Who is benefiting from your fitness data? A privacy analysis of smartwatches

Jessica Monteith, Oliver Shapcott, Anna Talas, and Pranav Dahiya

Department of Computer Science and Technology, University of Cambridge
{psjm3, ots28, at2008 & pd538}@cl.cam.ac.uk

Abstract. Over the last decade, the use of smartwatches has become prevalent, and the market is estimated to grow, reaching a value of $80.1 billion by 2028 [1]. The increase in the market share was primarily due to the attractive personal features related to fitness, which could fulfil the three basic psychological needs: autonomy, competence and relatedness [2]. As a result, user uptake increased rapidly. Fitness data is also very personal. Whilst many users share their fitness data, they don't want their data being used or shared without their consent. Data protection is required by law, but if users need to learn how their data is used and whether or not the operations follow the privacy policies, how do they know that their data is protected? Our research analyses the agreements between each party involved around the end users of smartwatches and looks at how the smartwatch vendors and application developers handle data. As our case studies, we provide an analysis of how privacy could be violated using four of the biggest market share holders, namely Apple, Fitbit, Samsung and Garmin.

Keywords: Smartwatches · Privacy · Fitness Tracking · Health Tracking

1 Introduction

The initial idea of smartwatches was seen in the early 1970s [3]. However, the concept of smartwatches being used as part of modern life was not seen until 2012 when the brand Pebble raised $10 million in a kick-starting campaign [4]. Since then, major technology brands have competed to gain market share with their most advanced designs for smartwatches.

Today smartwatches come equipped with many sensors, such as heart rate monitors, thermometers, GPS sensors and altimeters. However, smartwatches are used primarily for smartphone notifications and fitness tracking [5]. Whilst these offer many benefits to the users, the same data could be exploited to fulfil the interests of businesses or service providers without users' explicit consent.

Our research focuses on privacy concerns through the usage of smartwatches. Personalised data is extremely valuable nowadays to all kinds of business, e.g. target advertising, insurance, platform products such as Google Health, and prone to a data breach or deliberate attacks [6, 7, 8]. Privacy policies are designed to provide information regarding how privacy data is protected. However, not all users read them, and even if they do, not all of them understand what they

mean. To study how privacy is handled by different companies and the potential impact on end users, we looked at the three main groups in play: smartwatch vendors, end users and the smartwatch application (app) developers. Fig 1 shows the different agreements and bindings between these groups.

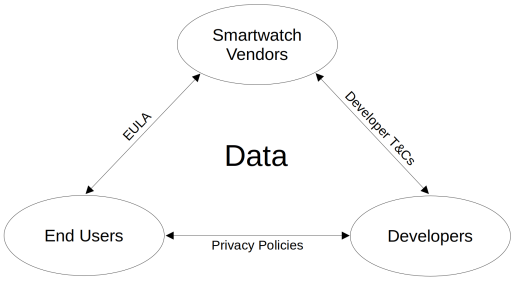

Fig. 1. Bindings of privacy between smartwatches vendors, application developers and end users

Through our case studies on Apple, Fitbit, Samsung and Garmin and their relevant smartwatch products, we looked at how each company treat privacy and how end users perceive their data usage by the companies. This paper aims to answer the question: *Whilst an end user agrees to apps on their smartwatch to collect their personal data, how much do they know about what happens to that data?*

2 Related Work

Cyr et al. [9] carried out an analysis of Fitbit devices in 2014. This paper provided insight into a complete hardware analysis of a wearable product, the sort of information a smartwatch produces, and where the data is stored. McMullen and Fairfield [10] conducted a quantified self-report card in 2019 to evaluate how vendors treat users' sensitive data produced by wearable devices. The four areas the report focuses on are legal rights, data collection and sharing, data access and security. The target of those works is to provide information to consumers to inform their device purchases and to promote vendors that practice good privacy features. Our analysis takes inspiration from the report card and aims to understand the relationship between vendors, users and app developers.

3 Case Studies

Apple
Apple has by far the largest market share in smartwatches, with 30.1% [11] of the UK market and 40% [12] worldwide. Linked mainly to the iPhone's market share and its interoperability. Their first watch was released in 2015, and Apple Watch quickly became a fashion icon. They announced publicly that protecting privacy data is one of their top priorities [13].

Fitbit
Fitbit's market share has declined over the years, but it still holds the second most significant market share in the UK with 31% [12] in 2021. Worldwide they

hold 3.8%, just below Garmin on the market [11]. Fitbit was acquired by Google in 2021 after Google addressed the competition concerns raised by the European Commission by committing not to use the health and wellness data for Google Ads. They would maintain a technical separation of Fitbit's user data from any other Google data used for advertising. They have also agreed to maintain user data access through Fitbit Web API without charging. The duration is ten years [14]. However, 'data silos' do not prevent Google from combining health data with other data Google already owns. Users also need clarification regarding how their health data is used.

