Privacy Concerns of Health Data Collected by Consumer Wearables: the Reality of Consumer Consent

We often see news reports about the health benefits of using consumer wearable devices. For instance, an Apple Watch saved a wearer's life from fatal internal bleeding by detecting irregularly fast pace of the user's heart rate and alerting him to check on himself. *(N/A, 2023)* In general, wearable devices can be divided into two categories: special purpose wearables and consumer wearables. In this essay, I will be focusing on consumer wearables, mainly including smartwatches or fitness trackers such as the Apple Watch, Fitbit, Oura Ring, etc. *(Perez & Zeadally, 2018)* The main difference between the two types of wearable devices is that, with consumer wearables, consumers are given the choice to use or not use the device based on their preferences rather than reasons for necessity. Technology for consumer wearable devices has been developing at a rapid pace and more consumers have been using these devices in their daily lives. However, with the development of technology, there has also been an increase in privacy related issues, posing ethical concerns about how consumer wearable users' information is being used. Through this essay, I will be acknowledging the positive aspects of using wearable devices to further enhance self-healthcare systems and discussing the serious privacy concerns that arise as wearable device companies gather and use the consumers' data. I will especially be focusing on the concept of consumer consent, whether consumers are truly knowledgeable of what they are agreeing to, and whether companies understand the implications of how they portray their privacy policies.

There are numerous benefits of using a consumer wearable device from a data-related perspective. As demonstrated through the incident in which an Apple watch saved a man's life by detecting changes in the heart rate data it gathered and informing him of such an irregularity, these devices have developed to the point where someone's life may depend on them. Based on this, consumer wearables enhance health consumers' ability to manage their own health by themselves rather than strictly relying on hospital or medical center visits. Most consumer wearables that track health conditions provide consumers with information about their heart rate, blood pressure, body temperature, physical activity levels, etc. *(Wu et al., 2019)* With such relatively objective data about how our body is functioning, consumers are able to monitor their health easily with somewhat high precision. Wearing a smartwatch allows consumers to have more self-efficacy and control in monitoring and managing their own health.

Therefore, wearable devices can be extremely helpful in self-maintaining one's health from home.

However, there are also a great amount of privacy concerns about using consumer wearables, especially in terms of how the consumers' personal information is gathered and used. One variation of these privacy concerns may be that the consumer's sensitive information about their health is sold or shared with a third-party company which could unethically take advantage of one's vulnerability. Issues regarding privacy breaches of wearable device companies have been happening since the early years when wearable devices were first introduced to the market. As mentioned by Silva in his article, "Fitbit faced a class-action lawsuit in 2011 for allegedly selling personal health data to third-party advertisers without user consent." *(Silva, 2023)* This is problematic because advertisers could unethically market certain products or services to consumers and profit from using their sensitive information that they might not have wanted to disclose. However, such privacy breach issues continue to occur in 2023, indicating that companies and consumers should pay more attention to figuring out the solution to this problem. In addition, the laws and regulations regarding the security of information gathered from consumer wearables are ineffective in protecting the consumers' data privacy. As most consumer wearables are "being used as consumer products instead of purely medical devices, HIPAA and the FDA are unable to provide effective regulatory oversight." *(Langley, 2014)* Due to such conditions, the current issue poses a greater threat with not enough legislative support to secure the consumers' personal data. Therefore, it is extremely important for both parties to be able to take responsibility for their own use and provision of data to promote healthy and safe use of consumer wearables.

