

Wearables & Data Privacy



Ji Su Yoo, Harvard University
June 2018

Abstract

Wearable technologies collect intimate personal health and activity data from users – how do companies handle this data? Where does all the data go? This report examines examples of data practices of four wearable and medical technologies as stated on their public websites. In this report, privacy is not considered merely as the absence of intrusion or the right to be left alone but the right to own and control one’s personal data. Currently, consumers in the United States have little control over how companies handle their personal data. MyDataCan, a doubly-encrypted data storage service, can be an optimal tool to restore an individual’s ability to control how they share personal data.

Wearables and Data Privacy



The consumer wearables market has exponentially increased in the past few years. According to Business Insider intelligence, consumer use of smartwatches and fitness trackers has increased from 9% in 2014 to 33% in 2018 [1]. One of the main motivations for using wearables is to monitor health and activity. The hope is that daily and longitudinal health data will help consumers better understand and improve their fitness and health lifestyles. There are many different types of wearables that are currently in the market:

- **Fitness trackers** monitor various physical activity metrics such as distance walked or ran, steps taken, calories consumed or burned, and heart rate. Their most common use is for exercise and improving one’s quality of physical health.
- **Wearable patches** have been enjoying a rising prevalence in the wearable healthcare market. These types of wearables take on the form of sticker-like adhesives that are applied to the skin, containing sensors that detect the wearer’s electrons to power itself. They are designed to be strong enough to always stay attached to the wearer’s skin, even if they are sweating, wearing clothing, or exerting harsher physical force. Some types of wearable patches contain medication, regularly releasing doses to the body over a set interval; these are used as alternatives to needles [2].

- **Smart apparel** are items with built-in technology that the consumer puts on their person. Examples of smart apparel include virtual reality headsets and glasses with tech such as Google Glass. Some types of smart apparel are set to take “wearable technology” to the most literal extreme; a few companies are planning to develop clothing items like shirts, shorts, and sweaters with sensors woven into the fabric that record the wearer’s various fitness-related statistics [3].
- **Smart watches** also monitor physical activity but they also have most of the functionality of a smartphone.
- **Posture monitors** help the user take care of the way they stand up, sit down, or lie down by detecting the curvature of their back and reporting ways in which they can improve their posture. These devices are usually attached to the back of the wearer’s neck, vibrating softly should they slouch their back [4].
- **Movement and vital sensors** frequently sample the motion of the user’s limbs and joints by means of a gyroscope or accelerometer. From that, the user can access the raw kinematic data of their movement. [5]
- **Chest straps** specifically target the state of the wearer’s chest, and as such, are mostly used to monitor the user’s heart rate.
- **Smart footwear** captures data pertaining to physical activity that requires movement, particularly the motion of the foot. As such, they tend to record information such as steps taken, distance walked or ran, and the elevation of ground. More intricate forms of smart footwear can even track the user’s muscular fatigue level. [6]

With all of these wearables, data handling and privacy protections differ depending on company practices. American polls have repeatedly found that Americans value privacy protections and there is now more awareness about privacy policies and data sharing practices [7]. However, privacy practices for companies are not always clear, making it difficult to know exact privacy risks. Consumers also may decide privacy the benefits of a fitness tracker outweigh their concerns about privacy. After all, there is no recourse for disagreeing with a company’s data handling practices except to not use a product. For athletes whose careers depend on physical performance, the benefits of performance analytics can likely overshadow privacy concerns. In recent years, companies have included more secure data handling practices, but they do not yet provide users with full control of how their personal data is handled. Below are five examples of wearables and how companies have arranged data handling.

