

Privacy and Security of Wearable Devices

By

Zakaria Alrababah

October 30, 2020

ABSTRACT

This research paper investigates the privacy and security concerns related to wearable technology. The research questions titled “to what extent can the use of wearable devices compromise the privacy and security of the user?” The scope of the research is broad, since it deals with two main ethical concerns. The analysis of the security and the privacy of wearable devices, done by the use of many secondary resources, and some primary research that I have conducted by way of a survey that had around 240 responses by people in the school.

I will be also discussing different privacy and security issues that are common in the use of the current versions of wearable devices; another concept that I will be talking about is the internet of things. In addition, how it can be useful in the implementation of wearable devices.

This paper will also suggest ways that companies can use in order to solve issues related to the privacy and security of their wearable devices, by evaluating different solutions, and stating what the companies need to do in order to protect themselves and their consumers.

I have concluded that the use of wearable devices has many advantages and disadvantages to the user; I have also concluded that security and privacy go hand in hand. Therefore, if the security of the user is at risk, his privacy will be at stake, the conclusion also states that the companies need to solve security issues need to prevent further privacy issues for the consumer.

CHAPTER ONE

INTRODUCTION

Lately the utilization of wearable technology has developed in notoriety, as a result of the advancements seen in the technological world. As more manufacturers start to push towards making modern day processors smaller and more effective, and designing new sensors that can track even more bodily statistics with even greater accuracy, more and more organizations saw this as an opportunity to incorporate technology into our daily items such as clothing and many others.

Security dependability has been a hazard and a very questionable issue as far back as the start of the web, Privacy has likewise been one of the greatest issues in regards to the sharing of data in the web. Wearable technology is not without such concerns, and to some extent, is even a greater concern due to the sensitivity of the data collected by such devices.

There are many types of wearable devices, and to each type a set of concerns and problems that related to it, yet security and privacy are issues that apply to all types of wearable devices, small or big.

The aim throughout this essay is to get a better understanding of the many possibilities in which the wearable technology of today could potentially comprise our own personal security and privacy, while also looking into the ways the companies that manufacture them have taken measures to prevent the possibility of such compromise.

Background of the IT system

Wearable technology, as the name implies, is a type of technology that can be worn on specific parts of the body. These can be best described as a form of mini-computers that have been designed in the shape of wristbands, clips, chest straps, and much more. They are designed to be comfortable to wear for long period of time and can often be designed with materials that are not typically associated with electrical devices, with common materials such as a metal and plastic being replaced with fabric (as seen on the Google Daydream VR headset, where the headset is mostly designed with soft fabric that makes it comfortable to wear for long periods of time) and rubber or silicone (as seen on some notable fitness trackers such as those made by Fitbit and Jawbone).

While worn, they can either help the user in simplifying common tasks or allow the user in performing them in a much more effective manner (e.g. the use of smartwatches for boarding planes in airports).

Lately the utilization of wearable technology has seen an increase, as a due to a direct result of the accessibility of these devices. Furthermore, as manufacturers begin designing components (e.g. CPU's and Batteries) that are smaller and more efficient. This has led to opening possibilities for companies to incorporate IT systems into items that many use on a daily basis (e.g. Watches and Wristbands) that are small and comfortable to wear and use for different people who have different uses for these wearable devices.

The IT System:

The internet of things (IOT)

The internet of things is a topic that is increasing in interest and has been a growing topic in the recent times, since the world is at constant advancements in the terms of technology, IOT can have a huge impact on how we can start to make things together. The internet of things is what allows certain physical objects communicate with the internet, these physical devices are embedded with certain chips that allow the devices to communicate with the internet.

How wearable technology utilizes IOT

It is worth mentioning before diving in deeper into the analysis as how this form of IT system works, it is essential to put into mind that wearable technology comes in different forms, most of these systems work and function in a similar fashion.

For the purpose of this explanation, we will be using the most common example of wearable technology, wristbands and smartwatches, as they are considered as the most recognizable and popular one among different consumers, as well as the fact that they tend to be multipurpose.

