User Perceptions of Accuracy and Data Privacy of Smart Fitness Devices

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, Computer Science, School of Engineering

Jennifer Gulley

Spring 2023

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

Advisor

S. Travis Elliott, Department of Engineering and Society

User Perceptions of Accuracy and Data Privacy of Smart Fitness Devices

Introduction

Smartwatches and fitness trackers are becoming increasingly popular with 190 million shipped worldwide in 2021 and expected to increase to an estimated 280 million in 2024 (Laricchia, 2022). One reason that fitness trackers have become so popular is that they motivate users in their workouts through goal setting (Niess et al., 2020). Smart fitness devices also allow users to connect and share their workout data with friends. "Social interaction" is another "key element to motivate users to perform physical activities" (Chen & Pu, 2014). However, users are concerned about the smart fitness devices' accuracy (Yang et al., 2015) and data privacy (Ioannidou & Sklavos, 2021). Understanding how smart fitness devices collect, analyze, and protect user data provides insightful information into the devices. This STS research project will explore user perceptions of the accuracy and data privacy of smart fitness devices and how the relationship between the devices and society impacts one another.

In order to evaluate the societal impact of smart fitness devices, I will be using the STS framework of Technological Momentum in my research. Thomas P. Hughes put forward the idea of Technological Momentum, which describes a relationship between technology and society. Hughes theorizes that "technological momentum infers that social development shapes and is shaped by technology" (Hughes, 1994). In other words, society shapes technology and technology in turn shapes society. Two critiques of this framework include Technological Determinism and the Social Construction of Technology (SCOT). The former theory states that "technological change drives social change" (Smith, 1994) while the latter asserts the opposite that society shapes technology (Klein & Kleinman, 2002). Rather than a one-way causal relationship between technology and society, Technological Momentum says that technology and society influence and shape one another.

The bidirectionality of the Technological Momentum framework is applicable to smart fitness devices and users' concerns due to the nature of software development. User feedback is a key component in the software development industry, especially as a new technology develops. Users both adapt to the technology while also giving feedback to the producers who then make changes to the technology. Technological Momentum provides a useful framework to analyze the relationship between smart fitness technology and society.

Background: Data Accuracy and Privacy Concerns

Smart fitness devices like the Apple Watch or Fitbit can motivate users and hold them accountable to their fitness goals (Amaral, 2021). While these devices can certainly be beneficial in staying healthy, users also have concerns about them. One concern for users is that they are "uncertain about how accurately their devices track their data" (Yang et al., 2015). Users of fitness trackers certainly want their device to provide them with accurate health information. Otherwise, users will be more likely to stop using the device and to no longer be motivated to work out. Furthermore, receiving inaccurate information from a fitness tracker can cause "heightened anxiety" in users since they might worry about health problems that do not exist (Kussin & Mitchell, 2022). Relying on the information that smart fitness devices provide is significant to people who use these devices for motivation in achieving their fitness goals as well as for keeping track of their general health. Another concern for users is data privacy and security.

Not only are users concerned with the accuracy of fitness devices, but they are also concerned about the devices protecting their data from getting into the wrong hands (Perez, 2019). Smart fitness devices provide an ample amount of health information but also store immense data on their users. Users cannot be completely sure where or how that data is being

stored and protected, which can be cause for concern. In an article written by Phil Muncaster in 2022, he explains that one of the main privacy concerns of fitness trackers is the potential for "location-based threats." Muncaster explains that a hacker might be able to gain valuable insights into a user's location throughout the day based on their fitness tracker which "could enable [the hacker] to physically attack the wearer, or their car/household at times it is judged to be empty." Understanding how smart fitness devices protect data is important for users to feel safe and secure when using these devices.

How Accurate is Data Tracking?

To get an idea of how accurate smart fitness devices are, we will look at three main categories that these devices track: step count, heart rate, and calories burned. According to a 2020 study, a fitness tracker worn on the wrist was compared to a "research grade" tracker to determine accuracy of step counting. The wrist worn tracker and the research grade tracker both performed well at counting steps at a certain speed but both trackers miscount steps at slower walking speeds, and the wrist worn tracker also miscounted steps at higher walking speeds (Woodland, 2022). One user of a smart fitness tracker noticed that steps were not counted when pushing a stroller but were counted when rocking a baby (Yang et al., 2015). Step counting seems very dependent on the activity that the user is doing.

