
[26] Steve Mann has been developing this sort of computing eyewear for thirty-five years Steve Mann, "Steve Mann: My "Augmediated" Life." *IEEE Spectrum*. March 1, 2013. Retrieved on June 14, 2013.
[27] Steve Mann, Raymond Chun Hing Lo, Kalin Ovtcharov, Shixiang Gu, David Dai, Calvin Ngan, Tao Ai, "Realtime HDR (High Dynamic Range) Video for EyeTap Wearable Computers, FPGA-based Seeing Aids, and Glasses (EyeTaps)." 2012 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE). Retrieved on June 24, 2013.
[28] Michael W. Boyce and P.A Hancock, "The Interpenetration of Mind and Machine." *Proceedings of the Human Factors and Ergonomics Society 56th Annual Meeting*, 2012, 56: 178. Retrieved June 11, 2013.
[29] LifeBoard for Gi-OS. Retrieved on June 24, 2013.
[30] "IBM's Watson Now A Customer Service Agent, Coming To Smartphones Soon," *Forbes*, May 21, 2013. Retrieved on July 15, 2013.
[31] Narrative Clip.
[32] Valencell, "PerformTek® Precision Biometrics: Engaging the Burgeoning Mobile Health and Fitness Market," White Paper. January 2013. Retrieved June 17, 2013
[33] Nike+ FuelBand.
[34] Fitbit is not yet shipping to Canada.
[35] BodyMedia FIT, web site indicates product can be shipped to Canada.

[36] Jawbone UP.
[37] PerformTek® Sensor Technology and Bryon Moyer, "You Put That Where?" *Electrical Engineering Journal* blog. February 5, 2013. Retrieved June 17, 2013.
[38] Pebble.
[39] Galaxy Gear.
[40] "GoPro's video revolution." *60 Minutes*. November 10, 2013.
[41] Google Glass.
[42] "Data protection authorities urge Google to address Google Glass concerns." News Release, Office of the Privacy Commissioner of Canada. June 18, 2013. Retrieved on June 24, 2013.
[43] "Vuzix M100 Production Model Shipping to Developers and Available for General Pre-Order." Press release. Retrieved on December 30, 2013.
[44] Recon Instruments. Retrieved on December 30, 2013.
[45] Oculus Rift.
[46] Paul Marks, "Muscle-zapper forces gamers' own hands against them," *New Scientist*, Magazine issue 2902, January 31, 2013. Retrieved on June 11, 2013.
[47] P. Lopes and Baudisch, P. "Muscle-Propelled Force Feedback: Bringing Force Feedback to Mobile Devices." *CHI 2013: Changing Perspectives*, Paris, France. CHI 13, April 27 – May 2, 2013, Paris, France. Retrieved on June 11, 2013.
[48] Sarah Mitroff, "Your Next Computer Will Live on Your Arm," WIRED, February 25, 2013, Retrieved on July 8, 2013.
[49] See "The Hottest Global Startups Of 2013," Forbes, December 16, 2013 and Thalmic Labs. Retrieved on January 6, 2014.
[50] Microsoft Research Digits. Accessed January 6, 2014.
[51] Will Knight, "What Comes After the Touch Screen?" MIT Technology Review, October 11, 2012. Retrieved July 7, 2013.
[52] See Leap Motion's web site.
[53] Health apps, virtual visits and remote monitoring – Canadians looking to manage their health one click at a time: PwC report. PwC press release, June 4, 2013, Retrieved on July 19, 2013.
[54] 2013 Canadian Telehealth Report (based on the 2012 Canadian Telehealth Survey), Updated to June 2013. Retrieved on December 30, 2013.
[55] Introducing our smart contact lens project, *Google Official Blog*, January 16, 2014. Retrieved on January 24, 2014.
[56] Proteus Digital Health.
[57] Erin Kim, "'Digital pill' with chip inside gets FDA green light." *CNNMoney*, August 3, 2012. Retrieved on July 17, 2013.
[58] Proteus' Digital Feedback System.
[59] See summary of How Wireless Therapy Will Change Health Care Delivery on Proteus' publications page.