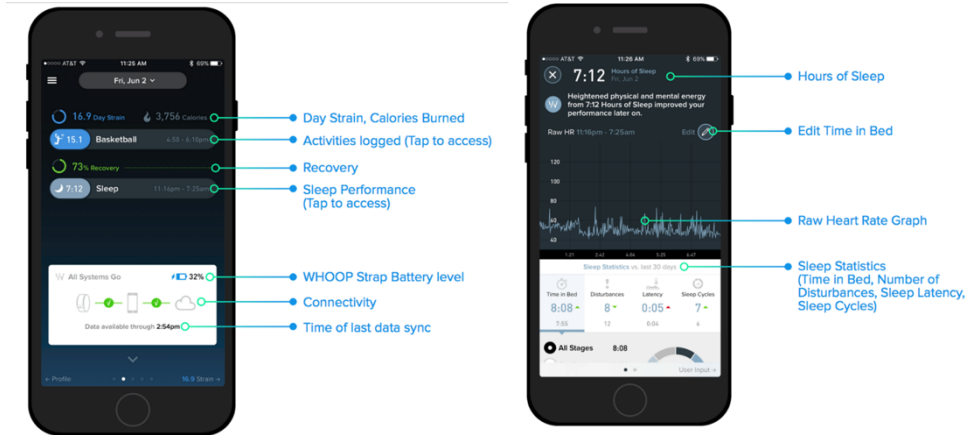
Apple Watch



Apple Watch health data is always stored local to the device itself; none of the data is shared to the company's own cloud storage service, iCloud. Apple's developer forums shows how users can verify this themselves [8]. The user can back up the device's data on iCloud, delete all the data from the device, and attempt to restore the deleted data from iCloud. Upon doing so, the user will see that the health app's data will not be recovered along with the rest of the personal data formerly on the device.

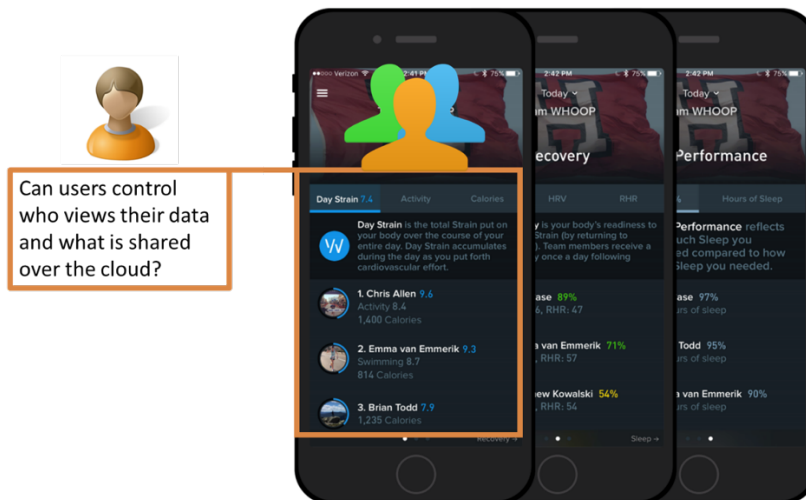
Apple HealthKit [9] and ResearchKit [10] are two open-source development frameworks for smartphone and smartwatch applications and medical research. If a user agrees, developers can build apps that use Apple Watch data for research studies or make consumer facing apps that help users gain insight about the personal health data. Users must authorize access to their Apple Watch data and the user must also be able to view, export, and share the data. Furthermore, users can input information directly into the Health App to supplement their Apple Watch data including information about allergies and medications.

