Healthcare Wearable Data Privacy Concerns and Future Solutions for More Accountable Data Handling

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Ramiz Akhtar
Spring, 2021

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signature Ramiz Akhtar Date 04/27/21

Ramiz Akhtar

Introduction

Healthcare wearable manufacturers are left largely unchecked regarding their post-collection handling of user health data even as their user base and influence continue to grow with a forecasted $78 billion increase in global market value for smart healthcare wearables between 2018 and 2025 (Banerjee et al., 2018; Ugalmugle & Swain, 2019). An unprecedented number of people around the world now seek convenient, personalized health insights. The days of healthcare wearables only collecting arguably trivial data, such as steps taken, have passed. An increase in the number of healthcare wearable users has been coupled with advancements in the wearable device capabilities through novel features such as pulse oximetry, sleep tracking, a single-lead electrocardiogram, and even tone analysis to determine a user's emotional state (Amazon.com, 2020; Apple Inc., 2020).

The need for greater transparency from wearable manufacturers regarding data collection practices and data security post-collection has arisen as healthcare wearable devices continue to advance in their sensitive data collection capabilities. Currently, the door is open for users' own health data to be used against them in scenarios such as an increased insurance rates for sleeping less than the healthy recommended standard (Allen, 2018). To better understand how to develop an ethical, sustainable, and modern privacy infrastructure, analysis of the privacy concerns surrounding wearable technologies is required.

Actor Network Theory (ANT) is used to dissect the complex interplay between key artifacts, such as wearable technologies and smartphones, and key stakeholders, such as wearable device manufacturers and consumers, that are all at the center of healthcare wearable privacy. The network perspective provided by ANT allows for an in-depth exploration of relational ties between these artifacts and stakeholders, thus increasing the likelihood of uncovering privacy concerns that

must be addressed for a sustainable privacy infrastructure. To supplement ANT, a framework called technological momentum by Thomas Hughes, a historian of technology, is utilized to emphasize that healthcare wearable technologies are maturing, and thus, are beginning to influence society at large. Therefore, to ensure that healthcare wearable privacy advances alongside healthcare wearable capabilities, the following question must be addressed: as wearable technologies progress, what are the prior, current, and forthcoming data privacy issues with the new generation of wearable technologies?

Literature Review

Imagine a future in which smart contact lenses are able to continuously monitor blood glucose levels for diabetic patients. Alphabet, the parent company of Google, has indefinitely postponed such a project after investing millions of dollars in research and development in an attempt to create wearable technologies of the future (Farr, 2018). While the glucose detecting contact lens has not yet come to fruition, Alphabet's expenditure on the project emphasizes that big technology companies are expecting significant growth in the wearable health technology sector, and thus, are spending heavily to stay ahead of competitors. New wearable technologies present technology companies with the opportunity to collect additional categories of user health data. However, the rate of advancement in privacy standards fails to match the rapid advancement of new health data collection methods.

Currently, wearable device data collection can be explored in terms of user identification, GPS location tracking, sensor-based data, and Internet-of-Things (IoT) data transmission (Banerjee et al., 2018). User identification includes data supplied by the user to the service that corresponds to a particular wearable device, including name, age, height, and weight. GPS location tracking is often used to record the path taken for outdoor exercises such as running. Sensor-based

data sources include heart rate, blood oxygen levels, and a single-lead electrocardiogram. IoT data transmission involves data encryption and transmission to the parent device of the wearable, which is usually a smartphone that contains the wearable manufacturer's proprietary software.

Once health data is collected by the wearable manufacturer's software, users are provided analytical insights into their health. However, beyond the provided health insights, users cannot follow data submitted to a service because data handling post-collection has effectively been black boxed by wearable manufacturers (Purcell & Rommelfanger, 2017). In exchange for insights, the user has effectively given up ownership of personal data. Users must also consider that malicious entities are capable of stealing the data at any moment throughout the health data collection process. In a recently discovered exploit of Apple's iPhone operating system, iOS, malicious parties were able to covertly steal text messages, GPS location, and private health data from users' phones after they visited certain web pages (Beer, 2019). While many wearable manufacturers use a cloud-based service to manage health data collected by the wearable, local copies of the data still exist on the smartphone for efficient access.

