Seig Hall
1851 NE Grant Ln
Seattle, WA 98195

December 6th, 2017

Irini Spyridakis
Loew Hall
3920 E Stevens Way NE
Seattle, WA 98195

Dear Ms. Spyridakis,

Enclosed is a report for your consideration on the ethical considerations of wearable technology as requested for Human Centered Design and Engineering 231 at the University of Washington.

The purpose of this report is to better inform consumers about the ethical issues surrounding the uses of wearable technology. The ethical issues focused on in this report are access to personal health information, access to GPS and location of consumers, and hackability of wearable technology and identity theft. This report will also give a brief introduction to the topic, some background knowledge of how wearable technology came to be, a discussion of the ethical considerations, and recommendations for future implementation and security uses of wearable technology.

If you have any comments, questions, or concerns please reach out to cfsmith1@uw.edu. We hope you find our report informative and useful when making decisions involving wearable technology in the future.

Sincerely,
Courtney Smith
Emily Nuri
Sam O’Brien

HUMAN CENTERED
DESIGN & ENGINEERING

UNIVERSITY *of* WASHINGTON

The Ethical Considerations of Wearable Technology

December 6th, 2017

Courtney Smith

Emily Nuri

Sam O'Brien

Table of Contents

List of Figures

Executive Summary

Many consumers do not realize the ethical issues surrounding the use of wearable technology. While there are some pros, there are also major ethical issues with wearable technology in relation to access to personal health information, access to GPS and location of consumers, and hackability and identity theft. People are in danger of not getting proper healthcare based off of self diagnosis due to their unprecedented access to their health data in real time. They are also in danger of no longer having their personal data stay private. Many companies track a user’s location at all times without explicit consent and store this data in big servers to be used later if they so please. The collection and storage of consumer data also leads to generated data being vulnerable to attacks. When data is shared over the internet and bluetooth, it automatically becomes vulnerable and creates opportunities for hackers to not only access user data but to then assume a user’s identity. Overall, users of wearable technology need to be more concerned about how their wearables affect their health and the security of the data being collected by their wearable devices. Users can increase awareness of these issues by fully reading terms of use and conditions and by pressuring wearable technology companies to protect the privacy and security of their data.

Introduction: What is Wearable Technology and Why is it Important

Wearable technology, or wearables, are electronic computers that are incorporated into clothing and accessories and are meant to enhance, if not exceed, handheld technology [1]. Wearables are often thought of as something simple like a watch but can include more invasive devices such as contact lenses or even implanted micro-chips. Since wearables are personal devices, they can be very discreet and allow users to track things including their health or diet without requiring much thought or effort. There are many groups of people who can benefit from this, including those who are health conscious, those who have a disability, those who are concerned about keeping track of their personal data, and so many more. Most technology wearables are designed with one purpose in mind, “to create constant, convenient, seamless, portable, and mostly hands-free access to electronics and computers” but have since evolved and have a different purpose with each passing day [1]. Part of these evolving iterations on wearable technology are the use and advancements of scanners within the device. The devices that contain scanners can track sensory inputs like mood, temperature, or heart rate, and the list is continually growing. Due to these features and other advancements in technology and innovation, wearable devices have gained popularity during the past few years. In Figure 1 [17], the visible exponential incline of wearable devices in recent years shows the wearable market is expected to be worth $5.8 billion by 2018 [2]. Wearables are advancing and growing at such a rate that users do not have time to stop and think about the ethical and moral implications of their actions, let alone the ability to wait and see what these implications might actually be.