Whoop



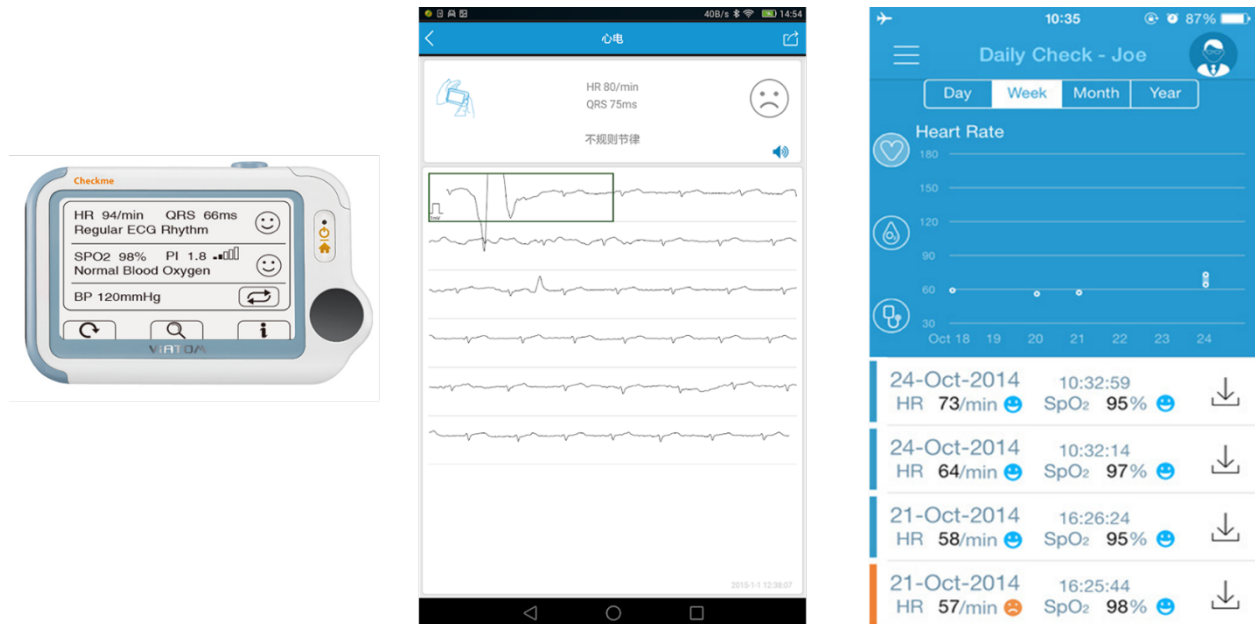
Whoop [11] offers professional analytics for recovery, sleep, and activity metrics, which is attractive for athletes who rely on their health for a living. Indeed, athletes and sports teams are primary users of Whoop fitness trackers. With user permission, Whoop transfers personal data back to its servers to then provide analytics and networking services for users.

For teams, the “Team Whoop” feature allows users to view other teammates’ statistics and progress. One goal of this feature is to build a social accountability and healthy competition within teams that use the app. It is unclear whether users can refuse to share data with their teammates and coaches. The Whoop website does not state any option to store the data locally without sacrificing access to the services and valuable features of the app [12]. It uses AES-256 encryption to secure personal data.



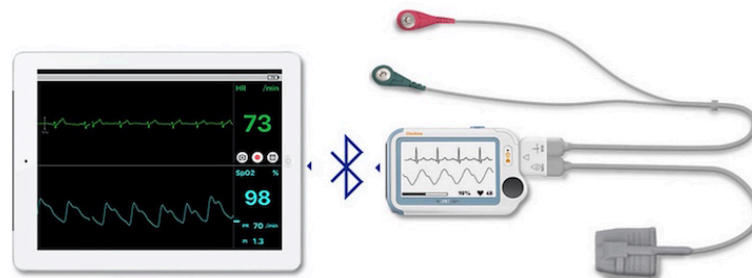
Can users control who views their data and what is shared over the cloud?

Viatom



The Viatom CheckMe Pro [13] medical tricorder is a portable scanning device that records basic vital measurements. The CheckMe Pro includes a pedometer, blood pressure tracker, pulse oximeter, electrocardiography (ECG) signal and waveform, and sleep apnea monitor. The product includes:

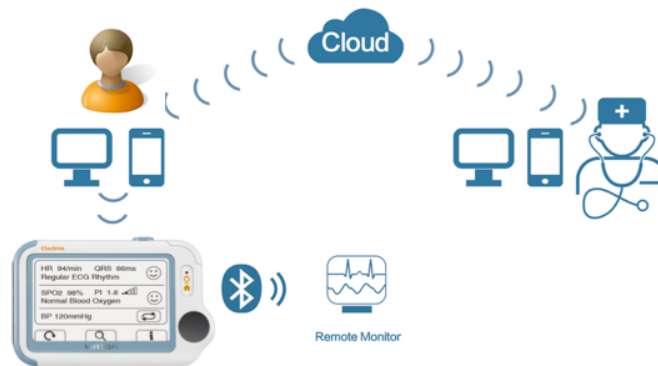
- An electrocardiography (ECG) cable with 2 lead wires that snap together
- An SpO2 finger sensor 25cm wide, FP-10
- ECG electrode, 10pcs