Wearable technology can also be thought of mini computers that are usually designed in a fashion that makes the comfortable to wear and use. They are designed to help augment and enhance a user's life by providing useful information tailored towards them, such as giving the user the ability to monitor the quality of their sleep and heart rate, or simply gain important notifications such as reminders and phone calls.

An important fact that needs to be known about these devices as that they tend to be considered as “complementary” devices, where they tend to need some form of parent device (e.g. Smartphone or Tablet) to function and generally tend to communicate between these devices through the use of some form of

wireless connection (most commonly Bluetooth or ANT+), with some tending to connect with the main device with the use of some physical connector (e.g. Gear VR headset for Samsung Smartphones).

These devices tend to contain an array of sensors that work to performing a certain function.

Some of these sensors include accelerometer and heart rate sensor, which are the most popular ones.

Applications of wearable technology

As mentioned in the previous section, the main aim out of the use of wearable technology is to augment the user's daily activities and lifestyle in two main ways: To simplify the process and/or provide detailed insights to daily tasks.

When looking deeper to the augmentation aspect of Wearable technology, the often tend to be health focused. These devices often provide a statistical reading of physical activities such as step counts as well as a BPM (beats per minute) (in the case that the wearable piece of technology is equipped with a heart rate monitor). Also, certain types of wearable technology might contain even more sensors that are more specifically tailored to specific kinds of sports or activities.

A good example of a specialized form of wearable technology would be the Android-Powered Polar M600 smartwatch. This specific watch tends to be targeted towards runners, with the sensors that it provides to track different types of data that are important to runners.

Shifting focus to the simplifying aspect, most wearable technology aims at helping the user to find easier methods to common tasks, making them easier to conduct and more effective in the long term.

Examples of wearable technology also include glasses, headbands, rings, bracelets, and hearing aid devices for people with hearing problems.

The uses for wearable devices are far reaching and can influence many of the current technologies. They can influence health and medicine, fitness, curing disabilities or coping with them, furthermore, if these wearable devices managed and used properly, they can lead to a huge improvement and efficiency in the lives of people who are using it.

In present time, the use of wearable technology has been leaning towards health and fitness, and leisure. Where many companies are competing to find the best way to promote their product and make it as useful as possible. There are many smart watches that have changed the way that wearable devices can be used.

Nowadays companies such as Fitbit have created smartwatches and fitness bands that are able to track vitals such as heart rate of the user and the calories burnt throughout the day, and if the watch / bracelet are synchronized with the user's phone the device will be able to track the location of the user and where he has gone.

This is useful for athletes as it is used to save routes they take on a daily basis, athletes may also take advantage of the heart rate sensor that is on the smart band, to make sure that they have their breathing right and monitored constantly in case anything bad happens to them.

Wearable devices have also been dominating the gaming/leisure industry, these days we can see that VR (virtual reality) headsets have started gaining an increase in interest and popularity and that is because VR headsets started being used in a better way to entertain people. For example, these days we have games that can be used to immerse the user to make him feel like he is a part of the game. Another application for VR headsets is a medical application, the headsets are used to treat patients with PTSD (post-traumatic stress disorder).

VR headsets can be used in the training of athletes. In preparation for competitions and such, for example an athlete utilizes wearable devices to tweak certain parts of their execution, for instance, a golfer who is hoping to enhance their swing, or a track cyclist needing to go faster can all be advanced and enhanced using wearable technologies such as the mentioned VR headset.

Body Sensors

Since one of the most common types of wearables seen being used by the consumers of today are fitness trackers, many of these contain a plethora of sensors that aim at tracking certain kinds of body related statistic (the most common of them being heart rate sensors). Some companies even go as far as to include sensors that can measure respiration rate and skin temperature, which they believe, can help users in being able to achieve a healthier lifestyle.

