How do Wearable Users' Expectations of Security and Privacy Align with the Actual Practices of Wearable Companies?

Ava Kowalski, *Colorado School of Mines* Akshitha Mudupu, *Colorado School of Mines*
Griffin Rutherford, *Colorado School of Mines*

Abstract

The team's research focuses on wearable devices developed by Apple and Garmin, specifically their smart watches. These watches collect different types of data that give insights to users about their physical health and lifestyle. Many users are unaware that other parties are given access to the data and whether the companies are following security and privacy practices. To address the research question, the team's approach used a mixture of analysis of company policies combined with user surveys. As a starting point, the team surveyed a representative sample of wearable users to ascertain their knowledge of data collection methods, perceived security risks, and trust in their devices' privacy safeguards. From the results of this survey, the team was able to conclude that most users' expectations of companies do not align with the statements in the privacy policies. In this paper, the team will discuss their motivation behind the research question, limitations of the research, as well as future work to improve this research.

1. Introduction

Wearable devices like smartwatches and fitness trackers capture highly sensitive health data such as heart rate, sleep patterns, and GPS locations that expose deeply intimate details of users' lives. Unlike healthcare providers, wearable companies are exempted from HIPAA rules, hence a regulation gap that subjects users' data to uncontrolled collection, sharing, or exploitation. The data, for example, would be sold to third parties used in predictive modeling without users' knowledge or consent, or leaked in security breaches. Knowledge of the gap between users' perception of companies' use of their data and companies' actual use is fundamental to advocating for more strict requirements of privacy, raising public awareness, and making manufacturers responsible for ethical use of their data.

By comparing perceived expectation to documented company behavior, the team aimed to ascertain areas of dissonance between expectation and reality—such as misperceiving data-sharing methods or overestimating protections of regulation. This approach was beneficial in a number of ways. By triangulating qualitative observations of users with quantitative analysis of policy, the team restricted the potential for a single-method study to be skewed towards a particular point of view, offering a more balanced picture. Analyzing highly used brands meant that the team's findings were actionable for policymakers and users, and participant recruitment across a range of groups (athletes, occasional users, technical groups) increased the results' generalizability. The transparency of the team's methods—working with publicly accessible policies and anonymized survey results—was also amenable to reproducibility and accountability, in keeping with the project's ethical goals. Overall, this work sought to allow users to be informed decision makers around their data and to push companies towards more transparent, more ethical methods of handling privacy in a sector in which innovation often precedes regulation.

2. Motivation

As the team mentioned earlier, most of the data from wearable devices do not fall under HIPAA protection, unless accessing Protected Health Information. HIPAA (Health Insurance Portability and Accountability Act) "establishes federal standards protecting sensitive health information from disclosure without patient's consent" [1]. Because Apple and Garmin are manufacturers and app developers of these smart watches, they must comply with HIPAA to ensure data security/privacy with health information [2]. Looking through Apple and Garmin's privacy policy, there is no mention of HIPAA. This is an example of when Garmin users' data should be regulated by HIPAA: "We may also transfer your personal data to an affiliate, a subsidiary, or a third party in the event of any reorganization, merger, sale, joint venture, assignment, transfer, or other disposition of all or any portion of our business" [3]. Personal data includes health data as well aside from location, name, email address, etc.

Another point of motivation for the team was to comprehend the data pipeline that Apple and Garmin follow with the watch data. Users are not aware of the design for gathering data, and companies are not transparent. Although it wasn't clear of the exact steps that Apple and Garmin take to process the data, there is a general pipeline that

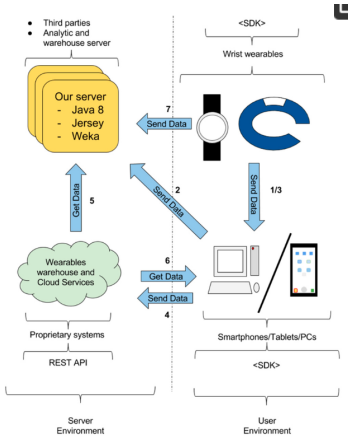

Figure 1: A diagram representing the data pipeline such as collecting data, storing, and sending data back to the cloud or device

companies follow for data collection/storage. In Figure 1, it shows the path taken from a user and cloud perspective. The two ways data is collected are through API and SDKs. With an API, the data can be pulled periodically and shared with multiple parties without the user's knowledge. SDKs use the apps to collect data in real-time directly from the device, often without a way to stop it. The data is then stored in the cloud, and can also be sent back to the device.