Samsung
Shortly after the modern-day inception of smartwatches in 2012, Samsung started their wearable communications device called Samsung Gear in September 2013, re-branded to Samsung Galaxy later in February 2019. Samsung Galaxy is both their watch and earbud brand. In the UK, Samsung smartwatches take up 15% of the market share [11] in 2022, and 10.2% [12] of the market share in 2021. These positive sales figures could be linked to Samsung's Galaxy Watch 4, released in August 2021.

Garmin
Traditionally specialising in GPS technology, Garmin diversified in 2003, adding wearable devices for sports to their product line. Having started with devices aimed at outdoor and sports activities, they have since created full-fledged smartwatches. They are a crucial competitor in the market, holding 4.6% of the smartwatch market share worldwide in 2021 [11] and 9% of the UK market share in 2022 [12].

4 The agreements between smartwatch vendors and end users

4.1 End User License Agreements

End User License Agreements (EULAs) are legally binding contracts that specify users' rights and restrictions to use licensed software. EULAs outline users' rights and permissions with the software, and unlike physical products, they are living contracts and typically persist with the associated software updates. Vendors use EULAs to protect their owner's rights, and users are declined their privilege to use the software if they do not accept the licensing agreements.

EULAs fall under the terms shrink-wrap and click-wrap licenses. Shrink-wrap licenses are generally viewable after purchase as they are supplied in the product box. Click-wrap licenses are licenses one must agree to on the product. The legality of these licenses has been disputed, and different legal standings exist in different jurisdictions [15, 16].

Research has shown that users often accept terms of service and conditions without a sound knowledge of what they are accepting [17]. In part, the lack of user comprehension of terms of service and other legal agreements such as EULAs concerns the technical jargon [17]. Attempts have been made to use more plain language [18]. Research by Waddell et al. [17] showed that paraphrasing

traditional EULAs across several windows led to a better attitude towards EULAs, as well as an increased exposure time.

We analysed the EULAs or equivalent documents with which users of our case study smartwatches are presented. We considered the following as necessary EULA features: user granting privileges, notices of copyright infringement, a usage restriction notice, warranty disclaimer, liability limitation notices, license terminations, and signposting to any relevant agreements, if applicable. These provide vendor protections, so we also consider user protections by analysing whether the following are present: *'criticism clauses'*, monitoring clauses, reverse engineering clauses, and update and change over time clauses [19].

	Apple[20]	**Fitbit**[21]	**Samsung**[22]	**Garmin**[23]
Software Provider Protections				
User granting privileges	✓	✓	✓	✓
Copyright infringement notice	✓	✓	✓	✓
Usage restriction notice	✓	✓	✓	✓
Warranty disclaimer	✓	✓	✓	✓
Liability limitation	✓	✓	✓	✓
License terminations	✓	✓	✓	✗
Relevant agreements linked	✓	✓	✓	✗
Product usage = agreement	✓	✓	✓	✓
User Infringing Clauses				
Criticism clauses	✗	?	✗	✗
Monitoring clauses			?	✗
Reverse engineering restrictions	✓	✓	✓	✓
Update and persistency	✓	?	✓	✗

✓= Present
✗ = Not Present
? = Exception
= Not evident or N/A

Table 1. End User License Agreement rating metrics

Apple

Apple has the most explicit EULA equivalent policies of the vendors examined. However, this has only sometimes been the case with their software licensing. For example, in 2015, a journalist at The Guardian wrote an article about Apple keeping Google Maps in its EULAs even after they dropped Google Maps from their services [24]. They have improved since then, as we found Apple's WatchOS 9.3 EULA was clear and comprehensive.

Fitbit

Fitbits' Terms of Service, section seven, state that one may not "disclose" or "publicly display" or "publicly perform" any "Fitbit Content" [21]. Fitbit has the strictest usage policies. Google is trying to consolidate the management of user profiles and the overall platform. As a consequence, section three *Use of an account* of the Terms of Service states that users will be "required" to have a Google account from a date which they will specify. If users do not have

an account by this date, they reserve the right to terminate the terms of this document [21]. Fitbit's Terms of Service also discuss how any arbitration must be done individually and not as part of a class action[1].

Samsung
Samsung compares equally well to Apple in most fields. We have given it an exception in the *Monitoring clauses* section of Table 1, because it is more apparent than in Apple's case. Unlike Apple, Samsung signposts the privacy policies within the EULA very clearly. Samsung also clearly stated the collection points they use to provide future software updates, as seen in the *Consent to use of data* section. It is worth noting that Samsung, like Fitbit, explicitly stated that arbitration must be done individually and not as part of a class action.