Though, the ability of such devices being able to monitor certain body vital could result in a huge breach of privacy, since such form of data might be shared with different organizations without the user's extent (e.g. Insurance companies or different health organizations) In the case that the device recording on such entertainment purposes.

Another application for wearable technology, is the utilization of virtual reality headsets for entertainment purposes, VR headsets such as the HTC vive and the PlayStation VR can give the user an immersive environment. The use of these headsets can give the user a three-dimensional view of their game in which they can interact with the environment inside the game.

It ought to be noted, in any case, that virtual reality is not just valuable in gaming. This innovation has a variety of uses in entertainment, but also Virtual reality can help in different museum and exhibits, for example when VR headset is used it can give a tour for the exhibit and give allow members to see 3D objects at different angles.

As Palmer Luckey, one of the creators of Oculus Rift, stated once, “this technology is going to revolutionize the way we live, learn, work, and play.”

Security concerns

Wireless connections can be a potential risk



Since a good portion of wearable technology tend to be designed in such a manner that most of their functionality relies on them being connected to a “parent device” (e.g. the connection between smartphones and smartwatches or smart bands) or provide improved functionality when connected it to other devices (e.g. Using a smartphone or tablet as a viewfinder and remote controller for GoPro camera’s).

Wireless connections tend to be preferred by many users due to the fact it can present less hassle to users and provides them with a level of freedom that simply cannot be achieved with regular wired connections.

Though many consumers for the wearable devices prefer using wireless connections, there tends to be many risks and drawbacks that can potentially lead to the violation of privacy and security, many devices mainly rely on their wireless connections to perform their many different tasks.

Most companies attempt to have their connections with minimal latency (which is a delay in the transfer of data), rather than ensuring that they remain secure with the strongest forms of encryption.

Bluetooth Low Energy (or Bluetooth LE for short) is an example of a connection that can potentially lead to the violation of the user's privacy and security. As very often, manufacturers, rushing their products to the market, think little about the loopholes they might be leaving for all kinds of intruders. Some of the devices would broadcast a unique ID that ruins the whole idea of masking the devices, while others change just the last few bytes of their MAC addresses, making them easily recognizable and traceable¹.

This poor implementation of Bluetooth devices can make it far easier for many to effortlessly locate devices within a certain range as well as conveniently perform different cyber-attacks, such as Man-in-the-Middle attacks, where users can easily eavesdrop on different users.

Privacy Concerns

When it comes to wearable technology, most people are only worried about their privacy. This is because they do not want their data online, also many people are concerned with what they put online for people to access.

In a survey² that was conducted in my school, participants were asked what their biggest concerns regarding the use of wearable devices was.

Participants given the option to choose what concerns they had about their use for wearable devices, they could choose between different concerns (such as privacy, security, etc...).

¹Andrii Degeler. "Bluetooth Low Energy: Security Issues and How to Overcome Them." *Stanfy | San Francisco Mobile App Developers*. N.p., n.d. Web. 04 Mar. 2017. <<https://stanfy.com/blog/bluetooth-low-energy-security-issues-and-how-to-overcome-them/>>. This information is regarding the state of bluetooth connection within devices during the release into the market

² Survey can be accessed through: <https://tinyurl.com/nisitgssurvey>



Figure 1: image showing a sample of the survey that was given to different students in the school