2.1. Related Work

The team looked at multiple articles of similar research that has been done on this topic. Another point of motivation was to see if there is a correlation between age and awareness of security and privacy. One article that was important to the research was "Analysis of Security and Privacy Issues in Wearables for Minors". This study investigates the security and privacy vulnerabilities in wearable devices targeted at minors, a demographic particularly sensitive to data protection issues. The authors stress the urgent need for stricter regulations to ensure wearable manufacturers implement robust privacy and security safeguards, especially when products are intended for vulnerable populations like minors [16]. The team's project built on and differed from the work of Fúster et al. by shifting focus from technical diagnostics to user perception and regulatory awareness. While their study provided a rigorous analysis of vulnerabilities in wearables, particularly those marketed to minors, the team's project investigated whether users were aware of such vulnerabilities and how this awareness (or lack thereof) shaped their behavior.

Another article that further emphasized the team's point of transparency was "Wearable Devices in Healthcare: Privacy and Information Security Issues". This article illustrates key weaknesses in both security controls and privacy protocols of existing wearables. Cilliers found that manufacturers used subpar methods of encryption, sometimes sending information in plaintext, leaving it vulnerable to being intercepted by ill-intentioned parties [17]. Data-retention policies were unclear or completely absent, so it was unclear how long users' information stayed on servers or how long it may be stored. Perhaps worst of all was the transparency of the practice of sharing: users were not informed clearly if and how their information was shared with third parties, for purposes of analysis, promotion, or other stated purposes. In contrast to Cilliers' expansive security framework, the team linked these concerns back to user trust, albeit on the question of whether users were aware of such risks and how companies were able to manipulate such ignorance to drive behavior.

3. Methods

3.1. Data Collection

For this study, the team recruited wearable device users to assess their awareness of data security in wearable technology. Since wearable devices, such as smartwatches and fitness trackers, are not required to be covered under HIPAA regulations, there was a gap in understanding how personal health data is protected. Participants were recruited from university athletic programs and fitness communities. Participants completed a survey designed to assess their understanding of wearable security and privacy. They were asked about their perceptions of what health and activity data are collected, such as EKG readings, heart rate monitoring, and GPS tracking. For data collection and analysis, the team used Google Forms for surveys, along with Python libraries and Excel to structure and process collected data.

To ensure the validity of the study, internally, all participants received the same survey and instructions to maintain consistency. Externally, the team recruited a diverse sample across different wearable brands and user demographics to ensure the findings were generalizable. The validity was reinforced by cross-referencing participant responses with published scholarly articles and official company privacy policies to curate an accurate comparison between user expectations and actual data security practices.

3.2. Data Analysis

Because the team's data came from the various wearable companies and surveys the team conducted, most of the data was qualitative. When researching the wearable companies, the team's goal was to analyze their privacy policies, data/user permissions, privacy rights, etc. Some important things the team paid attention to and considered when performing the initial research of these companies was to take note of what data they collected, if they were sharing the data with others and who, and how users could protect their data. With the survey, the team asked participants questions to gauge their opinions and awareness about security and privacy related to their wearables. Appendix A has the questions and answer choices the team asked in the survey.

3.3. Qualitative Analysis of Open-Ended Responses

For the open-ended survey questions (7, 8, 11, and 12), the team employed thematic analysis to identify recurring patterns in user responses. Responses were first coded by identifying key concepts, then grouped into emerging themes. This qualitative approach allowed the team to capture nuances in user perceptions that would not be apparent from quantitative data alone.

For example, when asked what they believed privacy policies entailed (question 8), responses typically fell into three categories: those expressing certainty (though often incorrect) about protection, those expressing

confusion/uncertainty, and those expressing cynicism about corporate data practices. The cynicism theme was particularly prevalent among older respondents (24+), suggesting age-related differences in trust toward technology companies.