Garmin
Garmin's EULA equivalent [23] is placed within each watch's user manual as a paper document and on their website as a PDF. It is the shortest of all the license agreements, likely because many of the 'standard' EULA features are abstracted elsewhere or to other documents. However, this also means that Garmin's Software Licensing Agreement only covers a few of the conditions we expect. For example, the agreement does not link or reference Garmin's other software usage policies. It also does not define license termination conditions or mention if the software license agreement persists between updates.

4.2 Security Measures and Policies

This section explores the smartwatch vendors' security policies and the functionality surrounding automatic updates. The National Cyber Security Centre (NCSC) encourages users to keep devices up to date and, where possible, use the automatic update functionality [25]. We work on the basis that automatic updates are a force for good. All vendors except Garmin offer bug bounty or responsible disclosure programs. We evaluate that responsible disclosure programs are a vital measure as they encourage vulnerabilities to be reported by individuals.

Data	Apple	Fitbit	Samsung	Garmin
Victim of ransomware attack(s)	Yes	Yes	No	Yes
Victim of data leak/breach	Yes	Yes	No	No
Public disclosure/Bug bounty scheme	Yes	Yes	Yes	No
Automatic update functionality	Yes	Yes	Yes	Yes
Publicly available security documentation	Yes	No	Yes	No
Maintains record of patches	Yes	No	Yes	No

Table 2. Security metrics, specific to watch divisions of the vendors

Apple
Apple has long tried to maintain the public perception that they are the 'Gold Standard' regarding privacy and security. One of their support pages states, "At

[1] Class Action - "a legal action that is organized by a group of people who all have the same legal problem" - Cambridge Dictionary.

Apple, we believe privacy is a fundamental right" [26]. However, journalists and academics have suggested otherwise [27, 28]. In 2021, users' health and well-being data from Apple and Fitbit was exposed in a non-password-protected data breach [29]. Apple's WatchOS applies "hardware-based platform security capabilities" to their other operating systems. They include functionalities such as secure booting and software updates. Apple also allows users to set up automatic updates.

Fitbit
Fitbit has in the past experienced security issues. In 2011 users' Fitbit sexual activity data could be seen from Google's search engine [30]. However, unlike other vendors, Fitbit does not publish a security policy, and they do not produce security update logs. So, tracking what measures are in place and what security functionality has been fixed is tricky.

Samsung
The latest Samsung smartwatches use WearOS, a smartwatch operating system created by Google. They are popular particularly among non-Apple device users as they integrate well with Android devices. Google lists WearOS security updates and patches in their system updates [31]. However, WearOS has experienced issues in the past. For example, in 2020, Barsallo Yi et al. demonstrated "a fuzz testing tool" called Vulcan [32] and found that across the 100 popular apps they tested, 18 test scenarios could cause system reboots across 13 different apps. Overall, WearOS models the Android approach. It sandboxes apps and abstracts the apps' sensor access. Like Android apps, the WearOS apps must still ask for the same individual permissions [33].

Garmin
Garmin suffered from a major ransomware attack in 2020 [34]. The attack affected Garmin Connect, the app that tracks health and fitness data and syncs with the smartwatch running Garmin Watch OS. It was widely reported that Garmin paid the ransom and that they were provided with a decryption key. It is unclear whether the data was leaked, however, it has been assumed that it was not [34].

5 Agreements between smartwatch vendors and application developers

5.1 Terms and Conditions

Developer Terms and Conditions are agreements between the vendors and developers. They outline the permitted uses and restrictions when building applications for the respective vendor platforms. These guidelines aim to help developers follow best practices when writing applications for the platform, as well as making sure that all legal requirements that have been put in place are followed. In the following section, we focus mainly on the parts of the terms and conditions that deal with collecting and sharing data from users.

Apple
Apple's Developer Program License specifically bans the sale and sharing of health information collected through its HealthKit API and Motion & Fitness

API. However, it does allow developers to use this data when consent has been agreed and information on how the data is used are given. On top of that, developers are allowed to share data with third-party health or fitness services if the user has granted permission to do so [35]. Apple's Developer Program License Agreement is pretty comprehensive at 88 pages long. Apple's App Store Review Guidelines [36] also state that *"All apps must include a link to their privacy policy in the App Store Connect metadata field and within the app in an easily accessible manner."* However previous research has shown that only 18% of iOS apps displayed privacy policies [37].