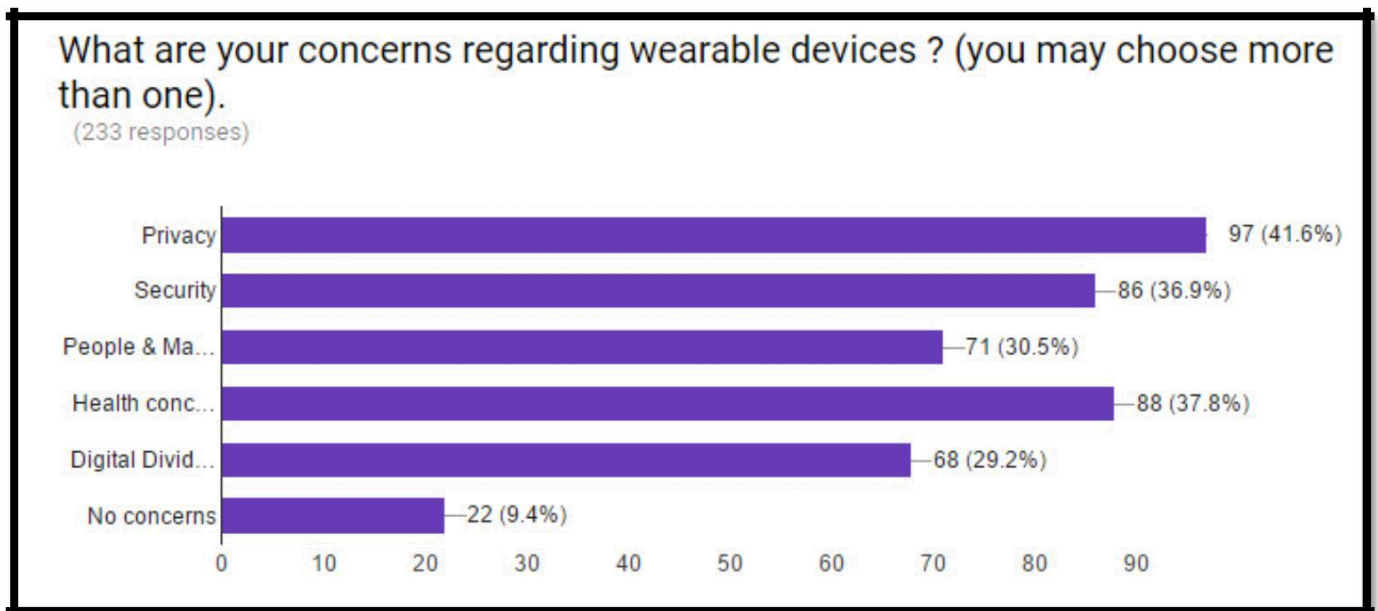


Figure 2: results from the question related to the privacy of the users upon their usage of wearable devices

As we can see from Figure 2 above, a majority of the participants who took the survey had concerns related to their privacy when they use wearable devices. These concerns may have different reasons.

Location Services and Constant location tracking



Figure 3: Image above shows Google Maps running on an Android Wear powered Smartwatch. In this case, the Huawei Watch.³

One of the main features that have been constantly advertised by many of the companies responsible for the fitness trackers many use today is the ability of these wearables. These devices track locations such as running and cycling routes, as well as a mini-GPS unit. That allows users to get step-by-step navigation (as seen done on Android Wear Watches using the Google Maps application)

While this may in many be cases be considered as an extremely valuable tool and feature for many consumers (e.g. Tracking kids with GPS, athletes looking to share their training routes with others), there are many potential risks that can possible lead to the violation of privacy.

This violation can occur in either two forms, through the device itself, or while it is transferring data between another devices (e.g. Sending GPS collected routes from a smartwatch to a smartphone)

Where the potential for privacy violation arises is from the process of transferring GPS tracked locations between different devices the use of wireless connection types such as Bluetooth or Wi-Fi.

Most wearable devices record and utilize location services to in order to help users keep track of things such as, places they have been when they have been running for example, or places that they have generally

³ Image taken from: <http://www.haroldkasperink.com/index.php/android-wear-everything-you-need-to-know-2/>

visited during the day that they need to keep track of. This can be a problem regarding privacy, because not all people would like to have their private data such as their location accessed by different people such as the watches.

Integrated Microphones and Camera

Microphones and cameras have almost become essential components of most of the wearable technology seen today, with some of manufacturers being forced to include them within their products as part of the requirements enlisted by software developers. Such requirements can be seen within popular mobile operating systems such as Android Wear, where companies designing watches to run the aforementioned operating system will need to include a microphone to allow different forms of functionality such as voice dictation and performing Google searches on the watch itself.