3.4. Analysis Methods for Quantitative Data

For the quantitative survey data, the team primarily utilized descriptive statistics to analyze response patterns. This included:

1. Frequency distributions to identify the most common responses across different categories
2. Cross-tabulation to examine relationships between variables (e.g., age group and comfort with third-party data sharing)
3. Graphical representations through bar charts to visualize response patterns across different demographic groups

The descriptive statistics provided valuable insights into general trends and patterns within the sample population. The breakdown of responses by age groups (17-19, 20-23, and 24+) and by device brand (Apple, Garmin, Other) allowed the team to identify potential patterns in how different demographic groups perceived and understood wearable data privacy.

From these survey results, the team could see different perspectives and how much people showed importance to security and privacy regarding their medical data. The team could also observe trends and what their expectations were of these companies. This survey helped the team be able to generalize results, with participants from different age groups and education levels.

4. Results

The total number of responses of the survey the team received was 43. The team focused on comparing the results by age groups, 17-19, 20-23, 24+, to generalize easily. Below, are the results of the survey questions by age:

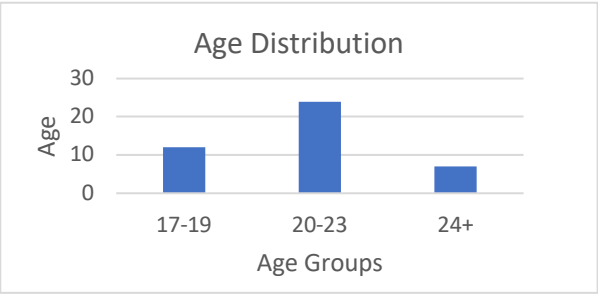

Figure 2: Overall age distribution from survey responses

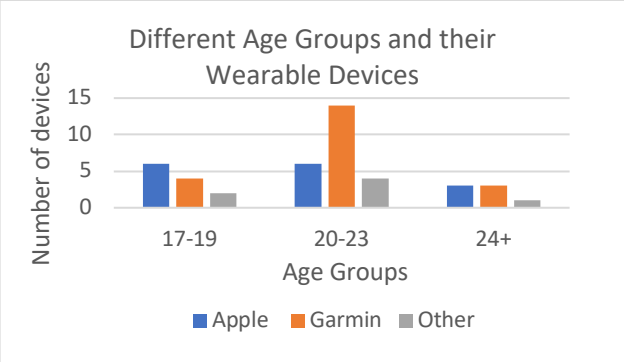

Figure 3: Distribution of watch brands between age groups

The next graphs convey the different perspectives of third parties between the different age groups.

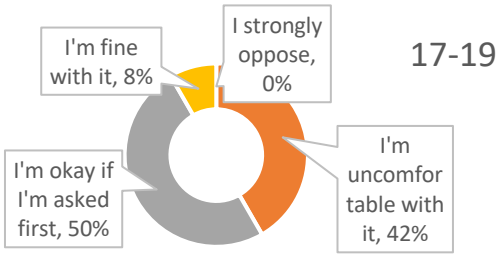

Figure 4: Responses to this question, how do you feel about third parties potentially accessing your wearable data, that were of the ages 17-19

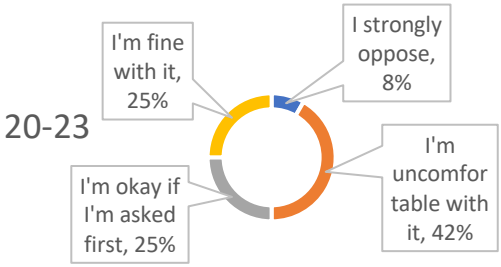

Figure 5: Responses to this question, how do you feel about third parties potentially accessing your wearable data, that were of the ages 20-23

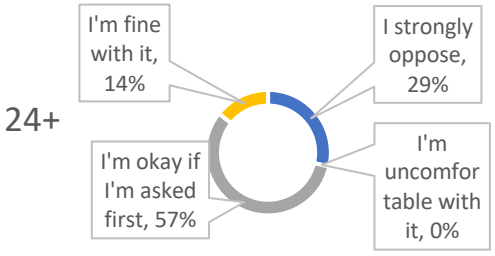

Figure 6: Responses to this question, how do you feel about third parties potentially accessing your wearable data, that were of the ages 24 and up

The next graphs show the responses of all participants with questions related to data collection and the company privacy policy, based on wearable device company.