	Apple[35]	**Fitbit**[38]	**Samsung**[39]	**Garmin**[40]
Requirements				
Privacy policy	✓	✓	✓	✓
Data encryption	✓	✓	✓	✗
Ask to collect data	✓	✓	✓	✓
Permissions				
Collecting user data	✓	✓	✓	✓
Sharing data with third parties (for legal reasons)	✓	✓	✓	✗
Sharing data with third parties (other)	?	?	✓	✗
Sharing data for advertising	✗	✗	?	✗
Sale of user data	✗	✗	✗	✗

✓= Present
✗ = Not Present
? = Exception (usually if explicit consent is given by user)
= Not evident or N/A

Table 3. Developers permissions and restrictions for different smartwatch vendors

Fitbit

Developers for the Fitbit app must agree to Fitbit's Terms of Service [38] for using their platform. The terms of service state that any application developed must have a user agreement that clearly informs the users of the terms and conditions and the privacy policy describing any information collected. This is particularly significant because it has mentioned that apps must display the user agreement and privacy policy **before** users give permissions, and on the agreement and policy, they shall, at a minimum, disclose the app's practices regarding user data. Many apps available on Fitbit Gallery do not have privacy policies that show that the app complies with Fitbits guidelines, and frequently these fail to show how the data is collected, used, stored and shared.

Samsung

Samsung Galaxy App development has recently moved to WearOS, an Android-based smartwatches operating system. This move means the Developer Terms and Conditions will be from Android Studio. The Android Developer Program Policy [39] says that selling or transferring Health Connect data, data for serving

ads, credit-worthiness data, medical device pursuant data or Protected Health Information data shall be prohibited. However, Google Play's Data safety section [41] also states that transferring anonymised user data does not need to be disclosed as "sharing".

Garmin
Garmin's terms and conditions leave the developers responsible for ensuring the users' privacy. They explicitly state that "You are solely responsible for the security of user data residing on server(s) or systems owned or operated by you, or by a third party designated by you (e.g., a web hosting company, processor, or other service provider)." [42, 40]. They require that developers adhere to Garmin's privacy policies and any other local laws where the app can be distributed. Developers can only retain data for the duration required for the 'reasonable operation' of the application. Users must explicitly grant permissions before any data is collected, and location data collection cannot be enabled by default. Also, developers cannot sell, rent or transfer the collected data to third parties. They must delete relevant user data if any previously granted permissions are revoked from the app. This makes the process easier for users than submitting an official request for deletion.

5.2 App Store Review Policies

In order to make an app available on the app store belonging to the respective vendor, developers have to submit their apps for review. This should guarantee that the apps found on the store comply with the terms and conditions set by the developers for the app. However, in reality, the review policies do not always stop apps which violate them from becoming available on the app store. Moreover, it is often difficult to find a vendor's privacy and data policies for developers, as there are no apparent links to them on their sites, and they might also not align with the review guidelines given.

Garmin explicitly states in their app review policy that "Garmin may, but is not obligated to, review your Application before it is uploaded to the Garmin Website", leaving all the responsibility on the developer without much oversight over their activities. However, Garmin reserves the right to remove or refuse to upload an application at any time regardless of whether it meets the application requirements set [43]. Likewise, Apple has a relatively strict app review policy outlined on its website. However, they also state that "90% of submissions are reviewed in less than 24 hours" [36]. Due to this, it seems likely that a lot of the process is automated.

We found numerous examples of apps on application stores that allowed the execution of open source scripts, such as home IoT applications, which may lead to potential security vulnerabilities. For instance, the apps we looked at on Fitbit's app gallery do not have privacy policies listed or linked on their pages, which is typically where users would look when they want to find information about the apps to be installed on their smartwatches.

Overall, it seems that the app review policies mostly centre around prohibiting harmful content such as obscene content, abuse and bullying, and having

strict rules about spam and malware. However, there is generally very minimal talk about user data privacy, and the guidelines often point to longer legal documents, which developers are unlikely to read as thoroughly.

6 Agreements between application developers and end users

Smartwatch vendors are not the only entities that have access to user data. One of the reasons these devices are so popular is the existence of app stores that offer an ecosystem of utilities and programs. Drawing a parallel to the effect stores have had on the smartphone market, the widespread adoption of these devices started in 2008, accompanied by the launch of Apple's App Store and Google Play. However, these stores need to be regulated effectively to ensure that users get the same quality of apps and security from third parties on the app store as they would with first-party apps. This section will cover the guidelines set by smartwatch manufacturers on the privacy policies that developers must follow to get their apps published on the app stores of the four vendors considered in this paper.

6.1 Privacy Policies

A privacy policy is a legally binding document that aims to provide information to users about what data is collected, and how it will be used. Companies must write their privacy policies to be GDPR compliant, which outlines guiding principles for how this information should be presented. With regards to apps published on vendors' stores, an important point to consider is usability, or how easy it is for developers to get access to the guidelines put in place regarding user privacy on published apps. Developers access to privacy requirements from each of the four vendors was examined from a usability perspective.