[60] Raytheon's Aviation Warrior and Donna Tam,"Pilot of the Future: U.S. Army gets wearable tech for the battlefield."*CNET News*. July 8, 2012. Retrieved on June 24, 2013.
[61] Kopin Corporation's Golden-i site.
[62] Motorola HC1 Headset Computer Specification Sheet. Retrieved on June 24, 2013.
[63] Also see Motorola's Hands-Free Mobile Computing: Increase Productivity with Motorola Solutions Wearable Portfolio. Retrieved June 27, 2013.
[64] *BCCLA Says Police "Body-Worn" Video Cameras Not About Police Accountability*, British Columbia Civil Liberties Association, June 30, 20009. Retrieved on July 9, 2013.
[65] "Edmonton police to test body cameras," CBC News Edmonton, October 9, 2012. Retrieved on July 9, 2013.

[66] *"The Human Cloud: Wearable Technology from Novelty to Productivity,"* Commissioned by Rackspace in association with the Centre for Creative and Social Technology (CAST) at Goldsmiths, University of London. June 5, 2013. Retrieved June 12, 2013.
[67] Sarah Rotman Epps, "Smart Body, Smart World: The Next Phase of Personal Computing." *All Things D*, October 29, 2012, Retrieved June 12, 2013.
[68] Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps. OPC Guidance document, October 2012.
[69] Donald Melanson and Michael Gorman, "Our augmented selves: The promise of wearable computing." Engadget. December 12, 2012. Retrieved on July 8, 2013.
[70] See baseball cap camera product description.
[71] See MP3 player hidden camera product description.
[72] See button camera product description.
[73] In a recent UK court case, a hidden camera inside a wristwatch was used to record examinations of the physician's female patients. According to media reports, the physician used a Tieex 4GB Waterproof HD Spy Watch DVR which looks like any other men's sports watch. "12 years for GP who filmed sex assaults on female patients with James Bond-style watch," *London Evening Standard*, May 23, 2012. Retrieved on June 10, 2013.
[74] Heart & Stroke eTools as discussed in "How insurers are turning to fitness apps to decide your health coverage," *The Globe and Mail*, December 19, 2013.
[75] Sprout. Accessed on January 3, 2014.
[76] Empatica. Accessed on January 3, 2014.
[77] Amir Muaremi, Bert Arnrich and Gerhard Tröster. "Towards Measuring Stress with Smartphones and Wearable Devices During Workday and Sleep," *BioNanoScience*. May 8, 2013, p.182. Retrieved on June 17, 2013.
[78] H. James Wilson, Wearables in the Workplace. *Harvard Business Review*, September 2013.
[79] Paul.M Schwartz, *Data Protection Law and the Ethical Use of Analytics*. The Centre for Information Policy Leadership Hunton & Williams LLP 2010 as referenced in Erin Courtland, "The Age of Predictive Analytics: From Patterns to Predictions, rdims #350219, August 2012.
[80] Daniel J. Solove, Privacy Self-Management and the Consent Dilemma (November 4, 2012). *126 Harvard Law Review 1880* (2013); GWU Legal Studies Research Paper No. 2012-141; GWU Law School Public Law Research Paper No. 2012-141. Retrieved June 19, 2013.
[81] Sarah Rotman Epps, "Smart Marketing In A Sensor-Laden World." *Forbes*, April 18, 2013. Retrieved on June 12, 2013.
[82] See, for example, Alice Marwick and danah boyd, "I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience," *New Media & Society*, February 2011, vol. 13, no. 1 114-133 and Carolyn Marvin, Your smart phones are hot pockets to us: Context collapse in a mobilized age. *Mobile Media & Communication* 2013 1: 153. Retrieved on August 22, 2013.
[83] As well, the controls imposed through digital rights management and end-user license agreements for wearable computing devices all have the potential to diminish individual control and autonomy. Jane Bailey and Ian Kerr, Seizing Control?: The Experience Capture Experiments of Ringley & Mann, 9 *Ethics & Information Technology.*, No. 2, 2007, pp. 129-139.
[84] Paul Miller, "Project Glass and the epic history of wearable computers: How we've tried to become more than human." *The Verge*, June 26, 2012. Retrieved on June 24, 2013.