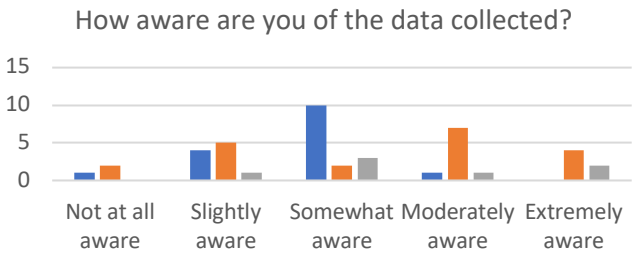

Figure 7: Responses of total participants by brand for the question, how aware are you of the data collected?

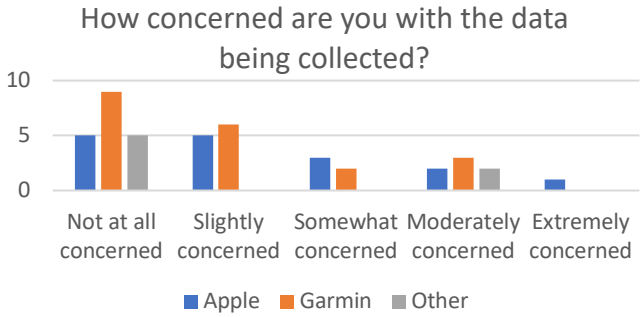

Figure 8: Responses of total participants by brand for the question, how concerned are you with the data being collected?

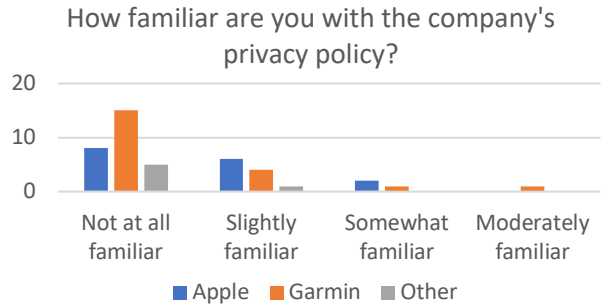

Figure 9: Responses of total participants by brand for the question, how familiar are you with the company's privacy policy?

The final graph depicts the percentage of participants that are comfortable sharing data.

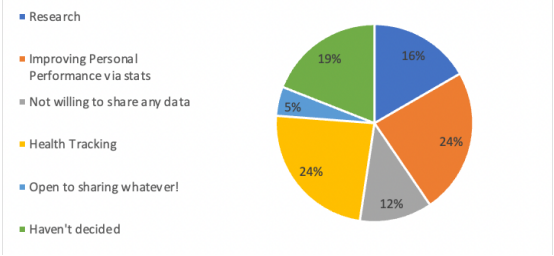

Figure 10: Responses of total participants for the question, what reasons would you be comfortable sharing your data?

5. Discussion

Based on the team's survey results, there is a clear disconnect between users' expectations of privacy and the actual practices of wearable companies. The data reveals several key findings worth discussing:

Many wearable users across all age groups express concern about third parties accessing their data, with 42% of younger users (17-19) and 42% of college-aged users (20-23) reporting being "uncomfortable" with third-party access. Among older users (24+), 29% "strongly oppose" such sharing, indicating potentially greater privacy awareness with age.

The team's findings indicate that despite companies like Apple and Garmin collecting sensitive health data including heart rate, sleep patterns, and GPS locations, users generally have limited awareness of how this data is processed. This is particularly concerning given that these wearable companies are not required to comply with HIPAA regulations that would otherwise protect such health information.

The complexity of privacy policies appears to be a significant barrier to user understanding. As shown in Figure 9, the vast majority of participants across all brands reported being "not at all familiar" or only "slightly familiar" with their device's privacy policy. This indicates that the current approach to transparency through lengthy, legally complex privacy notices is failing to effectively inform users.