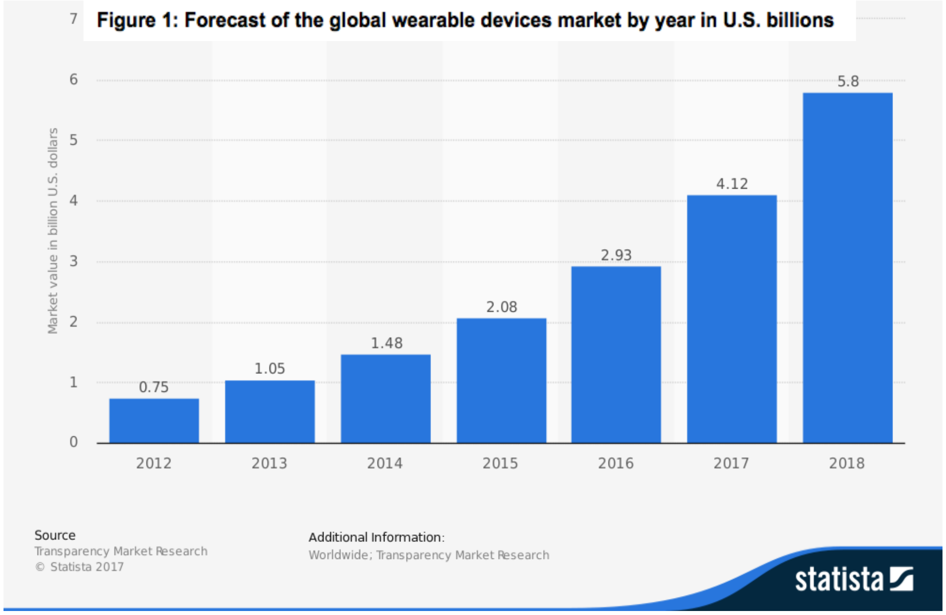
Figure 1: Forecast of the global wearable devices market by year in U.S. billions

Source
Transparency Market Research
© Statista 2017

Additional Information:
Worldwide; Transparency Market Research

While the data collected from wearable devices can be very useful knowledge for people to have readily available, it brings up many ethical concerns. These concerns include but are not limited to access to personal health information, access to GPS, access to the location of consumers, hackability, and identity theft.

Background: Making Technology Wearable

The ideation and creation of wearable technology essentially stems from the concept of ubiquitous technology. Ubiquitous technology is an approach to designing technology so that it appears anywhere and everywhere. This means that a user should be able to compute and access the internet at all times, in all places, and from devices other than their desktop personal computers. Wearable technology is arguably the most successful implementation of ubiquitous technology.

The first major example of technology becoming wearable and ubiquitous was the hearing aid. Hearing aids, first invented in the seventeenth century, are an excellent example of the process of technology improving the utility of a design. These hearing aids were typically large, uncomfortable “trumpets” that the user would point in the direction of a source of sound and would hold the other end up to their ear [3]. There were many different iterations of the ear trumpet, but it was not until the nineteenth century that Frederick Rein started to mass produce hearing aids in London [4]. Initially, the designs of the hearing trumpets were still bulky and immobile, but with time and different iterations of the hearing trumpet, Rein was able to produce the first sets of mobile, small hearing trumpets. This was arguably the first iteration of wearable technology and was the way hearing aids remained until the invention of the telephone in the late nineteenth century. The invention of the telephone introduced new technologies that allowed hearing aids to be turned digital. The telephone and microphone allowed smaller devices to more effectively transmit sound and frequencies; revolutionizing not only hearing aids the entire wearable technology industry [4].

Another essential factor in the development of wearable technology was the digital watch. The digital watch was first introduced in 1975, made by companies like Hewlett Packard and Pulsar [5]. The introduction of the digital watch was one of the first times where programmers and fashion designers had to work together. However, this sponsored a long and fruitful relationship and led to many implementations of the digital watch. Some were square, some were circular, and some even had a built in calculator. The introduction of the calculator in a watch was the first big step that wearable technology took towards ubiquitous technology. For a price of around $30, users were able to compute complex mathematical processes anywhere and everywhere with the click of a few buttons. This technology was revolutionary, and digital watches are still used to this day, but the most influential and life changing iterations of wearable technologies are the ones that monitor and improve the life of the user.

Discussion

The following is a discussion of the ethical considerations surrounding wearable technology and specifically addresses access to personal health information, access to GPS and Location of consumers, hackability and identity theft.

Ethical Issue 1: Access to Personal Health Information

Aside from improving hearing and helping a user tell time, different wearable technologies have many useful applications. One of the many innovative applications of wearable technology is designed with health in mind. However, health also brings up several concerns regarding the safety, reliability, and security of wearables. Figure 2 [18] shows the possible health data that wearable tech is now able to detect in one`s body. This includes heart rate with an oximeter, muscle activity with an electromyographic sensor