Considering the aforementioned privacy issues surrounding the use of wearable devices and their corresponding service, 60% of people interviewed in a study (n=20) were unconcerned about the privacy of their health data after submitting the data to a health wearable service (Lowens et al., 2017). Users who were concerned about health data privacy cited the potential for insurance companies to pay for access to an aggregate of health data and use it to determine insurance rates for customers. In contrast, users who were unconcerned about health data privacy stated that most health data collected, such as steps taken, is trivial and does not require extensive thought about privacy. While metrics similar to steps taken are arguably trivial, the need for greater transparency in data collection practices and data security is apparent considering the rapid advancement of

wearable technologies and new categories of data they can collect. A sustainable and modern privacy infrastructure needs to be in progress to prepare for the inevitable time when health wearables begin collecting even more sensitive health data such as blood glucose and blood pressure.

Methodology

To analyze the intricate problem of health data privacy, the frameworks of ANT and technological momentum are used. ANT provides an analytical basis for a complex network of relationships between technologies, governments, and people by identifying how each relevant stakeholder, physical artifact, and/or non-physical artifact interacts with each other. A primary criticism of ANT is that it ignores "intangible" elements such as values and norms and instead focuses on empirical observation that does not fully encompass a given topic (Cressman, 2009).

To compensate for ANT's shortcoming, technological momentum will be used to support ANT. Technological momentum emphasizes that a technological system must align with the needs of society in its early stages of development. However, as the technology matures and gains momentum, it becomes difficult to alter its trajectory because it has begun simultaneously influencing society at-large (Hughes, 1994).

The primary and secondary modes of conducting research are the documentary research method and policy analysis, respectively. The documentary research method utilizes a variety of sources ranging from technology media articles to peer-reviewed data privacy journals. There are three categories in which research will be organized and analyzed: prior, current, and forthcoming health data collection concerns, all coupled with suggested implementations for improved health data security. The key words researched include "wearable data privacy," "biometric security concerns," and "reading privacy policies." Policy analysis provides a way to evaluate the

implementation of existing legislation in the health data privacy field. The method involves defining shortcomings of current legislation, discussing ways to improve it, and comparing the expected outcome to the current reality.

The key policies analyzed include the Health Insurance Portability and Accountability Act (HIPAA) and the Biometric Information Privacy Act (BIPA), which was passed in the state of Illinois in 2008. In my Prospectus, which proposed this paper, the secondary mode of conducting research was slated to be interviews with healthcare wearable device users after presenting them with the potential data privacy risks associated with using healthcare wearables. The objective was to determine if the public's lack of healthcare data privacy education (as seen in the 2017 study by Lowens et al.) must be promptly addressed, potentially through legislative solutions or grassroots movements, in order to create a healthcare data future with greater accountability. However, due to a risk of COVID-19 transmission and numerous schedule conflicts with interviewees, interviews were replaced by policy analysis, which also highlights pressing obstacles and solutions involved in an accountable healthcare data future although exclusively through a legislative lens.

Analysis

Prior Health Data Collection Concerns

A prior health data collection concern is one that has a resolution in sight. Using ANT, two key artifacts when discussing health wearable data privacy are the wearable devices themselves and the smartphone. The current interplay between these devices involves the wearable device collecting health data points from the user's activities or current body state and transmitting that information to the smartphone often over Bluetooth or Wi-Fi. Once the raw health data is on the smartphone, health insights from the data are either derived on the device or after the smartphone sends the data to the cloud. Transmission of data from the wearable device to the smartphone is

the current standard because wearable devices have lesser processing power in comparison to a smartphone. However, as a result, data privacy is hindered by potentially two opportunities for leakage during data transmission: transmitting from the wearable device to the smartphone, and transmitting from the smartphone to the cloud (Ching & Singh, 2016). To maximize data privacy, raw health data transmission must be minimized. Increasing processing power in wearable devices is a resolution to decrease raw health data transmission. Moore's Law, a prediction by Gordon Moore in 1975 which states that the number of transistors on a processor would double every two years, continues to hold true, meaning processing power continues to steadily increase. In 2020, Intel's head of silicon engineering Jim Keller stated that there are many ways to continue doubling the number of transistors on a chip through innovations such as 3D architectures and new transistor designs (Rotman, 2020). With an increase in processing power, wearable devices would be able to derive insights from health data on-board, thus eliminating the step of transmitting raw health data to the smartphone and the cloud. Transmitting insights over Bluetooth or Wi-Fi is inherently more secure than transmitting the raw data itself. Interpreting data in the form of an insight, such as "your heart rate was on average 10% higher than yesterday," naturally obscures many of its characteristics that can be seen in its raw form, which in this example would be the user's heart rate throughout the day at ten-minute intervals. Therefore, wearable devices have a path forward towards greater health data security.

