Michael Smith

CSE 488 – Ethics and the Computing Professional

Dr. Bhrigu Celly

08 December 2017

[005467289@coyote.csusb.edu](mailto:005467289@coyote.csusb.edu)

Wearable Technology

**Introduction:**

The development of wearable technology has increased significantly over the past the past decade. From the development of Bluetooth headsets in 2002, to the modern VR/AR headsets being developed. With the marvels of this technology, several concerns are being brought with them. Concerns of privacy mostly. These concerns, that I will focus on, lie in the fields of privacy in social environments, in the workplace, and in regard to health information being leaked. Social engineers behind lenses of smart glasses, who are searching the internet for any information on you. Your boss texting you because he noticed that you are at an amusement park, when you called off saying you were home sick. Or your doctor messaging you, asking if you are okay, because your watch sent him a notification stating your heart rate became irregular. Would these possibilities become a normality for the future? Or should we create boundaries to prevent this "invasion of privacy."

**Case Details:**

Breaking up the field into three major components: social engineering with wearable technology, business with wearable technology, and health with wearable technology. First, we will discuss the use of wearable technology out in society. Imagine walking into a bar, you have the knowledge that the establishment has security cameras that record you for safety. Then someone approaches you and strikes up a conversation. You notice that they are wearing glasses; however, these glasses, while the conversation is happening, are taking images of your face and reverse searching the internet to pull up your social media. You do not notice, but the other person is reading through your accounts, learning your interests, hobbies, career, and everything else you have online. This few minute conversation lets the other person learn everything they need to, without you even knowing. As well they could have recorded that conversation without your consent. This should be considered an invasion of privacy. In fact, establishments have started already banning such technologies on their ground, to preserve their client's privacy. In 2014, 13 bars and restaurants have established a "no Glass" policy (Levy). It is expected as the technology becomes more popular, this policy will grow more popular in similar establishments, to protect their clients from privacy invasion.

Businesses have caught onto the trend and usefulness of this upcoming technology. Ideas floating around that this tech can replace so many devices and tasks for their employees. Tasks such as scanning a key card to open security doors or gates, would be replaced with a wave of your hand. Or such as logging into a computer terminal with an ever-changing password would be a wave of your hand as well. Some have even stated that paying for food or other items could be handled by this technology as well. In fact, in August of this year, a Wisconsin tech company became the first business in the United States to offer microchips to their employees. This chip will be inserted into the skin between the thumb and forefinger, and will allow employees to pay for food and drinks in the break room, open security doors, and login to their computers. (Scipioni). However, this technology will raise a lot of alarms for the public. What other information could be tracked with these chips? Are these chips safe from external control, such as hacking? Are there health concerns with these chips? The FDA, back in 2004, approved the use of Radio Frequency chips (RFID) to be used to relay information to doctors quickly; however, in 2014 the FDA stated that they were not aware of any harm that could be caused by these chips. And that they are still studying them to address any concerns about the potential harm from these chips (Graham). These chips are innovative technology, but they still remain new technology with potential risks to employees' health, privacy and security.

Wearable technology can be very beneficial for people with health concerns requiring constant attention with heartrate monitors, blood pressure analyzers, and other advances. This technology is able to transfer data in real time to patients' doctors for further analysis. Now imagine if you are having a stressful day at work and your heart rate becomes irregular due to the stress. Then you receive a text message from your doctor asking you if everything is alright. Now since that data was transferred to the doctor's office, that same data might have transferred to insurance providers, who might be seeing this regularly and raise your cost on health insurance because you become "at risk." Should this information be transferred to them as well? Or should that data be just between you and your doctor? This technology can give the patients ease of mind for their health; however, they should not have to worry about their insurance going up. Not to mention if this data is not correctly secured to health care standards, there is a huge liability risk. Offices do not want their clients' health information being leaked, therefore they have a lot of emphasis on the security standards.

**Case Question:**

With the advancements in monitoring wearable technology, should there be a limit to what the technology can do? Would we let our privacy be impacted by the possibilities of this technology, whether it be outside in society, or at work with our bosses monitoring us, or our health concerns being leaked outside our control?

