WEARABLE COMPUTING

Mayur Watamble

ABSTRACT:

Wearable devices are a trending topic in both commercial and academic areas. Increasing demand for innovation has led to increased research and new products, addressing new challenges and creating profitable opportunities. However, despite a number of reviews and surveys on wearable computing, a study outlining how this area has recently evolved, which provides a broad and objective view of the main topics addressed by scientists, is lacking. Wearable computing is a new research field which has undergone huge improvements in the last decade and it seems that it will become even more important in the near future. Unfortunately, designing high performance wearable computing devices is not an easy task and its implementation has faced many challenges. This field is an intersection of different research areas such as computer science and engineering using various technologies such as microelectronics and wireless communication. In this we will see an overview of wireless telecommunication technologies that enable the design of wearable computing devices such as Bluetooth, 3G LTE, Wi-Fi, ZigBee and WiMAX are outlined as well.

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*.

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, 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

DOI: 10.55041/IJSREM15287

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. 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 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, 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.

EXISTING TECHNIQUE

Wearable computing is the use of a miniature, body-borne computer or sensory device worn on, over, under or integrated within, clothing. 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, 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;
- infotainment (smart watches, augmented reality headsets, smart glasses);
- healthcare and medical (e.g. continuous glucose monitors, wearable biosensor patches) 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.

PROBLEM STATEMENT

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. 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.

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. 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. Inexpensive, versatile, everyday items, such as baseball caps, MP3 music players and shirt buttons, are available in Canada with James Bond-style hidden cameras. 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. 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. In the US, Empatica's 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. 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.

c) Aggregating data from wearable computing devices

As we saw with the OPC's research on predictive analytics, 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.

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.

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," 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. 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. Eyeglasses could filter out unwanted advertising, overwriting that space with data that is useful and desirable to the individual, such as directions.

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.

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.

PROPOSED METHODOLOGY

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 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. 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.

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. 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, Calo, Nissenbaum, Tene, Bailey, Kerr, and Sweeney. For example, work should be done to:

- 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 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.

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.

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” 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. 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, 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.

Wearable computing devices without proper security and authentication systems in place are vulnerable to attack. 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. As one commentator expressed it, "your personal data security is only as strong as the weakest link in your quantified self ecosystem."

FUTURE SCOPE

We're in a fascinating period when it comes to wearable computers where in both small startups and big-name firms are working on experimentation to tap new markets and convince people to buy the new technologies which could be of immense help to them.

The aim of wearable computing is to design wearables that are either very stylish or invisible. In today's fast moving world besieged with technology all around, there is immense marketplace in a huge country like India.

The need of the hour is to make people aware of the new technologies that are surging in the markets.

For instance, a lot of wearable devices have come up in the market so that the fruits of development may reach out to people which includes Apple testing iWatch, iRing, S6 Golf Watch, Wrist Gear, Sony Smart Band, 3 High-Tech Eye Glasses, Google Glass, Bluetooth Ring, iPhone-Connected Jewelry with wireless security alerts, Smart contact lenses for medical purposes, Smart Eyelashes and Fingernails etc.

CONCLUSION

Wearable computing enables significant new research opportunities in interface, artificial intelligence, and perception. As research into perception and user modeling through devices carried on the body progresses, new intelligent interfaces will result that will reduce work and complexity and lead to new capabilities. However, by simply making eye catching and lucrative wearable technology will not serve the purpose until it reaches out to the massive population and their full market potential is tapped.

REFERENCES

[1] Cliff Randell, Department of computer science, University of Bristol, U.K., Wearable computing: A review, www.cs.bris.ac.uk / Publication/ Papers/2000487.pdf.

[2] DARPA, Proceedings of the Wearables in 2005 Workshop, www.darpa.mil/MTO/Displays/Wear2005/, (1996).

[3] Lind, E.J., Jayaraman, S. Rajamanickam, R., Eisler, R. and McKee, T., A sensate liner for personnel monitoring applications, First

International Symposium on Wearable Computers, (1997), pp 98105.

[4] Mann, S., Mediated reality, Technical Report 260, MIT Media Lab, Perceptual Computing Group, (1994).

[5] Body media Incorporate,4, Smithfied –Street , 11 Floor, Pittsburgh,

PAAI5222,USA,Bodeymedia,productliterature, http://www.bodymedia.com

[6] http://en.wikipedia.org/wiki/Wearable_technology

[7] http://www.wearitatwork.com/home/discovering-ubiquity/

[8] Bradley Rhodes(n.d.)'A brief history of wearable computing', pp.[online].http://www.media.mit.edu/wearables/lizzy/timeline.html #1966a(Accessed:20th june, 2013).

[9] Howard Rheingold(1991)Virtual reality, Rockefeller Center:

Touchstone.

[10] Review of the International Statistical Institute, V. 37:3, 1969.

[11] Wheel of Fortune gambling game in LIFE Magazine, March 27, 1964, pp. 80-91.

[12] "Mobile Studies with a Tactile Imaging Device," C.C. Collins, L.A.

Scadden, and A.B. Alden, Fourth Conference on Systems & Devices for The Disabled, June 1-3, 1977, Seatle WA.

[13] The Eudemonic Pie, Thomas A. Bass, Houghton Mifflin Company, 1985.

[14] The IBM/Columbia Student Electronic Notebook Project, IBM, T. J.

Watson Research Lab., Yorktown Heights, NY, 29 June 1990. [15] Warwick.K, "I,Cyborg", University of Illinois Press, 2004.

[16] http://oldclick.com/news/google/apple-iwatch-or-google-glassfinally-taking-wearable-computing-mainstream/44966/.

[17] Article from the site located at www.ehow.com.

[18] http://www.ihs.com/pdfs/Wearable-Technology-sep-2013.

[19] Mashable.com/category/wearable-tech/

[20] www.wearable-technologies.com/

[21] John Lindström, Lulea University of Technology, Sweden Security challenges for wearable computing a case study. http://pure.ltu.se

[22] http://www.wearitatwork.com

[23] http://www.embs.org/ (medical)

[24] www.sciencedaily.com/news/matter_energy/wearable_technology/

[25] http://www.bostonglobe.com/sports/2014/05/24/sports-wearablesare-wave future/

[26] http://www.wearable.ethz.ch/

[27] http://www.informationweek.com/

[28] http://www.geeksugar.com/Smartwatches-Cars-35039102#photo35039114.

[29] http://www.digitalspy.co.uk/