Other forms of wearable technology with integrated microphones and cameras could be body worn cameras (or more popularly, action cameras), where the camera is small enough to be worn on different parts of the body. GoPro Action Cameras could be considered as the camera that popularized such type of cameras.

Devices with integrated cameras and microphones that are small enough to be worn comfortable and be used and activated without too much complication have been seen as powerful assets for different organizations, specifically within organizations that deal with law enforcement and security, such as police departments. Different police departments within the US have integrated cameras into police officer's uniforms as a form of collecting evidence that might be used on different suspects.

Though the integration of such devices can present a severe issue for both the user and other alike. Microphones can lead to the possibility one being recorded unannounced or even used to record others without one knowing, as is the case with the previously mentioned Android Wear operating system, where the any voice searches are saved within Google's databases unbeknownst by certain users.

"You may not realize it's been activated, and you may not realize it's stored part of an intimate conversation, or whatever else it picked up.

Accidental voice command activation happens, and saying something too close to "Ok Google" or hitting the wrong button at the wrong time could store any speech your smartphone is able to pick up. Something like "Itchy goggles" would probably trigger it on Android platforms.

Take a deep breath, and don't toss your phone in the pool; it's not like Google is recording every word you say whenever the device is on. But much the same way a poorly timed butt dial can have some negative effects on your life, that voice search is a hazard if you're not careful.”⁴

Even more dangerous could be the possibility of cameras that could be worn. While useful in some situations these devices can be highly invasive to many people privacies. Wearable camera that offer wireless form of connectivity may be hacked and lead to the user’s privacy being exposed. Many can also use these devices to violate other’s privacy.

In the United States of America, “Justice Department has said it would allocate \$20 million in grants for *“police departments to buy body cameras, and House Republicans this week proposed setting aside \$15 million for the technology.”⁵*

This has caused growing concerns within the public regarding various privacy concerns of implementing this form of technology.

“But equipping police with such devices also raises new and unsettled issues over privacy at a time when many Americans have been critical of the kind of powerful government surveillance measures that technology has made possible.”

“Officers wearing body cameras could extend that public eye into living rooms or bedrooms, should a call require them to enter a private home.”⁶

Solutions for Security and Privacy in Wearable Technology

Making wearable technology as standalone devices

⁴Whittaker, G. Clay. "Google Voice Search Stores Everything It Overhears." *Popular Science*. N.p., 2 June 2016. Web. 04 Mar. 2017. <<http://www.popsci.com/googles-recording-your-voice-too>>.

⁵Tanzina Vega. "Rights Groups: Police Body Cameras Raise Privacy Issues." CNN. Cable News Network, 15 May 2015. Web. 04 Mar. 2017. <<http://edition.cnn.com/2015/05/15/politics/body-cameras-civil-rights-privacy-coalition/>>.

⁶Matt Pearce. "Growing Use of Police Body Cameras Raises Privacy Concerns." *Los Angeles Times*. Los Angeles Times, 27 Sept. 2014. Web. 04 Mar. 2017. <<http://www.latimes.com/nation/la-na-body-cameras-20140927-story.html>>.

This solution suggests making wearable technology such as smartwatches not need other devices in order to function. Such as the mentioned smartwatches that need pairing of a phone by using Bluetooth or other protocols such as ANT+ and the internet of things discussed earlier.

This solution would solve the issue related to the privacy of the data that is stored in the wearable devices that people use, stored data can be things such as the health records, since many wearables tend to be connected to other devices such as mobile devices and computers the data is often stored there (due to the lack of storage space in the smart watch), so making the device a standalone device would help secure the data of the clients and would also help them make sure that their information would not be given and used without their knowledge.

This solution can solve the issue with security of the user, this is because the devices will not need to be connected to a mobile device, this means that the data of the client will be in one place instead of multiple places that it will be saved on in the mobile device, mobile devices have a tendency to save everything onto a cloud for safekeeping of the data for future use, also if the data continues to be save on a cloud there will be a bigger risk for hackers to access the data from several places if many copies are available in different sources.