**Case Standard:**

Currently there is no official restrictions on wearable technology. However, there has been a few individual restrictions set in public businesses across the past couple years. In 2014, Google Glass was banned from 13 bars and restaurants in the San Francisco area (Levy). Businesses have started to offer microchipping to their employees who have volunteered for these implants. Such as the Wisconsin tech company. However due to the restrictions of these chips they are only able to store minimal data and have no possibility of carrying extended monitoring technology, such as GPS or health monitoring. And lastly, in healthcare, the security measures required for this technology has been a concern in the industry. The FDA are making recommendation for manufactures to protect against vulnerabilities in medical devices. In 2015, the IEEE Cybersecurity Initiative released a report that was detailing the ways to limit the security vulnerabilities of these medical device's software to prevent malicious attackers (Ash). As the technology becomes more popular these standards are being established.

**Recommendations:**

Wearable technology is an impressive and limitless field, provides a lot of convenience to its users. However, the right precautions should be in place to prevent misuse of these possibilities. Restrictions to prevent invasion of employees' privacy, security to protect health information from external sources, and societal guidelines need to be made. My recommendation is to establish all these limits correctly before the technology develops past limitations.

**Case Solutions:**

Developing this technology with the ideas of respecting privacy, limit the data being collected to only what is needed, and create impenetrable security will open up a field that will provide convenience and peace of mind to its users.

**Benefits:**

If these ideas are followed, then this technology will allow individuals to track all the appropriate data as well as send it to a doctor for further analysis needed. It will allow employees to be efficient and relieve the burden of passwords or security cards. Lastly, will give society amazing technology without the sacrifice of privacy.

**References:**

Ash, Bill. “Wearable Technology: Enabling Security for Improved Healthcare Outcomes.” *Medical Design Technology*, 27 Apr. 2016, [www.mdtmag.com/blog/2016/04/wearable-](http://www.mdtmag.com/blog/2016/04/wearable-) technology-enabling-security-improved-healthcare-outcomes.

Bryant, Martin. “How Will the New Wave of Wearable Tech Transform Society?” *The Next Web*, 27 Mar. 2013, thenextweb.com/insider/2013/03/27/how-the-new-wave-of- wearable-technology-could-transform-society/.

Graham, Jefferson. “Are embedded microchips dangerous? Ask the Swedes - and pets.” *USA Today*, Gannett Satellite Information Network, 25 July 2017, [www.usatoday.com/story/tech/talkingtech/2017/07/25/do-microchip-implants-pose-](http://www.usatoday.com/story/tech/talkingtech/2017/07/25/do-microchip-implants-pose-) health-risks-ask-swedes-and-pets/507408001/.

Kelly, Heather. “Ticket for driving in Google Glass dismissed.” *CNN*, Cable News Network, 17 Jan. 2014, [www.cnn.com/2014/01/16/tech/innovation/google-glass-ticket-](http://www.cnn.com/2014/01/16/tech/innovation/google-glass-ticket-) dismissed/index.html.

Matyszczyk, Chris. “Don't Glass and drive -- lawmakers seek to ban Google Glass on the road.” *CNET*, 23 Mar. 2013, [www.cnet.com/news/dont-glass-and-drive-lawmakers-seek-to-ban- google-glass-on-the-road/](http://www.cnet.com/news/dont-glass-and-drive-lawmakers-seek-to-ban-%09google-glass-on-the-road/).

Levy, Karyne. “A Surprising Number Of Places Have Banned Google Glass In San Francisco.” *Business Insider*, Business Insider, 18 Mar. 2014, [www.businessinsider.com/google-](http://www.businessinsider.com/google-) glass-ban-san-francisco-2014-3.

RKD // AgencyND // University of Notre Dame. “John J. Reilly Center.” *Wearable technology // John J. Reilly Center // University of Notre Dame*, reilly.nd.edu/outreach/emerging- ethical-dilemmas-and-policy-issues-in-science-and-technology-2015/wearable- technology/

Scipioni, Jade. “Wisconsin company to implant microchips in its employees in August.” *Fox Business*, Fox Business, 24 July 2017, [www.foxbusiness.com/features/2017/07/24/wisconsin-company-to-implant-microchips-](http://www.foxbusiness.com/features/2017/07/24/wisconsin-company-to-implant-microchips-) in-its-employees-in-august.html.

Statt, Nick. “Wearables with augmented reality are mind-Blowing -- and an ethical nightmare.” *CNET*, 8 Jan. 2014, [www.cnet.com/news/wearables-with-augmented-reality-are-mind-](http://www.cnet.com/news/wearables-with-augmented-reality-are-mind-) blowing-and-an-ethical- nightmare/#ptlink.fid=5086&isc=1&did=bookmark.423d976a8f08ed546f2cc88c14438d3 d22086fbf&ctp=article.