Another issue is that the consumers' agreement to the company's privacy policy is almost always required for consumers to be able to use the device. In most cases, consumers must agree to the privacy policy of an electronic device, leaving them with no other choice but to press 'agree.' This may lead consumers to simply skip reading the terms and conditions or the privacy policy as it is highly unlikely that consumers will choose to disagree with the policies and return the product that they have already purchased. According to a survey done by Deloitte, out of 2000 participant consumers, 91% agreed to the terms and conditions without reading them and this rate increased to 97% when the participants' ages ranged from 18 to 34 years old. *(Medine & Murthy, 2019)* Not only that but the privacy statements and information regarding the collection of the consumers' consent are often presented in difficult and inaccessible language to the average consumer. In most cases, if these statements were communicated in a more easily comprehensible way, consumers would be more likely to disagree with the company's privacy policy. According to a study, 97% of

people took only 51 seconds to decide to agree with a privacy statement that should have taken around 30 minutes to read. *(Sui et al., 2023)* Based on this, it may be questionable when companies claim that they have received and collected consent from consumers to gather and analyze their data. Whether firms are able to truly collect consumer consent to use their data is an ethical problem that companies should consider when improving their privacy policies.

From the consumers' perspective, the bigger issue is that these privacy concerns are not taken seriously by the consumers. Consumers may tend to think that the benefits outweigh the risks of using wearable devices and ignore the consequences and possible ethical concerns. According to a survey, "four in 10 US consumers who use smartwatches or fitness trackers are concerned about data privacy." *(Arkenberg, 2021)* The results of the survey indicate consumers are aware of the risks of sharing their personal health data with wearable companies along with third-party companies. However, the long and inefficient privacy policies and terms presented by the firms restrict consumers from knowing how their data is being used and many consumers simply do not know how to protect their data and privacy. If consumers continue to stay ignorant or innocent of the privacy issues of their personal data gathered through consumer wearables, these data privacy issues that have been occurring since the early 2010s will continue to prevail and threaten the privacy of consumers.

The development and use of consumer wearables have been incredibly helpful for consumers' health. It allows consumers to self-manage and monitor their health and be alerted of any irregular changes. However, with enhanced technology and increased use of these devices, more privacy issues have been created throughout the years. Additionally, whether consumer consent truly indicates that consumers are knowledgeable of how their information can be gathered, used, and shared is still a debatable issue. Therefore, it is now important for companies to take action on the implications of ineffective and inconvenient presentations of privacy policies and actively help consumers understand the different ways their information may be used. As a result, consumers will be more informed of the specific data privacy concerns of using a wearable device and make responsible decisions.

References

Arkenberg, C. (2021). *Why consumers—and doctors—are wary about wearable data*. Deloitte Insights. https://www2.deloitte.com/uk/en/insights/industry/technology/wearable-technology-healthcare-data.html

Langley, M. R. (2014). Hide Your Health: Addressing the New Privacy Problem of Consumer Wearables. *Georgetown Law Journal*, *103*(6), 1641–1660.

https://heinonline.org/HOL/P?h=hein.journals/glj103&i=1669
Medine, D., & Murthy, G. (2019). *Nobody Reads Privacy Policies: Why We Need to Go Beyond Consent to Ensure Data Privacy - NextBillion*. https://nextbillion.net/beyond-consent-for-data-privacy/
N/A. (2023, February 20). Apple Watch saves owner's life from fatal internal bleeding after nap, here's what happened. *The Economic Times*. https://economictimes.indiatimes.com/news/new-updates/apple-watch-saves-owners-life-from-fatal-internal-bleeding-after-nap-heres-what-happened/articleshow/98091250.cms
Perez, A. J., & Zeadally, S. (2018). Privacy Issues and Solutions for Consumer Wearables. *IT Professional*, *20*(4), 46–56. https://doi.org/10.1109/MITP.2017.265105905
Silva, J. P. da. (2023, May 4). *Privacy Data Ethics of Wearable Digital Health Technology*. Center for Digital Health | Medical School | Brown University. https://digitalhealth.med.brown.edu/news/2023-05-04/ethics-wearables
Sui, A., Sui, W., Liu, S., & Rhodes, R. (2023). Ethical considerations for the use of consumer wearables in health research. *Digital Health*, *9*, 20552076231153740. https://doi.org/10.1177/20552076231153740
Wu, M., PhD, Luo, J., & Contributors, P. O. J. of N. I. (2019, November 25). *Wearable Technology Applications in Healthcare: A Literature Review | HIMSS*. https://www.himss.org/resources/wearable-technology-applications-healthcare-literature-review