Apple
Apple has an article titled "Planning your watchOS app" on their developer website. While this page is not linked to from the WatchOS documentation, a quick Google search can land a developer on this page. In the section titled "Adopt best practices during development", there is a link to the privacy requirements present in the documentation for UIKit, one of Apple's front-end frameworks. It is important to note that this is not the front-end framework that is recommended for developers in the WatchOS documentation, which is SwiftUI [44, 45].

Fitbit
Fitbit's guidelines for publishing an app on their store do not mention privacy policies at all. In fact, their privacy policy guidelines are not present on their developer website. However, a Google search led to an article titled "Fitbit Platform Developer and User Data Policy", which mentions that a privacy policy is required before an app can be published. This document also outlines what information should be included in privacy policies [46, 47].

Samsung
Samsung is in a slightly different position compared to Apple, since they rely on

Google to provide the operating system that run on their smartwatches. This means that end users have access to both Google's play store and Samsung's Galaxy store to install third-party apps. The guidelines for publishing an app on the galaxy store are easy to find on Samsung's developer website, with one of the first links on the page pointing to an article titled "App Distribution Guide". This guide contains a section on privacy and relevant policies for developers [48].

Garmin
Garmin's developer website links to Connect IQ documentation, which contains a section called "App Review Policies". This in turn links to the developer agreement which highlights relevant information regarding privacy policies [40, 42]. Garmin is the only vendor which does not place emphasis on developers being as transparent as possible about the type of data being collected and how it will be used.

6.2 Data Collection, Usage and Storage Policies

Each smartwatch product has different functions and interfaces that allow data to be collected. Users might not know the amount of data not related to fitness or health being collected by the smartwatch vendors. For example, Fitbit listed the following in their privacy policy:

"We also collect data about the devices and computers you use to access the Services, including IP addresses, browser type, language, operating system, Fitbit or mobile device information (including device and application identifiers), the referring web page, pages visited, location (depending on the permissions you have granted us), and cookie information... if you connect to Facebook or Google, we may receive information like your name, profile picture, age range, language, email address, and friend list."

And Garmin stated this in their privacy policy:

"We collect data from users about their usage of our products, services, websites, and apps. The types of analytical information that are collected include the date and time of access to our servers, software or firmware version, the location of the device, language setting, what information and files have been downloaded, user behavior (e.g., features used, frequency of use), device state information, device model, hardware and operating system information, and information relating to how the product, service, website, or app functions."

On the surface, this kind of data is mainly for the vendors' purposes, such as analytics, but the data reveals a lot about users' privacy that's not related to health metrics.

The data collected from smartwatches is undoubtedly interesting for the end users, but the power is magnified when compared to everyone else's data. Indeed there have been reports showing evidence that companies have used the data to track their employees' health [49, 50]. For example, Human Data Commons Foundation (HDC) published a report on "quantified self" devices [10], these are devices that obtain and measure metrics about the user on an ongoing basis. They raised concerns regarding how the privacy and consumer rights of individuals could be violated and used a weighted scoring system to compare the

selected companies across multiple categories: Legal Rights; Data Collection and Sharing; Data Access; Security. Their study has found that some companies collect data for purposes that have little to do with the needs or expectations of users, such as product development and marketing. In addition, some companies collect data from third parties to generate profiles about users. They have also found that some companies share the data they have collected with advertisers, insurance companies, employers and data brokers. However, not all of them make their data-sharing practices clear to the users.

Users could quickly lose track of where their personal data goes if the data is being shared with other apps and services unrelated to fitness. Take Google Fit as an example, the data collected on the smartwatch could be synchronised into the Google Fit platform. When that happens, your fitness data is linked to your Google account. That data is available on different servers, managed by different sets of services, and under different privacy policies.

All four smartwatch vendors considered in this paper have data minimisation policies (i.e. ensuring that developers only have access to the minimum amount of data required for maintaining application functionality) and promoting transparency to users about how their data is used. In addition, a robust permissions system is built into the developer tools provided by these companies, ensuring that developers explicitly ask users to grant access whenever sensitive information needs to be accessed. Fitbit notably mentions explicitly in their policies that humans should never access user data except when it is required for security purposes, such as to investigate abuse or to comply with law enforcement [46].

Recent studies have shown that motion sensors data such as that from accelerometers and gyroscopes can be used to track users and build unique profiles that can be used for re-identification by advertisers [51]. This makes smartwatches even more sensitive to infringement of user privacy than smartphones, considering the multitude of health-tracking sensors and features built into these devices. Apple, Samsung and Garmin all have specific permission that needs to be granted by the end user to each app before any sensor data can be accessed. Apple goes one step further and has assigned individual permissions to separate sensors, ensuring that users have granular control when developers ask for access to sensor data. Fitbit, however, only puts the heart rate sensor behind such a permission system, leaving all other sensors accessible to developers without user consent.