Current Health Data Collection Concerns

A current health data collection concern is one that does not have a definitive resolution in sight. Continuing the use of ANT, wearable manufacturers and consumers are stakeholders at the center of wearable device health data privacy. While the consumer agrees to the terms of using devices created by the wearable manufacturer, the wearable manufacturer has an ethical obligation

to be transparent with how the consumer's data will be used. However, that is not always the case. Apple has implemented an ultra-wideband chip called U1 into their latest smartwatch, the Apple Watch Series 6 (Espósito, 2020). Ultra-wideband technology allows for more accurate granular location tracking (Wuerthele, 2019). Apple's granular location tracking service is called iBeacon, and it allows developers to leverage the U1 chip to determine the user's precise location in interior spaces if the user has allowed location tracking for a given app (Apple Inc., 2019). An example use case of iBeacon is a gym determining how long a customer who has downloaded the gym's app is spending in each section. While the user would have had to enable location tracking for iBeacon to work, it is not abundantly clear when enabling location tracking that it can entail such granular location tracking (Li, 2019). Although location tracking is not intrinsically health data, the iBeacon example provides a basis to claim that wearable manufacturers are not necessarily transparent in regards to how collected user data can be used. Wearable manufacturers must clearly state the extent of the data collected and how it will be used.

A counter-argument to the discussion of a lack of transparency on behalf of wearable manufacturers is that all potential uses of data are stated in the device's privacy policy. In terms of the ANT analysis, the government and its privacy policy regulations will now be considered. Privacy policies are mandated by law if any personally identifiable information will be collected which includes names, birth dates, and email addresses ("Privacy Policies Are Mandatory by Law," 2020). Every common health wearable service requires at least an email to create an account and begin using the device; therefore, every common health wearable has a privacy policy. However, a central concern with regard to the current state of the privacy policy is the excessive length and neglect for the user's ease of readability. McDonald et al. created a model that determined the national cost for users to read the privacy policy for each website they visited in a

single day. The findings stated that the national opportunity cost for users to read the privacy policies word-for-word was around $781 billion per year. Each privacy policy averaged around 2514 words (McDonald & Cranor, 2008). Considering the opportunity cost and the long length of privacy policies, the current system that emphasizes user self-regulation, where the burden of reading the full privacy statement is on the user, is not ideal for communicating privacy risks to users. Privacy policies should be regulated to ensure that they are readable and convey privacy practices in an accessible way. Ideas for creating a better privacy policy include displaying some high-level topics for a summary of the policy with links into the depths of the full policy for more information as well as infographics that make the privacy information easier to digest. However, part of the responsibility is still on the reader to read these clear and readable privacy policies.

With the current state of privacy policies, users have been encouraged to have a higher risk tolerance with their sensitive health data because of the high opportunity cost to read privacy policies. Fitbit, a prominent health wearable device manufacturer, has stated in its privacy policy that users, "waive any rights of publicity and privacy," in regards to any data users submit to the Fitbit service (Paul & Irvine, 2014). Users effectively lose rights to their health data in order to use the Fitbit service. However, companies might view users waiving their right to health data as a necessary evil. A whitepaper released by a medtech startup called Minimally Invasive Spinal Technology emphasizes that, "a lack of diversity in data and its classification is the biggest culprit when it comes to biased algorithms" (Faruqi & Singh, 2021). It is abundantly clear that wearable device companies crave user health data to better their services and avoid biased and inaccurate health insight algorithms. However, the user should be made clearly aware that the wearable device company intends to use their data in that way.

As previously mentioned, a criticism of ANT is that it ignores values and norms while strictly focusing on non-encompassing empirical evidence. In terms of health data privacy, the ANT analysis above does not consider a wearable manufacturer's potential ethical decision to refrain from irresponsibly using user health data even after owning it per the manufacturer's privacy policy.

