Wearables

By Lei Zou

Introduction: Why should we be concerned?

According to a report from *BI Intelligence,* the global shipments of wearables have quadrupled from 20 million units in 2013 to over 80 million in 2017, making them the trendiest of smart devices. If you have a Fitbit wristband or an Apple Watch, then you are most likely enjoying how these smart wearables count steps and give you a professional looking report of your health status. Or if you, by any chance, own a pair of Google Glasses, then you are probably having fun taking photos simply by blinking your eyes. However, while consumers are delighting in discovering how convenient these wearables make their lives, their exposure to wearable companies and other third parties is growing as well.

The vast amounts of data that wearables such as smart watches, smart wristbands or smart clothes collect is tremendous, and people should realize how valuable this daily data is in the big-data era. Companies are willing to use or purchase this data so that they can mine it to extract useful information and convert it into profits.

People may think that the federal laws protect their personal information from being manipulated, but unfortunately, the reality is that our health-privacy regulatory system is too vague and fragmented to properly fulfil its duties (Chester). Moreover, there has not been any framework (either from government or self-regulatory perspectives) that is able to adequately address privacy related issues caused by wearable health devices (Montgomery). Smart wearables are making users' lives increasingly convenient, but there is a tradeoff whose consequences we may not be aware of: companies are not being monitored in their choices to balance protecting users' personal data and making more profits through its manipulation and exploitation.

According to a report from *The Washington Post*, 2018 was the year of data leakage, and there has been over millions of customers' personal data that leaked or hacked in 2018. The fact that large companies, even like Target and Home Depot, were unable to protect their customers' data makes concerns about privacy protection become greater. However, an article from *CNBC* indicates that customers' personal health data is about 10 times valuable than credit card information in black markets, and these health data keeps being collected by wearables and diffused among stockholders (the third-party apps).

A brief history

Before talking about more serious issues in detail, let us take a look at how wearable technology has evolved since it was first invented. The concept of wearables is not new to people, though they only recently became popular, sometime after 2010.

If we ignore the advanced functions of recent devices, the very first wearable was invented in the 13th century, and that was eyeglasses. After that, the next popular wearable device was Nuremberg egg, which was a clock. Since then, there has been little improvement in wearable devices, until the 20th century. As improvements in technology occurred through the 20th and 21st centuries, more and more advanced wearable devices were invented, including calculator wristwatches and digital hearing aids. What distinguish

recent smart wearables and those basic kinds is that smart wearables are trying to "understand" humans by advanced technology like data mining and deep learning. After Bluetooth technology was invented, wearables' producers finally have created a method for their products to tie with humans close enough (through smartphones) to let machines know more about people. Since 2006, the relationship between wearables and smartphones has become closer due to the adoption of Bluetooth. This combination of smart wearables and smartphones do make human lives become more convenient and become prevailing. By a glance of the history of wearables, products like Nike+ products, Google Glass and Fitbit started to enter the industry and became the main players in the industries. 2018 was the year of wearable technology, as Apple introduced its first generation of smart watch, the Apple Watch, and in this year it has become the most popular smart watch.

Since then, the concepts of wearables have seized the attention of people from all over the world. From a report of *Quartz,* by the year of 2016, the top five wearable companies were Fitbit, Xiaomi, Apple, Garmin and Samsung. Wristbands and smart watches are the dominant products in the market, exploiting the trend in self-monitoring of health and fitness as the population ages. Logically so, Aleksander Milenkovic, professor at University of Alabama, and his colleagues claim in their paper that the number of adults age 65–84 is expected to double from 35 million to nearly 70 million by 2025 when the youngest Baby Boomers retire. Additionally, health care expenditures are projected to reach almost 20% of the Gross Domestic Product (GDP) before 2028.

These statistics imply that people are increasingly concerned with their health and are willing to pay whatever they have to in order to ensure it. A 2014 survey revealed that fifty-six percent of respondents believed that wearable health devices could extend their life expectancy by 10 years (Kim). Signals suggest that the wearable device market will grow at a very fast rate in the future.

Moreover, smart wearables are no longer limited to wristbands and watches. "Wearable computers may be worn under, over, or in clothing, or may also themselves be clothes" (Kim). Smart clothing is able to monitor all fitness data that your body generates and provide you with advanced feedback through Bluetooth technology associated with your smartphone. The data these devices collect needs to be analyzed by the algorithms stored inside your smartphone.

Another emerging wearable device which has become popular recently is the virtual reality (VR) device. VR devices aim to create a virtual three-dimensional, highly realistic environment for users who wear special glasses and earpieces to bring the virtual environment to life. A VR device is mainly for gaming and learning purposes, so its markets will not grow as large as the market for fitness wearables. Current VR technology is not advanced enough technically for many applications, and is still too costly to offer en masse, but the technology is well on its way, and VR markets could expand dramatically. Facebook has taken the lead on developing VR devices. CEO Mark Zuckerberg, invested 2 billion dollars into Hive, a VR device company, and he personally believes that VR will become the mainstream in the near future.

Current Issues

As all these wearables have been developed by computer science, they are able to know more and understand more about their users than their users might realize, and this trend may cause some problems. One of the largest concerns would be privacy.

