Wear is the Privacy? - A Comparative Analysis of the Apple Watch and Xiami's Mi Band

Manya Sachdev

May 10, 2024

Abstract :

Wearable technology is slowly cementing its place in everyday life. Some call it "the closest thing to under the skin sensors". Such a product becomes an extension of the wearer. Thus, it is imperative to make sure that the user is not unknowingly exploited. Through a thorough examining of privacy policies, data collection architecture and consent practices, this paper presents a comparative analysis between two popular solutions for wearable technology in the market, the Apple Watch and Xiaomi's Mi Band. Investigation into the two products reveals significant differences in the way data is handled and perceived. Apple looks at data as something to be protected. Xiaomi, considers it a free asset. The insights reveal multiple implications in terms of user outlook towards products. By using the Apple watch as a benchmark for approval, we examine and identify gaps in Mi Band's architecture and offer solutions for improvement.

Index Terms: Wearable Technology, Apple Watch, Xiaomi, Mi Band, Privacy, Data, Consent

1 Introduction

Wearable technology has observed a heightened growth over the last decade. In the fitness industry specifically, devices such as the Apple Watch, FitBits, Garmin and other similar variants have changed the landscape and become inseparable assets for activity management and tracking. Naturally, with the global increase in usage of such devices, the question of privacy arises. Do users really know what data is being collected? Is the purpose behind particular data collection clear and warranted? Is the data being worked upon internally or are hidden, external parties involved in backstage processes?

In this paper, we focus our study on a specific subset of data collected by two devices, the Apple Watch and the Mi Band. We examine health and fitness metrics such as heart rate, sleep patterns, activity levels, and other manually logged data. Fitness tracking and health monitoring is a common use case of the two devices and hence has been selected as the focus of this study. Additionally, we will examine the life-cycle of this data collected within the larger data ecosystem. This will help us map out each stage of a data unit's journey and the privacy concerns faced along the way. In doing so, we consider data collection, data storage, data transmission and data utilization in a well segmented and structured manner. We will compare the two devices on the basis of some predefined metrics.

The expected outcomes include identifying potential privacy risks, system leaks and security vulnerabilities in one of the devices when compared to the other. We benchmark each result to known privacy principles and risk-aversion measures, assessing effectiveness with respect to competitor practices.

2 Literature Review

Data collection is an increasingly relevant topic in today's digital world. Solove defined four categories of damaging practices in this domain, detailing how such practices can result in severe privacy breaches which may cause harm to users. The four categories defined are Information Collection, Information Processing, Information Dissemination and Invasion. These are umbrella topics and are expanded into sub areas such as surveillance, monitoring etc. Datta, n.d.

A study conducted on tech wearables indicated several interesting results Mahinderjit, n.d. For the purpose of the experiment, a wearable sensor was administered to over sixty voluntary participants. The aim was to measure the level and magnitude of concern among users of such technology, what abstractions or de-identification procedures are applied to collected data and if who the receiver of the data collected is significant. It was found that participants expressed maximum concern when the data being collected was personal. Further, when temporal and geo-locationary tags were added to the data, concern level rose significantly and apprehension of being identified were heightened. Lastly, if the receiver was declared to be one of the researchers, the concern level among partipants on average was considerably less than if the receiver was declared to be a larger public population. This implies that people do care about who can see there data.

In another study detailed in the same paper, it was found that consumers did not consider metrics related to their daily activity to be note-worthy or sensitive. Interestingly, it was also found that "the lack of a physical keyboard on the device (technology wearable) prevented them from entering and storing any sensitive information thereby leading to a false sense of privacy." In one-on-one interviews conducted as part of the study, one participant doubled down on their supposed trust on a company, citing the example of a real case where Apple refused the FBI in their request to bypass the security passcodes set on an iPhone by a accused criminal.

Some more interesting results yielded as part of the study was the metrics that define perceived risk in a product. These consider the contextual scope of data collected, the sensitivity attributed to the data and the duration for which the data is stored. An example from the experiment tells us that a small subset of the participants considered "fitness bracelets" more risky when compared to a shoe-embedded activity tracker.

Certain companies are vague in their privacy policies, especially with regards to the location of operation. Different nations have different laws and the weaker ones are often exploited for being so. Mahinderjit, n.d.

3 Data Collection

3.1 Apple Watch

Health data collected by the Apple Watch can be divided in to two main categories - Automatically collected or *default collection* and Manually logged.