[85] Steve Mann, (2013): Wearable Computing. In: Soegaard, Mads and Dam, Rikke Friis (eds.). *The Encyclopedia of Human-Computer Interaction*, 2nd Ed. Aarhus, Denmark: The Interaction Design Foundation.

[86] Jennifer R. Kwapisz, Gary M. Weiss, and Samuel A. Moore. "Cell Phone-Based Biometric Identification." Biometrics: Theory Applications and Systems (BTAS), *2010 Fourth IEEE International Conference*, 27-29 Sept. 2010.
[87] Gordon v. Canada (Health), 2008 FC 258 (CanLII), Retrieved on July 22, 2013.
[88] 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. Retrieved on June 24, 2013.
[89] TBS Directive on Privacy Impact Assessment and *Policy on Privacy Protection*.
[90] "A Study of Electronic Monitoring in the Correctional and Immigration Settings." Sixth Report of the Standing Committee on Public Safety and National Security, September 2012. Retrieved on August 23, 2013.
[91] Government response to the recommendations of the Sixth Report of the Standing Committee on Public Safety and National Security: "A Study of Electronic Monitoring in the Correctional and Immigration Settings." Public Safety Minister Vic Toews, January 28, 2013. Retrieved on August 23, 2013.
[92] Electronic Monitoring Pilot II (EM - PII), Correctional Service of Canada. Retrieved on January 2, 2014.
[93] "Canada looks to put GPS bracelets on more migrants," *Globe and Mail* online, June 27, 2013. Retrieved on January 3, 2014.
[94] "Buying medical devices from the Internet: It's your health." Health Canada fact sheet. Retrieved on June 24, 2013.
[95] Medical Device Industry Profile 2013. Industry Canada. Retrieved January 2, 2014.
[96] Adverse Reaction and Medical Device Problem Reporting. Health Canada. Retrieved on July 19, 2013.
[97] See section 4(2)(b) of PIPEDA.
[98] Teresa Scassa, "Google Glass and the Privacy Gap," Blog post. June 19, 2013. Retrieved on June 19, 2013.
[99] Bill C-13, *"Protecting Canadians from Online Crime Act*". Retrieved on January 2, 2014.
[100] *Data protection authorities urge Google to address Google Glass concerns*. News Release on letter to Google. OPC and 36 of the Commissioner's provincial and international counterparts. June 18, 2013.
[101] Response from Google to data protection authorities regarding Google Glass. Peter Fleischer, Global Privacy Counsel, Google, June 27, 2013.
[102] *Captured on Camera: Street-level imaging technology, the Internet and you*. Fact Sheet prepared jointly by the Offices of the Information and Privacy Commissioners of Alberta and British Colombia and the Commission d'accès à l'information du Québec, and the Privacy Commissioner of Canada (OPC).
[103] Privacy Rights Clearinghouse Releases Study: Mobile Health and Fitness Apps: What Are the Privacy Risks? News Release, posted July 15, 2013. Retrieved on July 17, 2013.
[104] Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps. OPC Guidance document, October 2012.
[105] Gaming consoles and personal information: playing with privacy. OPC Guidance document. November 2012.
[106] Policy Position on Online Behavioural Advertising. OPC policy position. June 2012.
[107] Personal Data Management: The User's Perspective. *International Institute of Communications*. (Research was commissioned by the International Institute of Communications from IPSOS UU between March-August 2012, funded by the Microsoft Corporation.) November 22, 2012, p. 9. Retrieved on June 17, 2013.
[108] Personal Data Management: The User's Perspective. *International Institute of Communications*. November 22, 2012, p.9. Retrieved on June 17, 2013.
[109] Personal Data Management: The User's Perspective. *International Institute of Communications*. November 22, 2012, p.37. Retrieved on June 17, 2013.
[110] Julie E. Cohen, What Privacy Is For, 126 *Harvard Law Review*. 2013, p.1906.

[111] Daniel J. Solove, Privacy Self-Management and the Consent Dilemma (November 4, 2012). *126 Harvard Law Review 1880* (2013); GWU Legal Studies Research Paper No. 2012-141; GWU Law School Public Law Research Paper No. 2012-141. Retrieved June 19, 2013.