Regarding data collection awareness, the team observed varying levels across different device brands. Apple users predominantly reported being "somewhat aware" of data collection practices, while Garmin users displayed a more distributed range of awareness levels. This suggests different companies may have varying approaches to communicating their data collection practices.

Additionally, the team's analysis of company privacy policies revealed concerning practices, such as Garmin's disclosure that they "may transfer personal data to an affiliate, a subsidiary, or a third party in the event of any reorganization, merger, sale, joint venture, assignment, transfer, or other disposition" of their business. This broad language essentially permits sharing of health data with minimal restrictions, yet most users remain unaware of these provisions.

The qualitative responses from the open-ended questions (questions 7, 8, 11, and 12) further reinforced these findings. When asked what they believe their devices collect, many

users identified obvious metrics like heart rate and step count, but fewer mentioned the more sensitive data being gathered such as sleep patterns, GPS location history, or menstrual cycle tracking. This suggests a gap in understanding the breadth and depth of data collection.

Most concerning was the disparity between users' expectations of data protection and the regulatory reality. Many respondents expressed an assumption that health data from their wearable would be protected similarly to medical records, unaware that most wearable data falls outside HIPAA protections. This regulatory gap leaves sensitive health information vulnerable to sharing, analysis, and potential exploitation without robust oversight.

The implications of these findings are significant both for consumer awareness and potential regulatory reform. As wearables become increasingly integrated into healthcare ecosystems through features like atrial fibrillation detection and blood oxygen monitoring, the line between consumer product and medical device continues to blur, yet the regulatory framework has not evolved accordingly.

6. Limitations

The team's relatively small sample population of about forty participants compromised the statistical power and generalizability of the results, since low sample numbers can lower the scientific and ethical standards of the conclusions derived from research findings [4][5]. The use of self-reported survey data also inserted potential inaccuracies because of social desirability and recall bias to the data, where subjects could exaggerate familiarity with or concern for practices related to privacy information [6]. The cross-sectional survey approach only examined user attitudes at a snapshot in time and did not permit determination of how awareness or company policies change and could not determine causal effects between variables since it did not analyze the data at several moments in time [7]. The choice to consider only Apple and Garmin devices narrowed the range of data examined. Still, wider surveys of hundreds of manufacturers demonstrated much greater heterogeneity of practices about which the team's two-company approach could not inform [8]. Lastly, the qualitative review of policies did not feature formal readability or linguistics analyses; previous work indicates that the majority of health-related privacy policies are at least at the twelfth-grade level, beyond the understanding of many users and probably lessening policy familiarity [9]. Consumer-grade wearable sensors were also subject to quantitatively measurable errors—sleep-stage errors greater than 20 percent and heart-rate discrepancies under some conditions—that could mask user views of device dependability and subsequent effects on privacy [10].

7. Future Work

Future studies should engage a much larger and demographically representative cohort, informed by careful sample-size calculations to achieve adequate power and external validity [11]. Using longitudinal or mixed-design studies—following surveys with follow-up interviews or focus groups—would track the dynamic of increasing awareness of one's privacy and permit causal exploration of factors leading to user trust [12]. Broadening studies to span through a larger range of wearable brands and device types would give an improved picture of industry-wide practices, as shown in analyses across thousands of smart-device policies [8]. Experimental evaluation of in-app summaries of privacy, interactive consent modules, or notice layering is essential to find which interventions do best to increase user understanding, leveraging lessons from eye-tracking experiments on wearability of privacy-policy reading on wearables [13]. Lastly, comparative studies of regulatory models—like GDPR's plain-language obligations and possible enlargements of HIPAA's covered entities—could help inform policy reforms to fill existing disparities in consumer health-data protections [14][15].

8. Conclusion

The team's mixed-methods investigation disclosed an evident dissonance between data collection as perceived by wearable users and the actual practices of manufacturers regarding data privacy. While Apple and Garmin employed opt-in frameworks for data sharing and intensive encryption protocols, the complexity and length of their privacy notices undermined user understanding and impaired informed consent [3][9]. The prevailing regime, which barred most consumer-purchased wearables from HIPAA protection, put valuable health data at the mercy of the market and highlighted the necessity for extended legislative coverage [2]. Through the intersection of qualitative user insights with quantitative policy analysis, the present work mapped out actionable avenues—like user-centered consent UIs and improved plain-language notice—to advance transparency, build consumer trust, and inform the evolution of wearables' privacy regulation [14].