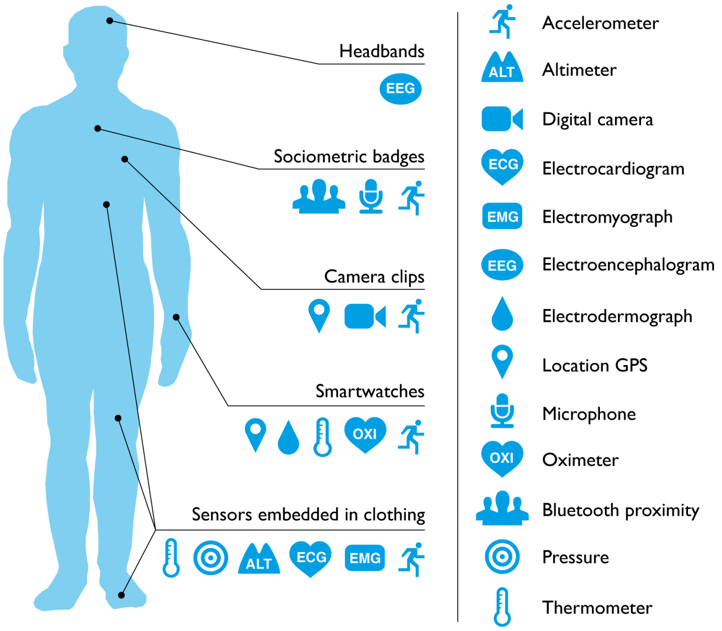

Figure 2: Data detectable and type of wearable tech that can sense it

embedded into clothing, stress with an electrodermal sensor incorporated into a wristband, and physical activity or sleep patterns via an accelerometer in a watch. In addition to these applications, a female’s most fertile period can be identified with body temperature tracking, while levels of mental attention can be measured with a small number of non-gelled electroencephalogram (EEG) electrodes. Levels of social interaction (known to affect general mood) can be monitored using proximity detections to others with Bluetooth or Wi-Fi enabled devices [18].

As more consumers purchase wearable tech, they unknowingly expose themselves to potential security breaches and provide companies the opportunity to use the data that they generate. With current consent laws, users who buy wearable devices often do not “own” their data. Instead, data is collected and stored by the manufacturers who sell the device and users often only see a summary of the results. Many manufacturers even charge users a monthly fee for access to their own raw data, which is regularly sold to third-party agencies. Most companies are also willing to share a user's location, age, sex, email, height, weight, and more [3]. Due to the public knowledge that health companies have this data, security breaches have become much more common, especially since personal data is extremely valuable. The chief of consumer security at Intel Security stated, "The information that is contained on your wearable that is stored either on your smartphone or stored downstream on a cloud is worth ten times that of a credit card on a black market." He also claims that, “information being stored on these wearable devices doesn't go away” [6]. Visibly, these statements demonstrate that these ethical violations are extremely serious for both users and tech companies. Worst of all, most users are not aware or warned about these possible security breaches and the potential misuse of personal data by wearable tech companies.

Another major issue with wearables is the multitude of unwanted health risks that they expose to consumers. According to Medicine and Radio-Diagnosis professional Dr. Pandey, many current wearables are untested and release Electro-Magnetic Radiation (EMR) and radio signals, which have become one of the most toxic forms of pollution and have become a major health concern [7]. Dr. Pandey also mentions that the radiation that is released by these gadgets can cause reduced sperm counts, eye irritation, anxiety, headaches, reduced appetite, nausea, mood swings, and sleep disruption [7]. Even with these extreme side effects, most tech companies shy away from explaining or bringing awareness of these issues to their users, which clearly poses an ethical conflict.

Finally, as the line between consumer health wearables and medical devices begins to blur, it is now possible for a single wearable device to monitor a range of medical risk factors [8]. This can be dangerous since the reliability of patient-entered data depends on the type of information one is entering, the patient's general and health literacy, and the specific motivations for recording the data. This can potentially give users a false sense of security about their health, can lead them to incorrectly self-diagnose some medical condition, or can even deter users from getting proper care due to deceiving results. Moving forward, practitioners and researchers need to work together and accommodate these technological advances in a way that ensures wearable technology can become a valuable asset for health care in the 21st century [9].