Forthcoming Health Data Collection Concerns

As Tim Cook, CEO of Apple, recently stated, "[It is] hard to argue against privacy" (Fathi, 2021). Currently, there exists a need to tighten health data privacy regulations nationwide. As technological momentum explains, a technology becomes less malleable as it matures, allowing it to influence society at-large with decreasing control from those who created it. Whether or not wearable manufacturers choose to use user health data responsibly in the current moment, health wearables continue to become more ubiquitous, more advanced in their feature set, and thus more mature. If proper regulations do not exist in anticipation of health wearables fully maturing, it will be too late in the future to effectively ensure that users' health data is protected and used in a manner they are comfortable with. The window for action in regards to modernizing healthcare wearable privacy is still open but rapidly closing.

The current national standard legally protecting patient health data is HIPAA, which was passed in 1996. HIPAA covers, "all individually identifiable health information that is created, stored, maintained, or transmitted by a HIPAA-covered entity" (Alder, 2018). A HIPAA-covered entity includes health insurance companies and providers such as doctors, clinics, dentists, etc. (CMS, 2020). However, notably missing are wearable device manufacturers because HIPAA does not cover voluntary purchases of wearable devices (Banerjee et al., 2018).

HIPAA must be updated to account for the growing prevalence of wearable health devices from a variety of manufacturers. A critical piece of legislation to model a HIPAA amendment after is BIPA. Although BIPA is a state law in Illinois, it has broadly defined the term "biometric information" to include "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual" (Roberg-Perez, 2017). A broad definition supports user privacy. BIPA also ensures that any entity that stores biometric data must have a policy that clearly describes retention schedule and how users can permanently destroy all of their stored data. In addition, private entities must inform the customer if their data is being used in any new way.

Health data is biometric data based on a study by Na et al. which found that machine learning can be used to take deidentified physical activity from wearable devices and then reidentify the individual from whom the data came from. The algorithm successfully reidentified the physical activity data of 94.9% adults (n=4720). Therefore, taking BIPA's key ideas and amending them to HIPAA would help ensure that there is a uniform federal law to promote transparency regarding how wearable manufacturers are using user health data and ensure that users retain control over their own data as health wearables inevitably continue to advance. In the current year of 2021, it is encouraging that conversation surrounding data privacy reform in general has gained traction. The Massachusetts Institute of Technology launched its Future of Data, Trust, and Privacy initiative in effort to promote technical research and dialogue regarding data privacy within AI and machine learning, both of which are critical tools for generating health insights (Conner-Simmons, 2021). Therefore, the need for advancements in data privacy have clearly been identified and the creation of modern data privacy legislation is a priority.

Conclusion

While health wearables have a path towards greater health data security through advancements in silicon and subsequently reduced data transmission, the privacy policies that govern health wearables must be revised. Wearable device manufacturers need to explicitly state the extent of user data they are collecting and how it will be used. By encouraging more readable, accessible, and interpretable privacy policies, users will have a feasible opportunity to understand how their data is being used and stored. However, as health wearables increase in prevalence and advance in their sensitive health data collection capabilities, a modern regulatory backbone needs to be implemented. Updating HIPAA to broadly protect biometric information and include similar policies to those within BIPA is imperative to ensuring that health wearable manufacturers rapidly adopt practices that promote more accountable data handling. Overall, the window for implementing transparent and accountable data handling practices is closing as healthcare wearables mature, ultimately pushing consumers, wearable device manufacturers, and the government to evolve the current system to one that prioritizes long-term sustainability and security.

References

Alder, S. (2018, March 1). What Does HIPAA Cover? *HIPAA Journal*. https://www.hipaajournal.com/what-does-hipaa-cover/

Allen, M. (2018, July 18). *Health Insurers Are Vacuuming Up Details About You—And It Could Raise Your Rates*. ProPublica. https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates?token=pc1OkzviktiLco0hJY5BDRPpI44H_bKV

Amazon.com. (2020). *Amazon Halo Privacy*. Amazon.Com Help. https://www.amazon.com/gp/help/customer/display.html?nodeId=GL99TQL4B7ADPBDH

Apple Inc. (2019, November). *Location Services Privacy Overview*. https://www.apple.com/privacy/docs/Location_Services_White_Paper_Nov_2019.pdf

Apple Inc. (2020). *Apple Watch Series 6*. Apple. https://www.apple.com/apple-watch-series-6/

Banerjee, S. (Sy), Hemphill, T., & Longstreet, P. (2018). Wearable devices and healthcare: Data sharing and privacy. *The Information Society*, *34*(1), 49–57. https://doi.org/10.1080/01972243.2017.1391912