Viatom CheckMe pro allows users to share their vitals with a doctor or family member. Any data sharing with the physician must first be authorized by the user. This device would allow doctors to receive data about their patients even when doing remote check-ups. If the user accepts, their data is transmitted to Viatom's servers using the following protocol:

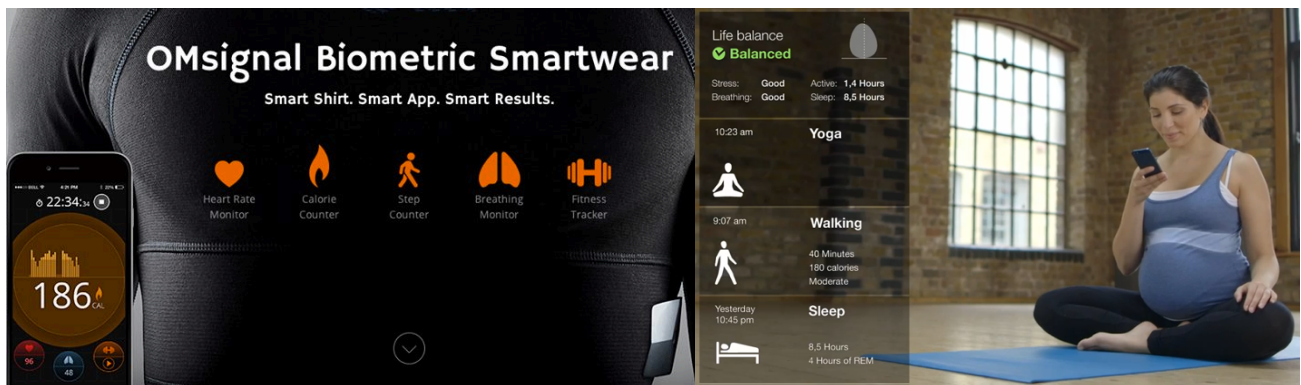
- Data is synced to the cloud automatically
- Data is shared to doctor automatically
- Data is stored in the cloud long term
- Data is properly encrypted to protect users' privacy

- Integrated solution to setup self-governed cloud

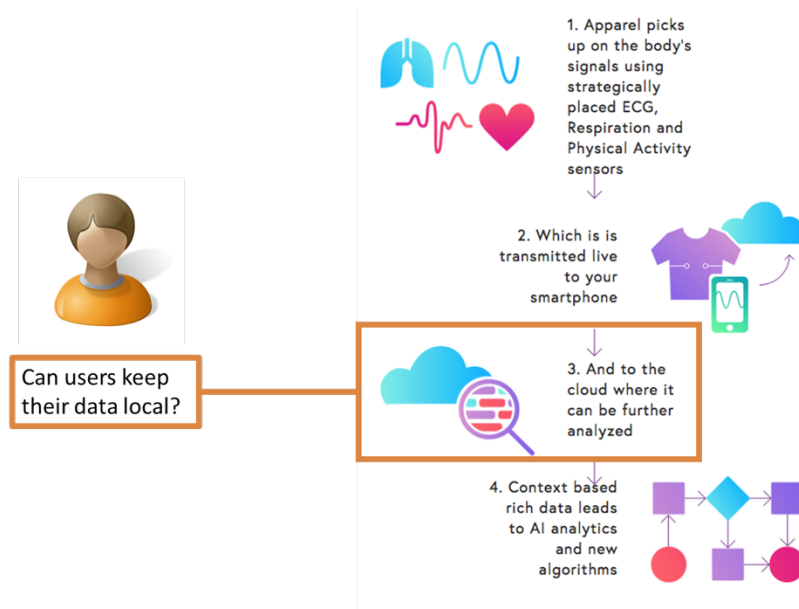


According to Viatom, there is proper data encryption, but “proper” is not defined specifically. Additionally, there is no further information about what a “self-governed cloud” entails.


OMSignal Smartwear



OMSignal [14] specializes in smartwear and analytics for healthcare. Their products incorporate sensors into apparel to capture data such as heart rate, steps, and breathing. The clothes capture contextualized, continuous, medical-grade biometric data. OMSignal uploads user data to the cloud for analysis and storage and users cannot keep data locally because the analytics are calculated remotely. OMSignal does not state any option to store the data locally. In fact, users may delete personal information from OMSignal databases but it would also remove the user’s ability to use OMSignal services [15].