Ethical Issue 2: Access to GPS and Location of Consumers

GPS tracking and monitoring has both positive and negative attributes. For example, parents can now give their children backpacks that have a GPS in them, so they can check where their children are and if they are safe. Another powerful application of wearable GPS tracking is with criminals. In the United States, GPS devices called Tracksticks are sometimes secretly installed on a criminal’s cars without their knowledge [12]. These applications of GPS tracking are clearly beneficial, but it still infringes upon the privacy of the criminals. It is important to establish a level of “secretive tracking” that is beneficial and another level that is not. Although tracking criminals can be helpful, it is still a violation of the privacy and property of their information generation. It is boundaries like these that are important to establish before the wearable technology industry gets too far ahead of its users.

The colossal technology industry is ever-growing, and with it grows the amount of information that is being generated and stored. In the past, the information that was generated by users was relatively simple in nature and was comprised mostly of which ads most effectively warranted a click or what kinds of websites users like to visit most.

However, with the introduction of new technologies like cell phones and smartwatches came a new type of information generation. These new devices are always powered on and are always with the user, and they are equipped with some of the most sophisticated microphones, cameras, GPS, and other powerful tools. All of these tools create a new source of information that some big tech companies are recording, storing, and selling.

More of these tech companies are using GPS to track the whereabouts of users and employees. Companies like Facebook, BP, AutoDesk, and Cigna often provide their employees with a Fitbit and use its GPS location to track them to “ensure productivity” [10]. Using wearable technology in this way is encroaching on the wearer’s right to privacy. The ability of the wearers of this technology to keep personal information about themselves private and confidential is taken away from them. When companies collect this information, it is important to consider the issues of privacy (who can see the data), accuracy (the accuracy of the information held about users), property (who has ownership rights over personal information), and accessibility (who has access to customer information) [11]. The GPS information of users is private, and when companies collect and sell the information that users generate, they expose user information to hundreds and even potentially thousands of people. In doing so, companies not only violate the privacy of the user, but they sell the user’s information property without asking the user for permission. If companies do ask, then they do it in “terms of use and conditions” that is hardly understandable and is designed to hide certain information. It is clear that selling user locations is a misuse of the power of GPS tracking.

Ethical Issue 3: Hackability and Identity Theft

While wearable technology helps to keeping life simple and interconnected for the user, it can pose serious security risks. One of these risks includes the security of the information not only collected on the wearable but also the information on devices that connect to the wearable. With the increasing amount of competing companies making interconnected wearables, many are sacrificing security for speed [13]. They are haphazardly pushing products out on the market and deal with issues as they come. Because of this rush to production, user’s devices are susceptible to hacking and can leave the users open to identity theft.

Currently, the most common wearables on the market are smartwatches, more specifically Fitbits or Apple watches [14]. A key feature of these rush-to-production devices is their ability to act as a method of payment. Most devices that can take a credit card can receive a signal from a smartwatch as a valid payment method. This is dangerous because it uses internet and bluetooth to transmit user’s payment information, making their credit card information vulnerable to interception. Having access to this personal information leaves a user’s identity unsecure and provides anyone with a moderate hacking ability the opportunity to steal user information.

Wearables also leave users susceptible to video and audio infiltration, both by outside individuals and by entities such as employers. Many people nowadays have tape or some other form of cover over their computer's webcam with the intention of preventing attackers the ability to see through the camera. This very concern should be taken into account when talking about wearables. With the level of intelligence built into these devices, wearables have recording and sensing abilities that can be hacked and used against a user. There are companies that will record an employee’s meeting without their knowledge or consent. Companies have also “checked in” to see if an employee is actually sick when they call in sick to work. Private conversations can be taped without user consent and can be used in situations as blackmail or even as evidence in a court of law. Our phones and computers record our every move and “the more devices and data we add, the more data there will be for others to mine” [10].

Conclusions

Recently developed wearable devices opened up new capabilities in human interactions with the world. Due to possible hands-free user experiences and easy accessibility to personalized information, the rise of wearable technology opens up a new wealth of possibilities for potential applications. These applications include sensing the user’s immediate environment, navigating, assisting medical professionals, and many more

[15]. However, wearable devices also store large amounts of personal information that can be accessed by third parties without user consent. This storage of user information generates a broad range of ethical issues involving personal privacy and security, all the while promoting identity theft, stalking and even discrimination. This paper demonstrates user's ethical perceptions of the use of wearable devices in multiple sectors and suggests that wearable device users should be highly concerned with the privacy of the information they provide online.