7 Discussion and Concluding Thoughts

There is little doubt that there is much interest in personal fitness tracking, at the same time, we live in a digital world where data is valuable. When valuable personal data is combined with other types of data to provide valuable information, it makes getting hold of this data an attractive business proposition. Unfortunately, the ecosystem for personal data is no longer a simple one-to-one relationship between a service provider and the consumer, making it very hard to answer the question - who owns our data? Transparency should be included as

one of the basic steps towards answering this question, as well as all the concerns raised around it.

When analysing the EULA options given to users, in many cases from the various smartwatch manufacturers, we were surprised that they had not incorporated some of the advice in previous works [17] to both paraphrase or split the EULA over many screens to increase the number of users understanding the agreements they were accepting. Doing so would help encourage users to understand better their rights concerning the software from the vendors, the software acquired from third parties and the use of data collected.

There is a need for change regarding users' understanding of terms and conditions. In 2014 an experiment by Europol demonstrated how users would agree to the terms and conditions, which also had a clause about giving up their eldest child, to connect to a public Wi-Fi [52]. The lack of privacy in fitness apps has also been a concern. In 2018 it was discovered that Strava heatmaps revealed the location of U.S. military bases [53].

In this analysis, we looked into the ecosystem in what smartwatches could do to our data, from legally binding documents to app review policies to user privacy protections. We have looked at other research into this area. There is still a considerable gap between what the vendors claim they are doing to protect their users' privacy and what is happening with the private data. We hope to see future research to refine some of the areas we touched, such as the smartwatch application development life cycle. Do the app review policies prevent rogue applications from making it onto the market? We would also like to see more profound research into the legal implications regarding the discrepancies between the app development terms and conditions and what has been released to the market.

As we continue to get the benefits of using devices to get useful data, hence knowledge, about ourselves, together with how valuable and powerful the data can be to insurance companies, employers and technology companies, these devices will become indispensable. From time to time, we should reflect on the data ecosystem and consider what good it does and what harm it can cause. We need to understand who and what is accountable so that the end users do not end up being kept in the dark or having to compromise the opportunity to use technology to enhance their quality of life to avoid their privacy being exposed.

Disclaimer

This paper represents the views of the authors and not of the University of Cambridge, or of any other organisation.

References

1. Vantage Market Research: Global Smartwatch Market Size & share to surpass USD 80.1 bn by 2028, GlobeNewswire News Room. Oct. 2022. https://www.globenewswire.com/en/news-release/2022/10/18/2536067/0/en/Global-Smartwatch-Market-Size-Share-to-Surpass-USD-80-1-Bn-by-2028-Vantage-Market-Research.html (visited on 02/10/2023)