The chart below summarizes the five wearables discussed so far with a brief description of their features and data handling procedures.

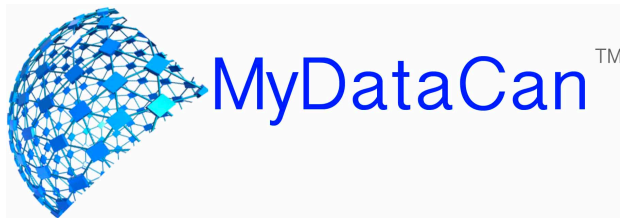
Apple Watch Smartwatch	Whoop Fitness Tracker	Viatom CheckMe Pro Medical Tricorder	OMSignal Smartwear
			
Built in GPS, Pedometer Accelerometer Heart Rate Gyroscope Ambient Light Sensor Barometric Altimeter	Accelerometer Heart Rate + Variability Sleep auto-detection Ambient Temperature	Pedometer Heart Rate + Analysis Sleep monitor, Detects Sleep Apnea Thermometer BP Tracking, Pulse Oximeter ECG signal + waveform	Pedometer, Gait Analysis Accelerometer Heart Rate + Variability Detects Sleep Apnea ECG signal + signature Respiration signal, rate, COPD Detect
Data only kept locally, potential developer access via API	Data shared over cloud, user access via app	Data shared over cloud w/ authorization, access via app + remote monitor	Data shared over cloud, user access via app

Goal: User Control of Data



While all the wearables detailed earlier allow the user to access personal health data, only the Apple Watch stores data locally. The others store information in company servers. OMSignal, Whoop and Viatom collect data automatically. How can we restore patient privacy – their ability to own and control data collection and sharing?

MyDataCan



MyDataCan [16] is a service that allows users to store their data in a double-encrypted server that only the user can access and control. The user can also share and distribute data to individuals or organizations.. Even if users cannot control how companies share their data, MyDataCan provides a way for users to curate the truest and most valuable version of the data that they can correct. This centralized storage system can draw on multiple types of health data that the user inputs and give the user a more holistic view.

With the user's permission, third-party applications to calculate analytics on the user's data. However, third-party apps are only allowed to run on the MyDataCan platform, giving users control over when and what they share, how much they share, and can retract their data from a study or app. Developers only see the users' personal health data if allowed by the user or they may do analysis on users' data but only extract their analysis results. MyDataCan draws on the limitations of current privacy regimes to provide flexible and unlimited control to the user.

References

1. Business Insider Intelligence estimates. <https://www.businessinsider.com/wearables-in-healthcare-b-2018-8>
2. Technology that is Flexible, Sticky, and Smart = Wearable Patches. Wearable Technologies Conference. <https://www.wearable-technologies.com/2015/08/technology-that-is-flexible-sticky-and-smart-wearable-patches/>
3. A Look at Smart Clothing for 2015. <https://www.wearable-technologies.com/2015/03/a-look-at-smartclothing-for-2015/>
4. Wearables that monitor your posture. Gadgets and Wearables. <https://gadgetsandwearables.com/2018/10/08/posture-corrector/>
5. APDM Wearable Technologies. <https://www.apdm.com/wearable-sensors/>
6. Smart shoes: Tracking fitness through your feet. Gadgets and Wearables. <https://gadgetsandwearables.com/2018/07/13/trackers-feet>
7. Pew Research Center Report. <http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>
8. Apple Developer Forums. <https://forums.developer.apple.com/message/27192#27192>
9. HealthKit. <https://developer.apple.com/documentation/healthkit>
10. ResearchKit. <http://researchkit.org/>
11. Whoop. <https://www.whoop.com/>
12. Whoop Privacy Policy. <https://www.whoop.com/privacy/>
13. Viatom CheckMe Pro. <https://www.viatomtech.com/checkme-pro/>
14. OMSignal. <https://www.omsignal.com/>
15. OMSignal Privacy Policy. <https://omsignal.com/privacy-policy/>
16. MyDataCan. <https://mydatacan.org/about.html>