Recommendations

When dealing with personal information like health and location data, wearable technology is often criticized for being a “sinkhole” of personal privacy, so it is vital to take proper precautions. The main recommended precaution is to fully read the terms of use and conditions before blindly clicking on “Agree” and thus unintentionally providing implicit consent. Reading the terms of use and conditions will inform users as to who has access to their data as well as what the data will be used for. Wearable technology companies should also step up and help protect the privacy and security of its users. For example, the Federal Trade Commission has claimed that companies can protect consumer privacy and security by (1) adopting security by design, (2) engaging in data minimization, and (3) increasing transparency by providing consumers with notice and choice for unexpected data uses [16]. By following these steps and implementing adequate safety precautions, the wearable technology industry can help promote and build trust in their consumers.

References

[1] Andrew Michael and Tehrani, “Wearable Technology and Wearable Devices: Everything You Need to Know,” *Wearable Devices*, Mar-2014. [Online]. Available: http://www.wearabledevices.com/what-is-a-wearable-device/. [Accessed: 04-Dec-2017].

[2] A. Kalinauckas, “Wearable technology,” *Engineering Technology*, vol. 10, no. 4, pp. 36–43, May 2015.

[3] H. Alexander, “Hearing Aids: Smaller and Smarter,” *The New York Times*, 26-Nov-1998.

[4] Mills, Mara. "Hearing Aids and the History of Electronics Miniaturization." IEEE Annals of the History of Computing 33.2 (2011): 24-44.

[5] “Modern Living: Going Digital,” *Time*, 22-Dec-1975.

[6] “The dark side of wearables: How they’re secretly jeopardizing your security and privacy - TechRepublic.” [Online]. Available: https://www.techrepublic.com/article/the-dark-side-of-wearables-how-theyre-secretly-jeopardizing-your-security-and-privacy/. [Accessed: 04-Dec-2017].

[7] A. RAZANI, “Are wearables exposing us to unwanted health risks?,” *ReadWrite*, 13-Apr-2016. [Online]. Available: https://readwrite.com/2016/04/13/wearables-health-risks-radiation-dl4/. [Accessed: 04-Dec-2017].

[8] L. Piwek, D. A. Ellis, S. Andrews, and A. Joinson, “The Rise of Consumer Health Wearables: Promises and Barriers,” *PLOS Medicine*, vol. 13, no. 2, p. e1001953, Feb. 2016.

[9] H. Lewy, “Wearable technologies – future challenges for implementation in healthcare services,” *Healthc Technol Lett*, vol. 2, no. 1, pp. 2–5, Feb. 2015.

[10] G. Marshall, “The worrying potential of wearable data,” *Wareable*, 27-Mar-2015. [Online]. Available: https://www.wareable.com/internet-of-things/whos-watching-your-smartwatch. [Accessed: 04-Dec-2017].

[11] G. Boyce, “Beyond Privacy: The Ethics of Customer Information Systems.” Macquarie University, Sydney, Australia, Jun-2002.

[12] “GPS tracking: Ethical or not? | Computing and Society,” *Computing and Society*, 29-Sep-2012. [Online]. Available: http://blog.nus.edu.sg/itsfun/2012/09/29/gps-tracking-ethical-or-not/. [Accessed: 04-Dec-2017].

[13] L. Arsene, “Bitdefender Research Exposes Security Risks of ...,” 09-Dec-2014. [Online]. Available: https://www.darkreading.com/partner-perspectives/bitdefender/bitdefender-research-exposes-security-risks-of-android-wearable-devices-/a/d-id/1318005. [Accessed: 04-Dec-2017].

[14] “Best Wearable Tech of 2017,” *CNET*, 21-Nov-2017. [Online]. Available: https://www.cnet.com/topics/wearable-tech/best-wearable-tech/. [Accessed: 04-Dec-2017].

[15] R. Chinta, R. Fong, I. Murdock, W. Kang, and Q. Williamson, “A Novel Approach to Home Automation: Application Development with Google Glass.” rutgers, Jul-2014.

[16] Janice Phaik Lin Goh, “Privacy, Security, and Wearable Technology,” *American Bar Association*, vol. 8, no. 2, pp. 1–5, 2015.

[17] *Hacking risk for wearable fitness tracker EU 2015 | Survey*. .

[18] L. Piwek, D. A. Ellis, S. Andrews, and A. Joinson, “The Rise of Consumer Health Wearables: Promises and Barriers,” *PLOS Medicine*, vol. 13, no. 2, p. e1001953, Feb. 2016.