Beer, I. (2019, August 29). Project Zero: A very deep dive into iOS Exploit chains found in the wild. *Project Zero*. https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html

Ching, K. W., & Singh, M. M. (2016). Wearable Technology Devices Security and Privacy Vulnerability Analysis. *International Journal of Network Security & Its Applications*, *8*(3), 19–30. https://doi.org/10.5121/ijnsa.2016.8302

CMS. (2020, August 2). *Are You a Covered Entity?* https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity

Conner-Simmons, A. (2021, April 20). *MIT launches new data privacy-focused initiative*. MIT News | Massachusetts Institute of Technology. https://news.mit.edu/2021/mit-launches-data-privacy-focused-initiative-fod-0420

Cressman, D. (2009). *A Brief Overview of Actor-Network Theory: Punctualization, Heterogeneous Engineering & Translation*. School of Communication, Simon Fraser University.

Espósito, F. (2020, September 16). Apple Watch Series 6 is the first to include the U1 chip, here's how it could be used. *9to5Mac*. https://9to5mac.com/2020/09/15/apple-watch-series-6-is-the-first-to-include-the-u1-chip-heres-how-it-could-be-used/

Farr, C. (2018, November 16). *Alphabet stops its project to create a glucose-measuring contact lens for diabetes patients*. CNBC. https://www.cnbc.com/2018/11/16/alphabet-verily-stops-smart-lens-glucose-measuring-contact-lens.html

Faruqi, R., & Singh, A. (2021). *Best Practices for Addressing Risks Associated with a Lack of Diversity in Machine Learning*. MINIMALLY INVASIVE SPINAL TECHNOLOGY, LLC. https://s3-us-east-2.amazonaws.com/mist-whitepapers/MIST_Algorithmic_Inclusivity_2021.pdf

Fathi, S. (2021, April 3). *Tim Cook Responds to Facebook Criticism of iOS App Tracking Transparency Changes, Says It's "Hard To Argue Against" Privacy*. MacRumors. https://www.macrumors.com/2021/04/03/tim-cook-responds-facebook-ios-privacy/

Hughes, T. (1994). *Technological Momentum*. MIT Press.

Li, H. (2019, September 17). All the privacy issues Apple didn't talk about at its annual event, and why they matter. *VentureBeat*. https://venturebeat.com/2019/09/17/all-the-privacy-issues-apple-didnt-talk-about-at-its-annual-event-and-why-they-matter/

Lowens, B., Motti, V. G., & Caine, K. (2017). Wearable Privacy: Skeletons in The Data Closet. *2017 IEEE International Conference on Healthcare Informatics (ICHI)*, 295–304. https://doi.org/10.1109/ICHI.2017.29

McDonald, A. M., & Cranor, L. F. (2008). The Cost of Reading Privacy Policies. *A Journal of Law and Policy for the Information Society*, *2008 Privacy Year in Review*, 22.

Paul, G., & Irvine, J. (2014). Privacy Implications of Wearable Health Devices. *Proceedings of the 7th International Conference on Security of Information and Networks*, 117–121. https://doi.org/10.1145/2659651.2659683

Privacy Policies are Mandatory by Law. (2020, July 21). *TermsFeed*. https://www.termsfeed.com/blog/privacy-policy-mandatory-law/

Purcell, R. H., & Rommelfanger, K. S. (2017). Biometric Tracking From Professional Athletes to Consumers. *The American Journal of Bioethics*, *17*(1), 72–74. https://doi.org/10.1080/15265161.2016.1251652

Roberg-Perez, S. (2017). The Future Is Now: Biometric Information and Data Privacy. *Antitrust*, *31*(3), 6.

Rotman, D. (2020, February 24). *We're not prepared for the end of Moore's Law*. MIT Technology Review. https://www.technologyreview.com/2020/02/24/905789/were-not-prepared-for-the-end-of-moores-law/

Ugalmugle, S., & Swain, R. (2019). *Wearable Medical Devices Market Share: 2025 Growth Statistics*. Global Market Insights. https://www.gminsights.com/industry-analysis/wearable-medical-devices-market

Wuerthele, M. (2019, September 10). *Here's what Apple's new U1 chip in the iPhone 11 & iPhone 11 Pro does*. AppleInsider. https://appleinsider.com/articles/19/09/10/heres-what-apples-new-u1-chip-in-the-iphone-11-iphone-11-pro-does