2. Edward L Deci and Richard M Ryan: The "what" and "why" of goal pursuits: Human needs and the self-determination of behavior. Psychological inquiry 11(4), 227–268 (2000). DOI: 10.1207/S15327965PLI1104_01
3. Erik Gregersen: Smartwatch, Encyclopedia Britannica. July 2022. https://www.britannica.com/technology/smartwatch (visited on 02/17/2023)
4. Brief history of the Smartwatch, Rotate Watch Kits. Dec. 4, 2020. https://rotatewatches.com/2020/12/04/brief-history-of-the-smart-watch/ (visited on 02/12/2023)
5. Felix Richter: What Smartwatches Are Actually Used For, Statista. Aug. 2017. https://www.statista.com/chart/10783/use-cases-for-smartwatches/ (visited on 02/08/2023)
6. Jill McKeon: 61M Fitbit, Apple Users Had Data Exposed in Wearable Device Data Breach, Health IT Security. Sept. 2021. https://healthitsecurity.com/news/61m-fitbit-apple-users-had-data-exposed-in-wearable-device-data-breach (visited on 02/14/2023)
7. Xiangyu Liu, Zhe Zhou, Wenrui Diao, Zhou Li, and Kehuan Zhang: When Good Becomes Evil: Keystroke Inference with Smartwatch. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. CCS '15, pp. 1273–1285. Association for Computing Machinery, Denver, Colorado, USA (2015). DOI: 10.1145/2810103.2813668
8. Cheryl Winokur Munk: The biggest security risks of using fitness trackers and apps to monitor your health, CNBC. Nov. 26, 2022. https://www.cnbc.com/2022/11/26/the-biggest-risks-of-using-fitness-trackers-to-monitor-health.html (visited on 02/14/2023)
9. Britt Cyr, Webb Horn, Daniela Miao, and Michael A. Specter: Security Analysis of Wearable Fitness Devices (Fitbit). In: (2014)
10. Greg McMullen and Rochelle Fairfield: 2019 Quantified Self Report Card, Human Data Commons Foundation. 2019. https://humandatacommons.org/wp-content/uploads/2019/11/HDC-Quantified-Self-Report-Card-2019.pdf (visited on 02/19/2023)
11. Statista Consumer Insights: Smartwatch market share worldwide in 2020 and 2021, by vendor, Statista. https://www.statista.com/statistics/1296818/smartwatch-market-share/ (visited on 01/01/2023)
12. Statista Consumer Insights: eHealth tracker / smart watch usage by brand in the UK in 2022, Statista. https://www.statista.com/forecasts/997782/ehealth-tracker-smart-watch-usage-by-brand-in-the-uk (visited on 01/01/2023)
13. Privacy, Apple Inc. 2019. https://www.apple.com/privacy/ (visited on 02/18/2023)
14. European Commission: Mergers: Commission clears acquisition of Fitbit by Google, subject to conditions, Dec. 2020. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2484 (visited on 12/23/2022)
15. Brandon L. Grusa: Contracting Beyond Copyright: PRoCD, Inc. v. Zeioenberg. Harvard Journal of Law & Technology 10(2), 353–367 (1997)
16. Feist Publications, Inc. v. Rural Telephone Service Company, Inc. Case No. 89-1909. United States Supreme Court. 1991. https://www.law.cornell.edu/supremecourt/text/499/340 (visited on 02/18/2023)
17. T. Franklin Waddell, Joshua R. Auriemma, and S. Shyam Sundar: Make It Simple, or Force Users to Read? Paraphrased Design Improves Comprehension of End User License Agreements. In: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems. CHI '16, pp. 5252–5256. Association for Computing Machinery, San Jose, California, USA (2016). DOI: 10.1145/2858036.2858149

18. Michael E J Masson and Mary Anne Waldron: Comprehension of legal contracts by non-experts: Effectiveness of plain language redrafting. Applied Cognitive Psychology 8, 67–85 (1994)
19. Annalee Newitz: Dangerous Terms: A User's Guide to EULAs, Electronic Frontier Foundation. Feb. 2005. https://www.eff.org/wp/dangerous-terms-users-guide-eulas (visited on 02/09/2023)
20. Apple watchOS Software License Agreement, Apple Inc. July 2021. https://www.apple.com/legal/sla/docs/watchOS8.pdf (visited on 02/15/2023)
21. Terms of Service, Fitbit. Sept. 2022. https://www.fitbit.com/global/us/legal/terms-of-service (visited on 02/17/2023)
22. Gear End User License Agreement for Samsung Software (EULA), Samsung Electronics. July 2017. https://www.samsung.com/us/Legal/SamsungLegal-EULA-GEAR/ (visited on 02/13/2023)
23. Important Safety and Product Information Important Safety and Product Information, Garmin Ltd. Jan. 2023. https://static.garmin.com/pumac/ISPI_Fitness_PulseOx.pdf (visited on 02/19/2023)
24. Alex Hern: I read all the small print on the internet and it made me want to die, The Guardian. June 2015. https://www.theguardian.com/technology/2015/jun/15/i-read-all-the-small-print-on-the-internet (visited on 02/16/2023)
25. Device Security Guidance, National Cyber Security Centre. June 2021. https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/keeping-devices-and-software-up-to-date (visited on 02/14/2023)
26. About privacy and security for Apple products centred on education, Apple Inc. Jan. 2023. https://support.apple.com/en-gb/HT208525 (visited on 02/14/2023)
27. Johana Bhuiyan: Apple says it prioritizes privacy. Experts say gaps remain, The Guardian. Sept. 23, 2022. https://www.theguardian.com/technology/2022/sep/23/apple-user-data-law-enforcement-falling-short (visited on 02/19/2023)
28. Thomas Germain: Apple Says Your iPhone's Usage Data is Anonymous, but New Tests Say That's Not True, Gizmodo. Nov. 21, 2022. https://gizmodo.com/apple-iphone-privacy-dsid-analytics-personal-data-test-1849807619 (visited on 02/19/2023)
29. Heather Landi: Fitbit, Apple user data exposed in breach impacting 61M fitness tracker records, Fierce Healthcare. Sept. 2021. https://www.fiercehealthcare.com/digital-health/fitbit-apple-user-data-exposed-breach-impacting-61m-fitness-tracker-records (visited on 02/17/2023)
30. Leena Rao: Sexual Activity Tracked By Fitbit Shows Up In Google Search Results, Tech Crunch. July 2011. https://techcrunch.com/2011/07/03/sexual-activity-tracked-by-fitbit-shows-up-in-google-search-results/ (visited on 02/14/2023)
31. What's new in Google System Updates, Google LLC. 2023. https://support.google.com/product-documentation/answer/11412553?hl=en#zippy=%5C%2Cjanuary%5C%2Cdecember (visited on 02/18/2023)
32. Edgardo Barsallo Yi, Heng Zhang, Amiya K. Maji, and Saurabh Bagchi: Vulcan: A State-Aware Fuzzing Tool for Wear OS Ecosystem. In: Proceedings of the 18th International Conference on Mobile Systems, Applications, and Services. MobiSys '20, pp. 480–481. Association for Computing Machinery, Toronto, Ontario, Canada (2020). DOI: 10.1145/3386901.3397492
33. Marcos Tileria, Jorge Blasco, and Guillermo Suarez-Tangil: WearFlow: Expanding Information Flow Analysis To Companion Apps in Wear OS. In: 23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2020). USENIX (2020)