Automatically recorded:

1. Heart Rate and Blood Oxygen Measurements: The device houses inbuilt heart rate sensors that are always active. They take heart rate measurements on a periodic basis and automatically send a copy of the data points to the Health app on both the watch and the associated iPhone. Similarly, certain models of the watch (Series 8 and above) are equipped with advanced sensors that can measure blood oxygen levels and send automatic alerts to the user in care of an unusual dip or irregularity in measurement. The data is stored and aggregated on-device. A copy is reflected on the phone app where users can browse trends in figures and closely examine details.
2. Activity Metrics: The device meticulously tracks activity metrics such as stand hours, steps and calories burnt. It allows users to set flexible target values and sends reminders via notifications throughout the day to help the user meet them. In addition to just the values for these metrics, the watch records the concentration and frequency of activity at particular points during the day. It uses such measures over a period of time to define a user's *usual activity* or time-annotated movement patterns. Arm movement and accelerometers are used for this purpose.
3. Noise Level: The device automatically detects abnormalities in noise levels and sends alerts when sounds are excessively loud or over a predefined decibel.
4. Time Spent in Daylight: Certain models of the device (Series 6 and over) are equipped with ambient light sensors that measure how much time the user, i.e. the watch, has spend in the sun.

Manually logged (optional):

1. Menstrual Data: The Apple Watch is inbuilt with a period-tracker app that allows users to log exact dates and time related to their menstrual cycle. It performs on-device computations on this data and send alerts regarding fertility windows to the user.
2. Sleep Data: The device allows users to set a customizable sleep schedule. This allows both the Apple Watch and the associated iPhone to estimate time spend at rest/in bed.
3. Miscellaneous: The Health app on the device also allows users to log details related to current medications and body measurements. Information about body measurements has been declared to be used by the device to improve the accuracy of the activity metrics measured.

3.2 Mi Band

Mi Band has been known to exploit gaps in company policies to increase the scope of data collection. They collect information about users through both direct and indirect sources. Direct refers through first-hand interaction with a Xiaomi product. Indirect refers through aggregation methods applied on data collated from third party sources, both publicly affiliated and those separate.

Some of information collected includes:

1. Exercise Metrics: The Mi Band collects a large number of data points with respect to activity metrics. This includes steps taken, *score of health condition*, time and targets of exercise, whether the targets have been met, stride frequency and length, calories, altitude of operation etc.
2. Biological Metrics: These include sleep data, oxygen saturation level and variation, heart rate - resting and active, weight. All of the above mentioned data metrics are automatically synchronised across Xiaomi accounts and devices.
3. Phone Details: Any time the device is used to answer a phone call or view a text message, Xiaomi records low level details related to each transaction. These include specific phone numbers, message content, contact details as stored in the device etc.
4. Music App Metrics: The device keeps a record of music control function, a feature that is not present in most other competitors in the market. Names of songs played by the user, volume the device was operated at are just some of the details that are collected automatically by a Xiaomi phone and transferred to the Mi Band.
5. External Devices: If any external device (NOT a Xiaomi product) has been paired with the Mi Band, operational details for the external item are collected. These include unique identification numbers, IP addresses, model numbers, operating system details etc.
6. Miscellaneous: Usage details such as battery percentage and charging status are also collected.

4 Comparitive Anaysis

Table 1
Snapshot comparison between Apple and Xiomi with respect to privacy principles

Practice	Apple	Xiomi
Data Aggregation	Maybe	Yes
Data Minimization	Yes	No
Transparency	Yes	Maybe
Purpose Limitation	Yes	No
Purpose Specification	Yes	No
Accountability	Yes	No
Limit Retention	Yes	No
Consent	Yes	No
Default Setting	Opt-In	Opt-Out
Computations	On Device	Off Device

There are several severe and concerning fallacies in Xiaomi's architecture that warrant more than a raised eyebrow. A renowned cybersecurity researcher Gabi Cirlig, conducted an indepth, computational analysis on Xiomi Devices."Exclusive: Warning Over Chinese Mobile Giant Xiaomi Recording Millions Of People's 'Private' Web And Phone Use" n.d.

4.1 Data Collection

Xiaomi heavily uses both its smartphone and Mi Bands, to closely monitor and track large volumes of user data. This includes metrics such as browser history, app usage details, device metadata,

biological information etc. The collected data is not just stored on-device for user functionality purposes. In addition to most computations being held off-device, the raw data itself is transmitted to remote servers in different parts of the world. Here, laws pertaining to the location of the data server are followed, regardless of the region of operation and usage. In comparison, Apple prides itself on following the principles of *Privacy by Design*. It minimizes data collection from its devices and limits the scope to what is truly necessary to provide a specific service.

4.2 Encryption and De-identification

According to Xiaomi's documentation (public and private sources), data collected is well encrypted to ensure no leakages during the many transfers it is a part of. However, no or weak de-identification processes seem to have been applied, leading to hackers - both ethical and harmful - being able to decode and map data to individuals effectively. The encryption methods used by the company have failed in the past and large amounts of users' personal data has been found scattered on various parts of the internet. Apple on the other hand, follows strong and robust de-identification methods on any and all data collected. Till now, apart from one attack in 2021, no significant leaks have occurred and anonymisation practices seems to have been successful.