On wrist worn devices, heart rate is measured by LED light that is shown into the skin on the wrist and the device measures how much red and green light is being absorbed (Exist, 2016). However, tattoos or moving your arm too much can interfere with accurate measurements (Exist, 2016). In a Harvard study in 2020, heart rate measurement was tested on six different fitness trackers. Participants completed four different activities: "sitting still, breathing deeply, walking, and typing," and they wore electrocardiogram patches as the baseline for the true heart rate

(Harvard Health, 2020). The researchers found no differences in heart rate between the trackers and the electrocardiogram patches for people with different skin tones. However, the researchers found heart rate differences for different activities where walking caused the reported heart rate to be greater than the true heart rate, and typing caused the reported heart rate to be lower than the true heart rate. However, according to a study at the Stanford University School of Medicine, six out of seven "devices measured heart rate with an error rate of less than 5 percent" for walking and running on treadmills or using stationary bicycles (Dusheck, 2017). It seems that smart fitness trackers can measure heart rate reasonably well, but error increases when measuring heart rate for more complicated tasks. This is to be expected since wrist worn trackers do not meet the same standards that medical grade trackers must meet.

According to the Stanford study, none of the smart fitness trackers measured calories burned accurately. In fact, "the most accurate device was off by an average of 27 percent" (Dusheck, 2017). Calories burned is determined through a calculation based on other information like movement and/or heart rate. The tracker does not actually know how many calories one is burning but is rather making an educated guess (Skwarecki, 2022). Heart rate seems to be the most accurate measurement for fitness trackers followed by step count. Calories burned, however, is highly inaccurate.

How Protected is User Data?

The data tracked by smart fitness devices can be rather personal and therefore users want their health information to be protected. To get a sense of how smart fitness devices protect user data, we will examine four companies: Apple, Fitbit, MyFitnessPal, and Strava. According to Apple's and Fitbit's privacy policies, both companies encrypt user data to protect it from hackers (Apple, Inc., 2023; Fitbit, 2022). However, data encryption alone does guarantee protection from

hackers gaining access to personal health information. GetHealth, a health and wellness company, exposed over 61 million records of fitness tracking data from Apple and Fitbit due to a database that was not password protected (Roberts, 2021). It is concerning that health data from Apple and Fitbit was leaked through a third party, and users should be wary about how exactly their data is being protected.

MyFitnessPal also experienced a data breach that "exposed the usernames, passwords, and email addresses of over 150 million users" in 2018 (Kaspersky, 2021). While a hacker may not be able to steal your identity from fitness data, he may be able to launch phishing attacks from the data gathered which can be dangerous for users who are unaware of what these scams look like (Lukic, 2021). Under Armour (who owns MyFitnessPal) was not aware of the breach until a month after it occurred but announced the problem after four days, significantly quicker than most companies would announce the issue (Lukic, 2021). Although a data breach should not occur in the first place, Under Armour was communicative with its users which can help prevent some users from experiencing negative effects of the data leak.

Another application that experienced a security flaw was Strava, an app where users can track their running and cycling (*Running, Cycling & Hiking App*). Strava put out a heatmap of where users were running or cycling, and this led to exposing the locations of secret United States military bases (Brown, 2022). Not only did it reveal the locations for these bases, but it also revealed patterns of activity "down to the identities of individual soldiers and the routes they take" (Martin, 2018). Data leaks such as this one can be dangerous to many people and shows why security of these devices is important.

Aside from data breaches, another privacy concern for users is that smart fitness device companies may sell user information to third party companies. Although they remove personal

identification, “Fitbit…collects your information to sell to third parties” (Kaspersky, 2021). Simply because data is de-identified does not mean that it is completely anonymous (Wetsman, 2021). This is concerning for users as they do not want their personal information in the possession of other people. In addition, the Health Insurance Portability and Accountability Act (HIPAA) does not protect users’ health information from being shared or sold if it was collected via fitness trackers (Kaspersky, 2021). It is concerning that the law to protect people’s health information does not apply in all circumstances.

Technological Momentum and Smart Fitness Devices

Viewing smart fitness devices through the Technological Momentum framework provides insight into how these devices affect society and vice versa. Three areas of how fitness tracking technology and society influence each other will be examined.