Adding different policies to help maintain privacy of the user

Adding several policies can help solve the solution of privacy for the user, the user needs to read the documentation and instructions of the device in order to know what is being shared, also the user needs to have an understanding for where his data is being saved, and who can access the data. For example, with GPS tracking the user needs to be aware that their location is constantly being monitored, a policy that companies would add is that they would state this fact for the user so that they can avoid getting into any situations where their privacy or security will be in jeopardy.

User guidelines and terms of use

In order to prevent further privacy issues, developers will need to add guidelines for the use of their products, this will be beneficial for the user and the and the developers of wearable devices, this is because adding these guidelines will help protect both the customer (since the customer will be better educated and will not have any issue knowing what are the appropriate uses for the devices are) and the use of these guideline will also help prevent any potential legal problems that may occur with the clientele in the future.

Transparency with users

Developers need to give consumers more and better information about their devices about their wearable devices, as wearable devices are starting to be smarter and smarter users need to understand what the devices collect about them, users also need to know how to use devices effectively and in a way that will not compromise and threaten their personal security, because if the security is breached this will lead to a problem with privacy since information will be leaked and private information will be given to the public.

CHAPTER TWO

CONCLUSION

The modern technological advancements in wearable technology has increased the amount of risks that can compromise the security and the privacy of the user. This is because of the availability for users to use GPS tracking, also the use of Bluetooth low energy in various different types of wearable devices also causes different types of security concerns, also the continued use of the microphones and cameras also factor in causing privacy concerns for the user.

In order to help solve these issues companies must start implementing different policies and start being transparent with the users for them to know their rights and know what they can do with the device, and what type of data is collected about the user upon the usage of such devices, users must also be aware that the misuse of wearable devices can also help breach their privacy.

REFERENCES

- [1]. "Applications Of Virtual Reality." *Virtual Reality*. Virtual Reality Society, 27 Feb. 2017. Web. 13 Mar. 2017. <<https://www.vrs.org.uk/virtual-reality-applications/>>.
- [2]. Arirangnews. "Wearable Devices Raise Privacy Concerns." *YouTube*. YouTube, 06 Aug. 2014. Web. 13 Mar. 2017. <https://www.youtube.com/watch?v=0e_QkV1vS94>.
- [3]. Corbin, Kenneth. "IoT Makes Security and Privacy Top Challenges for Wearables." *CIO*. CIO, 08 Mar. 2016. Web. 13 Mar. 2017. <<http://www.cio.com/article/3041637/wearable-technology/iot-makes-security-and-privacy-top-challenges-for-wearables.html>>.
- [4]. Degeler, Andrii, Mr. "Bluetooth Low Energy: Security Issues and How to Overcome Them." *Stanfy*. Andrii Degeler, 24 June 2015. Web. 16 Sept. 2016. <<https://stanfy.com/blog/bluetooth-low-energy-security-issues-and-how-to-overcome-them/>>.
- [5]. Drolet, Michelle. "7 Potential Security Concerns for Wearables." *Network World*. Network World, 11 Apr. 2016. Web. 13 Mar. 2017. <<http://www.networkworld.com/article/3054584/security/7-potential-security-concerns-for-wearables.html>>.
- [6]. "EInvestigator." *EInvestigator.com*. N.p., 09 Jan. 2017. Web. 13 Mar. 2017. <<https://www.einvestigator.com/police-body-cameras-the-pros-and-cons-for-law-enforcement-and-citizens/>>.
- [7]. Hussain, Zainab. "Weary of Wearables: IP, Privacy, and Data Security Concerns." *ABA LawPractice Today*. N.p., 14 Jan. 2016. Web. 11 Sept. 2016. <<http://www.lawpracticetoday.org/article/weary-of-wearables-ip-privacy-and-data-security-concerns/>>.
- [8]. Ibmthinkacademy. "How It Works: Internet of Things." *YouTube*. YouTube, 03 Sept. 2015. Web. 13 Mar. 2017. <<https://www.youtube.com/watch?v=QSIPNhOiMoE>>.
- [9]. Mansfield, Matt. "Can Wearable Technology Threaten the Cyber Security of Your Business?" *Small Business Trends*. N.p., 18 Feb. 2016. Web. 13 Mar. 2017. <<https://smallbiztrends.com/2016/02/wearable-technology-security-issues.html>>.
- [10]. Nig, Cindy, Mrs. "5 Privacy Concerns about Wearable Technology." *Varonis Blog*. Cindy Ng, 30 Oct. 2015. Web. 09 Sept. 2016. <<https://blog.varonis.com/5-privacy-concerns-about-wearable-technology/>>.
- [11]. Osborne, Charlie. "Smartwatch Security Fails to Impress: Top Devices Vulnerable to Cyberattack." *ZDNet*. ZDNet, 04 Dec. 2015. Web. 13 Mar. 2017. <<http://www.zdnet.com/article/smartwatch-security-fails-to-impress-top-devices-vulnerable-to-cyberattack/>>.
- [12]. Stuart, Gray. *Information Technology in a Global Society*. Geneva: International Baccalaureate Organisation, 2011. Print.