4.3 Consent

While Xiaomi states a long list detailing out various ways in which data is collected, monitored, stored and used, it has been found that Xiaomi often takes user consent to be *true* by default and sends sensitive browser data to its remote serves. This data from mobile browsers is collected even if users are in incognito mode. This practice is in stark contrast to the processes followed at Apple. Here, the company is notorious for prioritising user consent and security. They are extremely transparent in their services.

4.4 Third Party Involvement

Third Party Involvement is a factor that is heavily debated. Lack of transparency with regards to an additional party's privacy practices leave a grey area for user data to be exploited without their knowledge. Xiaomi uses multiple third party applications to support its internal business practices. These parties are not required to follow the same privacy standards (not that they are super high to begin with). This leaves room for violating user trust. Sensor Analytics is one such company contracted by Xiaomi to provide statistics and insights on users' behavioral habits. The company was found to have copies of device and browser data from Xiaomi devices on its local domain servers. Apple holds a very strong benchmark when it comes to partnering with third party applications. It informs users when a third party is involved in a data transaction at the exact moment and allows individuals to choose whether to green light the transaction or not. By default, the Apple watch does not share any metrics with third parties.

4.5 Grievance Redressal

A significant difference found between the two companies is the way they respond to privacy concerns. On multiple occasions, Xiaomi has explicitly denied research findings and allegations with regards to how it collects and uses user data. In one instance, they doubled down on their anonymisation methods and claimed that collecting browser data, even sensitive, is done only to improve product delivery. Apple on the hand hand, takes privacy concerns very seriously. It has set processes in place that take detailed notes of grievances. On investigating serious claims, they are quick to spring into action. They declare findings of their security and privacy investigations publicly and release software updates to help fix them. At every stage of the process, users of the product are aware of the situation and possible vulnerabilities in the system.

4.6 Privacy Governance

Xiaomi's Mi Bands collect both personal and impersonal data. The purpose is not well-defined but has been loosely stated to be *product functionality*. Though attempts have been made by the company to be open and transparent about data collection practices, there is a clear lack of a structured governance procedure. There has never been any mention of formal privacy assessments conducted nor has there been any sign of partnerships with civil and judicial authorities. *The Apple falls very far from the tree.* Apple designs most of its products around the principles of privacy by design - data minimization, purpose limitation, privacy by default, consent architecture, access control, execution verification. The company is extremely transparent in the exact mechanisms used at each stage. Consent mechanisms are a common practice and data minimisation is a standard. Further, they have a dedicated Privacy Steering Committee that oversees operations and acts as the point-of-contact to raise compliance issues. Apple also conducts regularly scheduled Privacy Impact Assessments during and after product development for continued improvement. With regards to data security, they posses two certifications, ISO 27001 and ISO 27018. With regards to cross-border data transfer, Apple follows the APEC Cross Border Privacy Rules. It is unclear whether Xiaomi follows similar practices.

5 Discussion

Shockingly, according to Xiaomi's stated policy, even if a user opts out of certain features, the company and its devices may override such requests. An excerpt from their privacy documentation states, "Even if you opt-out, we may still collect and use information under certain exceptions such as providing you with a product or service; meeting our legal obligations; detecting and preventing security incidents, misuse and fraud; auditing, research, analytics and measurement; verifying and maintaining the quality or safety of services and devices; identifying and repairing errors and bugs; and other notified or expected purposes. We may also send you certain non-promotional communications regarding HUAMI and our products and services, and you will not be able to opt out of those communications (e.g., communications regarding updates to our Terms or this Privacy Policy)."

Comparing Xiaomi's Mi Band to the Apple Watch is very eye opening. It is glaringly evident which company cares about the user and product ethics and which company is okay with stretching privacy requirements. Apple lays down a strong emphasis on *Privacy by Design*. It incorporates strict encryption protocols and emerges as a front runner in protecting data. Xiaomi, is veering very hard to the other side of the spectrum. Its track record as detailed by previous examinations of its data collection practices and disclosure methods, point to an untrustworthy product.

Regulatory compliance and certifications such as CCPA and

GDPR are useful in evaluating and comparing privacy practices. However, while Apple has shown alliance to such measures of user protection, Xiaomi has not shown the same level of commitment.

A recurring issue of *consent* emerges when examining Xiaomi's architecture, and also the larger wearable technology space. Apple reflects consent architecture at every, granular stage. Xiaomi has not displayed the same sentiment. Data collection mechanisms are unclear and data sharing practices are open to interpretation according to the language used in the documentation provided by them.

With the Mi Band 6 in particular, we can see several fallacies in the privacy architecture.