Supply and Demand

The supply and demand of fitness trackers is a good example of how the technology influences society and how society in turn influences the technology. When a technology succeeds, people will want to buy it. According to the Worldwide Survey of Fitness Trends, the number one fitness trend in 2022 was wearable technology (Thompson, 2022). As with any trend, people want the newest and trendiest technology. Smart fitness devices have recently become this technology. Devices that produce accurate health information and protect users’ privacy will result in higher demand and will therefore further drive the development of this technology.

COVID-19 could have been a social factor that contributed to smart device popularity and increasing the demand for the products (Osborne, 2021). As people were stuck at home and

could not go to gyms, smart fitness devices helped people to keep up on their exercise. Additionally, the social network aspect of these devices made it easier for people to connect with others that they probably would not have been able to spend time with due to the pandemic. The pandemic shaped how society operated which changed consumers' demand for these products. When there is demand for these devices, other companies will jump in and produce their own versions of fitness tracking technology. Society drives the development of technology through their market demand.

Users' negative perceptions about the accuracy and privacy of their personal health data can drive the development of the technology. Developers create products for users, and then users request changes to improve the product. As users feel that the smart fitness devices are failing, they will request changes, and demand for the products will decrease until the necessary changes have been made. Users may shape the devices as the demand changes due to inaccurate and unprotected data.

Staying Fit

Smart fitness devices provide "motivation to achieve personal bests" and "healthy competition" (Lupton, 2017). These devices can create a society that is concerned about their health and can encourage people to stay active. The social network aspect of these devices promotes sharing your activity with your friends. Sharing health data with friends gamifies exercise and creates a competitive atmosphere which can make exercise more enjoyable. This gamification is a result of technology shaping society as well as society shaping technology. The technology to share your data shapes a culture of competition with exercise. Society's culture then influences the companies to further gamify their technology.

HIPAA

Smart fitness device companies can sell/share user health information since this information is not protected under HIPAA. The technology's lack of privacy pushes society in a way that may lead to changes in laws. A new act has been introduced called the Stop Marketing And Revealing The Wearables And Trackers Consumer Health (Smartwatch) Data Act to "ensure that health data collected through fitness trackers, smartwatches, and health apps cannot be sold or shared without consumer consent" (Alder, 2019). If this law passes, the smart fitness device companies would have to adapt to not sell or share user data and may need to change their technology to better protect user data. This potential law is evidence of technology shaping society, and with this law, society will be shaping technology.

Discussion

To explore users' perceptions of smart fitness devices, I investigated the accuracy of the data tracking and the security of user data. Different features of fitness tracking devices are more accurate than others. Heart rate is the most accurate feature of fitness trackers and calories burned is not accurate at all. It is up to the user to decide what measurements are important to him or her. It is also important to remember that these fitness trackers are not medical instruments and therefore are going to be less accurate than a medical grade health monitor. Keeping this in mind, fitness trackers still provide a good estimate for health measurements and can be more beneficial than having no estimate at all. A user should not make important health decisions based on fitness tracker data but should instead consult a doctor if something seems wrong.

Regarding the data protection of smart fitness devices, different companies have different systems in place to protect user data. Companies like Apple and Fitbit encrypt user data and make users aware of this so that they can feel secure. However, data encryption alone will not prevent data breaches and there is the risk in any company that data will be leaked. Users should take special precautions when it comes to their personal fitness data. One thing users can do is to adjust the settings of the application to ensure their data is not being shared with other apps. This will help minimize who has access to your data. Another thing users can do to help protect their data is to be aware of and recognize phishing scams. Users should never provide fitness trackers with sensitive information like their social security number. Users should also be aware of the specific companies' privacy terms to know whether the company may sell or share data with third parties. With any company that a user provides personal information, there is a chance that information could be stolen or sold to others. Ultimately, it is up to the user to determine if the risk of their fitness data being leaked is worth the use of smart fitness devices.

Consumers should and do raise their concerns regarding these devices so that companies make the necessary changes to improve their products. User feedback is essential in developing the technology further. Whether it is positive or negative feedback, companies will likely take users' thoughts into account when developing the next version. In this way, society is directly driving the development of the technology. The technology also shapes society in that its success or failure will affect users in some way. When the technology succeeds, a culture of staying active, "counting steps," and competing with your friends to burn the most calories arises. When the products do not meet user expectations, consumers might take action to influence the technological development or to make societal changes. With the Smartwatch Data Act, the

failure to secure data may cause society to implement new laws to better protect users. In this way, technology is shaping society.