[112] M. Ryan Calo, Against Notice Skepticism in Privacy (and Elsewhere), *87 Notre Dame L. Rev. 1027*, 1033 (2012)
[113] Nissenbaum, Helen. 2009. Privacy In Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press.
[114] Omer Tene, "Privacy: The New Generations," *International Data Protection Law*, 2010.
[115] Jane Bailey and Ian Kerr, Seizing Control?: The Experience Capture Experiments of Ringley & Mann, 9 *Ethics & Information Technology.*, No. 2, 2007, pp. 129-139.
[116] Jane Bailey and Ian Kerr, Seizing Control?: The Experience Capture Experiments of Ringley & Mann, 9 *Ethics & Information Technology.*, No. 2, 2007, pp. 129-139.
[117] The online DataMap project.
[118] See, for example, theDataMap online portal.
[119] Paul Miller, "Project Glass and the epic history of wearable computers: How we've tried to become more than human." *The Verge*, June 26, 2012. Retrieved on June 24, 2013.
[120] See Recommendation 5 in *Opinion 02/2012 on facial recognition in online and mobile services*. Article 29 Data Protection Working Party. 00727/12/EN WP 192. Retrieved on July 16, 2013.
[121] M. Ryan Calo, Against Notice Skepticism in Privacy (and Elsewhere), *87 Notre Dame L. Rev. 1027*, 1033 (2012)
[122] KL Dannecker, Sazonova NA, Melanson EL, Sazonov ES, Browning RC. "A Comparison of Energy Expenditure Estimation of Several Physical Activity Monitors." *Medicine & Science in Sports & Exercise*. 2013 May 10 as discussed in Reynolds, Gretchen. "How Accurate Are Fitness Trackers?" *The New York Times*. June 12, 2013. Retrieved on June 12, 2013.
[123] Thomas Kirste, André Hoffmeyer, Philipp Koldrack, Alexandra Bauer, Susanne Schubert, Stefan Schröder and Stefan Teipel. "Detecting the Effect of Alzheimer's Disease on Everyday Motion Behavior," *Journal of Alzheimer's Disease.* Vol. 38, No. 1, 2014.
[124] The US Federal Drug Administration issued cybersecurity guidance for networked medical devices containing off-the-shelf software in 2005.*Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software*. US Federal Drug Administration. January 14, 2005. Retrieved on July 19, 2013.
[125] Li Chunxiao, Anand Raghunathan and Niraj K. Jha. "Hijacking an Insulin Pump: Security Attacks and Defenses for a Diabetes Therapy System." *2011 IEEE Conference on e-Health Networking, Applications and Services*.
[126] Michael Carney, "You are your data: The scary future of the quantified self movement." *PandoDaily*. May 20, 2013. Retrieved on June 10, 2013.
[127] 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. May 2013. Retrieved on July 16, 2013.
[128] Hitachi's Business Microscope. Accessed on February 13, 2014. See also: "Wearable Gadgets Transform How Companies Do Business," *The Wall Street Journal*, October 20, 2013.
[129] John Sullivan, "Printable 'bionic' ear melds electronics and biology." *News at Princeton*, May 8, 2013, Retrieved on June 13, 2013.
[130] Woon-Hong Yeo, Yun-Soung Kim, Jongwoo Lee, Abid Ameen, Luke Shi, Ming Li, Shuodao Wang , Rui Ma , Sung Hun Jin, Zhan Kang, Yonggang Huang and John A. Rogers. "Multifunctional Epidermal Electronics Printed Directly Onto the Skin," *Advanced Materials*. 2013, 25, 2773–2778

[131] Nick Stockton, "Pentagon's Mad Scientists Want a Tattoo That Tracks Troops' Vitals." *WIRED Magazine*, March 27, 2013.
[132] See, for example, Cityzen Sciences' smart textiles, which are "embedded with micro-sensors enabling them to monitor temperature, heart rate, speed and acceleration as well as to geolocalise."
[133] *Special Report to Parliament: Checks and Controls: Reinforcing Privacy Protection and Oversight for the Canadian Intelligence Community in an Era of Cyber-Surveillance*, Office of the Privacy Commissioner of Canada. January 28, 2014.