- [13]. Thierer, Adam D. "The Internet of Things and Wearable Technology: Addressing Privacy and
- [14]. Security Concerns without Derailing Innovation." *By Adam D. Thierer :: SSRN*. N.p., 12 Sept. 2014. Web. 13 Mar. 2017. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2494382>.
- [15]. "Wearable Technology -- Modern Marvel or Invasion of Privacy? | Liberty Treehouse." *YouTube*. YouTube, 24 Mar. 2014. Web. 13 Mar. 2017.<<https://www.youtube.com/watch?v=B5hjNFR9hLQ>>.
- [16]. "Wearable Technology and Privacy Concerns | MIT Sloan Executive Education." *BostonBusiness Leadership Training*. MIT Sloan Executive Education, 05 Dec. 2015. Web. 13 Mar.
- [17]. 2017. <<http://executive.mit.edu/blog/the-downside-of-wearable-fitness-technology#.WMbINPI97cs>>.
- [18]. Matt Pearce. "Growing Use of Police Body Cameras Raises Privacy Concerns." *Los Angeles Times*. Los Angeles Times, 27 Sept. 2014. Web. 04 Mar. 2017. <<http://www.latimes.com/nation/la-na-body-cameras-20140927-story.html>>.
- [19]. Tanzina Vega. "Rights Groups: Police Body Cameras Raise Privacy Issues." CNN. Cable News
- [20]. Network, 15 May 2015. Web. 04 Mar. 2017. <<http://edition.cnn.com/2015/05/15/politics/body-cameras-civil-rights-privacy-coalition/>>.
- [21]. Whittaker, G. Clay. "Google Voice Search Stores Everything It Overhears." *Popular Science*. N.p., 2 June 2016. Web. 04 Mar. 2017. <<http://www.popsci.com/googles-recording-your-voice-too>>.
- [22]. AndriiDegeler. "Bluetooth Low Energy: Security Issues and How to Overcome Them." Stanfy | San Francisco Mobile App Developers. N.p., n.d. Web. 04 Mar. 2017. <<https://stanfy.com/blog/bluetooth-low-energy-security-issues-and-how-to-overcome-them/>>. This information is regarding the state of bluetooth connection within devices during the release into the market.
- [23]. Survey can be accessed through: <https://tinyurl.com/nisitgssurvey>
- [24]. "Your Health & Fitness Partner." What Is ANT+ - THIS IS ANT. Dynastream Innovations Inc, n.d. Web. 13 Mar. 2017. <<https://www.thisisant.com/consumer/ant-101/what-is-ant>>.
- [25]. Adam D. Thierer, The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation,21 Rich. J.L. & Tech 6 (2015).