Conclusion

Users' perceptions of smart fitness devices are important for the development of technology. Two areas of user concern include the accuracy and privacy of the devices; therefore, these issues were investigated. By examining the step counting, heart rate, and calories burned features of smart fitness devices, it was determined that certain features are more accurate than others. Smart fitness device companies try to protect user data, but no company can 100% ensure that data is protected. For some, using slightly inaccurate or potentially unsecure fitness trackers might be better than nothing, while others may choose to forgo the devices. A user's tolerance for the potential issues with smart fitness devices is subjective to the individual, and users must decide for themselves whether to buy these products.

In order to understand how smart fitness devices and society interact with each other, the framework of Technological Momentum was utilized. Technological Momentum states that technology both shapes and is shaped by society. Smart fitness devices are shaping society by the mere fact that they are becoming so popular. Users also shape the products with their feedback. Users find problems like data inaccuracy or unprotected data, and companies must make changes so that users continue to buy their products. Failure of the devices could also lead to societal changes as seen with the potential new law, the Smartwatch Data Act. Technological Momentum was a useful tool to explore how smart fitness devices and society impact one another.

References

Alder, S. (2019, November 25). *Smartwatch Data Act Introduced to Improve Privacy Protections for Consumer Health Data*. HIPAA Journal. Retrieved May 5, 2023, from https://www.hipaajournal.com/smartwatch-data-act-consumer-health-data/

Amaral, T. (2021, April 30). *The Pros & Cons of Fitness Trackers*. wellnessworkdays. Retrieved September 12, 2022, from https://www.wellnessworkdays.com/post/the-pros-cons-of-fitness-trackers

Apple, Inc. (2023). *Protecting access to user's health data*. Apple Support. Retrieved March 17, 2023, from https://support.apple.com/guide/security/protecting-access-to-users-health-data-sec88be9900f/web

Brown, A. (2022, June 22). *Security flaw in Strava, a social fitness app, exposed identities of Israeli soldiers at military bases*. Forbes. Retrieved March 17, 2023, from https://www.forbes.com/sites/abrambrown/2022/06/20/strava-fitness-app-israeli-mossad-data-breach-security-hack-segments/?sh=a82e44c68d7d

Chen, Y., & Pu, P. (2014). Healthytogether. *Proceedings of the Second International Symposium of Chinese CHI on - Chinese CHI '14*. https://doi.org/10.1145/2592235.2592240

Dusheck, J. (2017, May 24). *Fitness trackers accurately measure heart rate but not calories burned*. Stanford Medicine. Retrieved March 16, 2023, from https://med.stanford.edu/news/all-news/2017/05/fitness-trackers-accurately-measure-heart-rate-but-not-calories-burned.html

Exist. (2016, February 21). *How do fitness trackers measure your heart rate?* Retrieved March 16, 2023, from https://exist.io/blog/fitness-trackers-heart-rate/

Fitbit. (2022). *Fitbit Privacy Policy*. Fitbit. Retrieved March 17, 2023, from https://www.fitbit.com/global/us/legal/privacy-policy

Harvard Health. (2020, May 1). *How accurate are wearable heart rate monitors?* Retrieved March 16, 2023, from https://www.health.harvard.edu/heart-health/how-accurate-are-wearable-heart-rate-monitors

Hughes, T. P. *Technological Momentum*. (1994). Cambridge, Massachusetts. London, England. The MIT Press.

Ioannidou, I., & Sklavos, N. (2021). On General Data Protection Regulation Vulnerabilities and Privacy Issues, for Wearable Devices and Fitness Tracking Applications. *Cryptography, 5*(4), 29. https://doi.org/10.3390/cryptography5040029

Kaspersky. (2021, September 3). *Do fitness trackers put your privacy at risk?* www.kaspersky.com. Retrieved March 17, 2023, from https://www.kaspersky.com/resource-center/preemptive-safety/fitness-tracker-privacy.