5.1 Lack of Transparency on Company Ownership

The device, the Mi Band 6, is sold and developed by different companies. Xioami is the parent seller while the Zepp Health Corporation is responsible for developing the technology. The same company has also contributed to the technology behind Amazon's fitness tracker, the Amazfit. To users, the privacy policy that is pushed on the device is Xiaomi's general privacy policy. However, according to previous investigations of the device, when company representatives were asked to provide device-specific guidelines, investigators were provided with a document signed by Zepp Health Corp. This document has not been shared publicly by the organisation, but excerpts have been floated on the internet by independent researchers. This has caused mass confusion with regards to the device's data management practices. The lack of clarity, transparency and accountability forges roots for distrust between consumers of the product and the company.

5.2 Data Sharing

Xiaomi is transparent in selling/sharing personal data collected from the Mi Band to third parties, both publicly affiliated and separate. The purpose is not explicitly stated in the privacy documents but it is speculated to be for target advertising purposes. However, it is unclear exactly how much and what data is shared. The affiliated companies are not listed and declared. All external parties are allowed to follow disparate privacy policies on the data once they receive it.

6 Conclusion

The comparative analysis carried out yields insightful results and highlights the difference in the level of adherence to privacy practices by two large companies in the same market. Apple Watch has come out as a lot more secure and trustworthy. The Mi Band lacks in accountability, transparency, and consent. Further, the unclear ownership status of the parent company, Xiaomi, only adds to the level of distrust and concern in its practices. The difference between explicitly stated practices and the actual occurrences found by cybersecurity specialists is alarming to say the least.

Future research on this topic of tech wearables could explore and experiment with more innovative solutions to enhance user privacy and autonomy. **How can we help the company reach its objective and supply the best possible product while simultaneously ensuring the protection of user data?** Interdisciplinary collaboration between software engineers, hardware experts, doctors and network specialists can help design better systems that meet the the maximum possible objectives for all co-existing parties.

Acknowledgements

This research received support during the Digitisation and Privacy course, instructed by Professor Subhashis Banerjee, Ashoka University.

References

Datta, Prerit (n.d.). "A Survey of Privacy Concerns in Wearable Devices". In: *IEEE* (). URL: https://ieeexplore.ieee.org/abstract/document/8622110.

"Exclusive: Warning Over Chinese Mobile Giant Xiaomi Recording Millions Of People's 'Private' Web And Phone Use" (n.d.). In: (). URL: https://www.forbes.com/sites/thomasbrewster/2020/04/30/exclusive-warning-over-chinese-mobile-giant-xiaomi-recording-millions-of-peoples-private-web-and-phone-use/?sh=624644961b2ahttps://apple.com/in/privacy/labels/.

Mahinderjit, Manmeet (n.d.). "Wearable Technology Devices Security and Privacy Vulnerability Analysis". In: *Research Gate* (). URL: https://www.researchgate.net/publication/303870892_Wearable_Technology_Devices_Security_and_Privacy_Vulnerability_Analysis.

"Mi Band 6" (n.d.). In: (). URL: https://foundation.mozilla.org/en/privacynotincluded/mi-band-6/.

"Mi Smart Band 6 PRIVACY POLICY" (n.d.[a]). In: (). URL: https://assets.mofoprod.net/network/documents/Mi_Band_6_Privacy_Policy.pdf.

"Mi Smart Band 6 PRIVACY POLICY" (n.d.[b]). In: (). URL: https://assets.mofoprod.net/network/documents/Mi_Band_6_Privacy_Policy.pdf.

"Privacy Evaluation for Apple Watch" (n.d.). In: (). URL: https://privacy.commonsense.org/evaluation/Apple-Watch.

"Privacy Governance" (n.d.). In: (). URL: https://www.apple.com/legal/privacy/en-ww/governance/.

"PRIVACY POLICY" (n.d.). In: (). URL: https://www.mi.com/uk/about/privacy/.

"Putting Our Bodies Online: The Privacy Risks of Tech Wearables" (n.d.[a]). In: (). URL: https://www.cigionline.org/articles/putting-our-bodies-online-the-privacy-risks-of-tech-wearables/.

"Putting Our Bodies Online: The Privacy Risks of Tech Wearables" (n.d.[b]). In: (). URL: https://www.cigionline.org/articles/putting-our-bodies-online-the-privacy-risks-of-tech-wearables/.

"This is how we protect your privacy." (n.d.). In: (). URL: https://www.apple.com/in/privacy/approach-to-privacy/index.html?ref=thedigitalspeaker.com.

"Transparency is the best policy." (n.d.). In: (). URL: https://apple.com/in/privacy/labels/.

"Xiaomi Health Privacy Policy" (n.d.). In: (). URL: https://privacy.mi.com/xiaomihealth/en_US/.