9. References

[1] Centers for Disease Control and Prevention. (n.d.). *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*. CDC Public Health Law Program.
[2] MedSafe. Does HIPAA Apply to Wearable Health Technology? MedSafe, n.d.
[3] Garmin Ltd. Global Privacy Policy. Garmin, n.d.
[4] Kumari M, Srivastava S. Sample Size and its Importance in Research. PMCID: PMC6970301, 2019.
[5] Vickers AJ. Sample size considerations in research. Endodontology, 2023.

[6] Fisher RJ, et al. The relationship between social desirability bias and self-reports of mental health and substance use. PMC5519338, 2017.
[7] Chandrashekara S. Methodology Series Module 3: Cross-sectional Studies. PMC4885177, 2016.
[8] Hamid A, Samidi HR, Finin T, et al. A Study of the Landscape of Privacy Policies of Smart Devices. arXiv preprint, 2023.
[9] Graber DA, D'Alessandro MP, Johnson-West C. Reading level of privacy policies on Internet health Web sites. ResearchGate, 2002.
[10] Strahler J, Coughlin ED, et al. Evaluating Accuracy in Five Commercial Sleep-Tracking Devices. Sensors, 2024;24(2):635.
[11] Kumari R, Srivastava K. How to choose a sampling technique and determine sample size for external validity. ScienceDirect, 2024.
[12] CDC. Cross-sectional studies: strengths, weaknesses, and recommendations. PubMed 32658654, 2020.
[13] Fritscher BF, Huang Y, et al. Read or skip privacy policies when installing apps on wearable devices. Nature, 2024.
[14] Gal M, Meijer L, et al. Law in Books and Law in Action: The Readability of Privacy Policies. SSRN, 2018.
[15] Howard T. Does HIPAA Apply to Wearable Health Technology? MedSafe, 2023.
[16] Sharma A, Kumar R. A Survey on Wireless Sensor Networks. *Wireless Networks*, 2022.
[17] Cilliers, L. (2020). Wearable devices in healthcare: Privacy and information security issues. *Health Information Management Journal, 49*(2–3), 150–156.

Appendix A

1. What is your age?
2. What best describes your current status?
3. What is your major/educational background?
4. What brand of wearable device do you use?
    a. Apple
    b. Samsung
    c. Garmin
    d. Other
5. On a scale of 1-5, how aware are you of the data collected by your device?
    a. 1- Not at all aware
    b. 2- Slightly aware
    c. 3- Somewhat aware
    d. 4- Moderately aware
    e. 5- Extremely aware
6. On a scale of 1–5, how familiar are you with your wearable company's privacy policy?
    a. 1- Not at all familiar
    b. 2- Slightly familiar
    c. 3- Somewhat familiar
    d. 4- Moderately familiar
    e. 5- Extremely familiar
7. Can you describe the types of data you believe your wearable device collects about you?
8. What do you think wearable device privacy policies means for how your data is used?
9. On a scale of 1–5, how concerned are you with the data collected by your device?
    a. 1- Not at all concerned
    b. 2- Slightly concerned
    c. 3- Somewhat concerned
    d. 4- Moderately concerned
    e. 5- Extremely concerned
10. How do you feel about third parties (e.g., advertisers, insurers, researchers) potentially accessing your wearable data?
    a. I'm fine with it
    b. I'm ok if I'm asked first
    c. I'm uncomfortable with it
    d. I strongly oppose it
11. For what types of insights would you be willing to share more data?
12. Imagine your data is being shared with a third party. What would you want to know?

Team Contributions

Throughout all tasks during this project, all the team participants did an equal share of the work. For any write ups, each team member was assigned a specific section and was completed by a set deadline. Same goes for presentations, each member did a number of slides and presented on the completed slides. For research, each team member focused on different parts of the project such as the related works, company policies, wearable devices, etc. When creating the survey, all team members contributed to generating questions.