We know where you are

As the largest segment of the smart wearables market is for fitness applications, these device need to store and read users' daily activity data. One example is the step-count function. Almost all brands of fitness wearables are able to count users' daily steps, analyze users' daily activity levels and provide health feedback. However, what people might not realize is that the method these devices employ to collect the steps includes location tracking. Wearables can count users' steps by simple mathematical calculations. As a result, these device not only store users' daily step counts, but also have access to track down users' location (with internal GPS function) whenever customers are wearing them. Another research team from University of Toronto also unveiled that data collected by smart wearables can be used to find exact location of users and even passwords (also see).

Connections with other data sources to piece together a story

No one knows what happens to the collected data. Wearable companies' privacy policy, like Apple, allow the companies to share the collected data with their so-called "strategic partners", and, of course, wearable companies will not describe in detail how these partners have been selected and what they will do with the data. Moreover, some fitness third-party Apps, such as Strava, even has access to store and analyze users' data through the wearables and there are no restrictions about what they can do with it. Thus, users' data do not remain private, and it becomes public information among technology companies. Unfortunately, this is not the end of the story.

Almost all wearables need to connect to a smartphone so that they can store and analyze the data using more powerful chips within the phone than the smart wearable itself has. This gives wearables another "opportunity" to access more private information through the smartphone. Working with the installed Apps, wearable devices are potentially able to access users' notifications or calendars in the smartphones as users connect wearables to their smartphones through Bluetooth. Therefore, an individual's personal activity can be linked to location, contact lists, downloaded music, bank information, and any other information stored on the phone.

The blurry definitions and guidance offered in the Stored Communication Act (SCA), passed in 1986, could be one reason that such data-trading occurs without hesitation. In their article, Nayanica Challa, professor at University of Chicago, and his team discover that it is very difficult to define whether the collected wellness data, such as steps and heart rates, as content, meaning "substance and meaning underlying a communication", or non-content, "such as telephone numbers and email addresses". The fitness data collected, for instance, is just numbers or programming codes, so the data does not carry any meaningful information by itself (e.g., people with no related knowledge would not understand what the data means), but it does deliver useful information to those with related knowledge.

Challa also states that "If wearable data are considered content, then they will receive limited disclosure protections of section 2702(b)".

Tracking Employees' Activities

Another issue is raised by employers. Many companies with large workforces are beginning to use fitness wearables, like Fitbits and Apple Watches, to monitor their employees' daily activities to evaluate productivity and health conditions. There are many ways that employers could benefit from asking their employees to don smart wearables. According to Patience Haggin's report on the *Wall Street Journal*, for instance, by monitoring employees' step counts and other activity, employers are able to get preferential terms on employee insurance.

Another issue would be discrimination. These wearables can only monitor and display users' overall activity performance and cannot tell employers what its users are doing exactly. Employees with disabilities, advanced age or those who are not feeling well one day may easily be penalized for working too slowly, and could claim discrimination.

Moreover, if the data indicates some sort of emergent medical condition, should employers inform their employees right away? Furthermore, according to Haggin, there is legal precedent for holding employers responsible if they had enough information to recognize a problem and not take action. Therefore, employers who do not disclose are definitely violating the regulations. If employers do notify their employees, that would raise some issues about privacy as well and this leads us to the second issue about work-related wearables and industrial spying.

When workers with monitoring wristbands or headsets attend meetings or other official assemblies, the meeting information might be monitored. For instance, by tracking users' location, people can know exactly when, where and who attended the meeting. By recording audio or video, meeting contents could be leaked out as well. Many hospitals offer surgeons smart headsets so that other doctors could see exactly what the surgeons see when they are operating. Moreover, the recorded footage could be used as educational purposes and diffused widely. *Time Magazine* reporter Jason Gale claims in his report that surgeons wear smart headsets during operations is displaying patients' privacy to all kinds of people around the world.

Employers could also be collecting data from their employees when they are at home, as there is no clear boundary to separate workplaces from home in many instances. If anything went wrong, employees would probably be blamed as they are the ones who actually use wearables. Such applications of wearables provide employers benefits in the sense of increasing workers' productivity and reducing unnecessary costs, but pushing all responsibilities to employees would be irresponsible and could cause negative results. Employees may fear that their employers will take advantage of their own data and use it against them. This new type of confrontation, raised by smart wearables, between employees and their supervisors might further amplify the distrust in workplaces.

Ethical questions arising from the smart wearables industry

A number of ethical questions arise when we consider smart wearables, including these listed below:

Industrial Parts:

1. Are employers permitted to legally mandate on-the-job wearables within certain limits? Which one is more significant: monitoring employees' performance or privacy? (Policy or agreement outlining purposes and limits of mandating wearables, as well as how the date would be handled)
2. If health problems are detected by monitoring employees' health and motion status, should employees be informed?
3. What should be established to deal with the wearables with recording and locating capacities which would likely lead to spying issues?
4. Who is taking control about managing and storing collected data?
5. Should periodic public conversation or hearing about wearable companies' data use policy be held?
6. Should leaders follow the ethical framework without any consequences?
7. Do leaders consider customers' or stakeholders' benefits the most?

Customer Parts:

1. Is the data collected stored securely in the cloud? Who else has the access to it?
2. Do wearable companies need permission from customers every time they use the data?
3. Do wearable companies have to disclose all stakeholders, and, if any, the data trading information to customers?
4. Do wearables companies need to disclose that what data they also collect besides heath data, and what are they able to do with those additional data?
5. Should devices provide "appropriate solutions" to customers just based on collected data without even interacting with any persons at all?