Klein, H. K., & Kleinman, D. L. (2002). The Social Construction of Technology: Structural Considerations. *Science, Technology, & Human Values,* 27(1), 28-52. https://doi.org/10.1177/016224390202700102

Kussin, Z., & Mitchell, A. (2022, January 26). *Why fitness trackers are doing more harm than good*. New York Post. Retrieved November 1, 2022, from https://nypost.com/2022/01/26/why-fitness-trackers-are-doing-more-harm-than-good/

Laricchia, F. (2022, May 5). *Smartwatch and fitness tracker shipments worldwide 2021-2024*. Statista. Retrieved October 18, 2022, from https://www.statista.com/statistics/1290443/smartwatch-fitness-tracker-shipments/

Lukic, D. (2021, February 1). *How Under Armour's App MyFitnessPal Got Hacked*. IDStrong. Retrieved March 17, 2023, from https://www.idstrong.com/sentinel/myfitnesspal-data-breach/

Lupton, D. (2017, December 19). *The social factors that influence whether you'll use your wearable device*. The Conversation. Retrieved March 17, 2023, from https://theconversation.com/the-social-factors-that-influence-whether-youll-use-your-wearable-device-89080

Martin, D. (2018, January 30). *Pentagon reviews fitness tracker use over security concerns*. CBS News. Retrieved March 17, 2023, from https://www.cbsnews.com/news/pentagon-reviews-fitness-tracker-use-over-security-concerns-fitbit/

Muncaster, P. (2022). *Every breath you take, every move you make: Do fitness trackers pose privacy risks?* WeLiveSecurity. Retrieved November 1, 2022, from https://www.welivesecurity.com/2022/01/26/every-breath-you-take-every-move-you-make-fitness-trackers-privacy-risks/

Niess, J., Knaving, K., Kolb, A., & Woźniak, P. W. (2020). Exploring fitness tracker visualisations to avoid rumination. *22nd International Conference on Human-Computer Interaction with Mobile Devices and Services*. https://doi.org/10.1145/3379503.3405662

Osborne, C. (2021, January 12). *Covid-19 a 'significant' factor in wearable device adoption, market surge*. ZDNET. Retrieved May 5, 2023, from https://www.zdnet.com/article/covid-19-a-significant-factor-in-wearable-device-adoption-market-surge/

Perez, A. J. (2019, August 16). *Use a fitness app to track your workouts? your data may not be as protected as you think*. USA Today. Retrieved September 12, 2022, from https://www.usatoday.com/story/sports/2019/08/16/what-info-do-fitness-apps-keep-share/1940916001/

Roberts, D. (2021, September 27). *Apple Healthkit and Fitbit Records of 60 million users exposed*. IDStrong. Retrieved March 17, 2023, from https://www.idstrong.com/sentinel/apple-healthkit-and-fitbit-records-of-60-million-users-exposed/

Running, Cycling & Hiking App. Strava. (n.d.). Retrieved March 17, 2023, from https://www.strava.com/

Skwarecki, B. (2022, June 2). *Why you can't trust your fitness tracker on calorie burn*. Lifehacker. Retrieved March 16, 2023, from https://lifehacker.com/why-you-cant-trust-your-fitness-tracker-on-calorie-burn-1849003730

Smith, M.R. (1994). Technological Determinism in American Culture. *Does Technology Drive History?: The Dilemma of Technological Determinism*. (pp. 1-17). Cambridge, Massachusetts. London, England. The MIT Press.

Thompson, W. (2022). *Worldwide survey of fitness trends for 2022*. ACSM's Health & Fitness Journal. Retrieved March 17, 2023, from https://journals.lww.com/acsm-healthfitness/Fulltext/2022/01000/Worldwide_Survey_of_Fitness_Trends_for_2022.6.aspx

Wetsman, N. (2021, June 23). *Hospitals are selling treasure troves of medical data - what could go wrong?* The Verge. Retrieved May 5, 2023, from https://www.theverge.com/2021/6/23/22547397/medical-records-health-data-hospitals-research

Woodland, R. (2022, July 27). *How accurate are fitness trackers?* LiveScience. Retrieved March 16, 2023, from https://www.livescience.com/how-accurate-are-fitness-trackers

Yang, R., Shin, E., Newman, M. W., & Ackerman, M. S. (2015). When fitness trackers don't 'fit'. *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing - UbiComp '15*. https://doi.org/10.1145/2750858.2804269