34. 6 Things to Learn from the Garmin Security Breach, Fortra's Terranova Security. Feb. 2022. https://terranovasecurity.com/garmin-security-breach/ (visited on 02/17/2023)
35. Apple Developer Program License Agreement, Apple Inc. June 2022. https://developer.apple.com/support/downloads/terms/apple-developer-program/Apple-Developer-Program-License-Agreement-20220606-English.pdf (visited on 01/01/2023)
36. App Store Review Guidelines, Apple Inc. Oct. 2022. https://developer.apple.com/app-store/review/guidelines/#legal (visited on 01/01/2023)
37. Julie M. Robillard, Tanya L. Feng, Arlo B. Sporn, Jen-Ai Lai, Cody Lo, Monica Ta, and Roland Nadler: Availability, readability, and content of privacy policies and terms of agreements of mental health apps. Internet Interventions 17, 100243 (2019). DOI: 10.1016/j.invent.2019.100243
38. Fitbit Platform Terms of Service, Fitbit. Aug. 2022. https://dev.fitbit.com/legal/platform-terms-of-service/ (visited on 12/26/2022)
39. Android Developer Program Policy, Google LLC. Dec. 2022. https://support.google.com/googleplay/android-developer/answer/12867690 (visited on 01/01/2023)
40. Garmin Connect SDK Agreement, Garmin Ltd. July 2019. https://developer.garmin.com/downloads/connect-iq/sdks/agreement.html (visited on 01/01/2023)
41. Provide information for Google Play's Data safety section, Google LLC. https://support.google.com/googleplay/android-developer/answer/10787469 (visited on 02/12/2023)
42. Garmin Connect IQ App Review Guidelines, Garmin Ltd. Oct. 2021. https://developer.garmin.com/connect-iq/app-review-guidelines/ (visited on 01/01/2023)
43. Garmin, Garmin Ltd. July 2019. https://developer.garmin.com/downloads/connect-iq/sdks/agreement.html (visited on 02/12/2023)
44. Planning your WatchOS App, Apple Inc. https://developer.apple.com/watchos/planning/ (visited on 02/19/2023)
45. watchOS apps, Apple Inc. https://developer.apple.com/documentation/watchos-apps/ (visited on 02/19/2023)
46. Fitbit Platform Developer and User Data Policy, Fitbit. Aug. 29, 2022. https://dev.fitbit.com/legal/platform-developer-and-user-data-policy/ (visited on 02/12/2023)
47. Publishing Guide, Fitbit. https://dev.fitbit.com/build/guides/publishing/ (visited on 02/19/2023)
48. App Distribution Guide, Samsung Electronics. https://developer.samsung.com/galaxy-store/distribution-guide.html (visited on 02/19/2023)
49. Emine Saner, The Guardian. May 2018. https://www.theguardian.com/world/2018/may/14/is-your-boss-secretly-or-not-so-secretly-watching-you (visited on 02/12/2023)
50. Christina Farr: How Fitbit Became The Next Big Thing In Corporate Wellness, Fast Company. Apr. 2016. https://www.fastcompany.com/3058462/how-fitbit-became-the-next-big-thing-in-corporate-wellness (visited on 02/12/2023)
51. Anupam Das, Nikita Borisov, and Matthew C. Caesar: Tracking Mobile Web Users Through Motion Sensors: Attacks and Defenses. In: Network and Distributed System Security Symposium (2016)
52. Londoners give up eldest children in public Wi-Fi security horror show, Sept. 2014. https://www.theguardian.com/technology/2014/sep/29/londoners-wi-fi-security-herod-clause (visited on 02/15/2023)

53. U.S. soldiers are revealing sensitive and dangerous information by jogging, Jan. 2018. http://wapo.st/2BDFrA4 (visited on 02/15/2023)