I just wanted to track my steps! Blocking unwanted traffic of Fitbit devices

Andrei Kazlouski
Computer Science Department,
University of Crete
Foundation for Research and
Technology, Hellas
Crete, Greece
andrei@ics.forth.gr

Thomas Marchioro
Computer Science Department,
University of Crete
Foundation for Research and
Technology, Hellas
Crete, Greece
marchiorot@ics.forth.gr

Evangelos Markatos
Computer Science Department,
University of Crete
Foundation for Research and
Technology, Hellas
Crete, Greece
markatos@ics.forth.gr

ABSTRACT

The recent advent of wearable fitness trackers has fueled concerns in regards to the privacy they provide. In particular, previous works have indicated that the associated fitness apps may contact unexpected Internet destinations.

In this work we identify the third-party connections of the official mobile Fitbit application and its partners, and study whether they can be blocked without hindering the essential functionality of the devices. We show that disabling traffic to the domains contained in well-maintained blocklists does not prevent Fitbit trackers from correctly reporting activity data, including steps, workouts, duration and quality of sleep, etc. Moreover, we demonstrate that Fitbit activity data are correctly synchronized for 6 partner apps of Fitbit when utilizing the above blocking rules.

Our results suggest that more than 88% of the third parties for the Fitbit-associated apps are contained in credible domain-based blocklists. Furthermore, we find *all* studied app to contact between 1 and 20 non-required third parties. Finally, over 50% of the blocked destinations are identified by the default installation of uBlock Origin – universally used content filter (adblocker).

Unlike previous works on blocking unnecessary IoT communications, our methodology can be easily utilized by end-users.

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**.

KEYWORDS

wearables, privacy, IoT, third parties, traffic filtering

ACM Reference Format:
Andrei Kazlouski, Thomas Marchioro, and Evangelos Markatos. 2022. I just wanted to track my steps! Blocking unwanted traffic of Fitbit devices. In *Proceedings of the 12th International Conference on the Internet of Things (IoT '22), November 7–10, 2022, Delft, Netherlands.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3567445.3567457

1 INTRODUCTION

Global sales of wearable fitness trackers have been drastically increasing for the past decade [24]. The prevalence of remote working and the decline of physical activity levels are likely to maintain the interest in commercial wearable devices in the foreseeable future. Albeit millions of people around the globe utilizing wearables, the end-users have limited control over what Internet destinations are contacted by smart devices as part of their operation. That is mainly due to the fact that installing the official companion app is strictly required to use most fitness trackers available on the market. A number of concerns have been raised in regards to the privacy such applications provide and the risks of ubiquitous data collection on the users of wearables. Previous works have indicated that IoT devices in general [18, 26] and wearable trackers in particular [9, 10] tend to contact a significant number of third parties. In general, any connection that is provided by an entity that is not the manufacturer of a device can be considered third-party. While some of such communications may be essential for the functionality of the device, others are not strictly required and can only compromise the privacy of users. In this paper we refer to such third-party connections as *unwanted*, *undesired*, or *unnecessary*.

Existing methods to utilize wearable devices without contacting unwanted third parties involve installation of custom-made mobile applications [6, 7]. Such apps fully prevent the device from connecting to the Internet but do not support most features of the original applications. Furthermore, these solutions are compatible only with a limited number of commercial wearable devices. Alternatively, a previous work on blocking unnecessary third parties for the communications of IoT devices [11] designed a dynamic solution for identifying and blocking undesired traffic. However, the proposed approach involves different blocking strategies for various device groups and is extremely challenging to set up for end-users. Moreover, since it does not rely on existing maintained blocking lists, false positives may occur which will likely lead to improper functioning of the wearables/apps. Finally, since the previously proposed solutions require a specifically configured Internet access point, they are not applicable when using the device outside of designated networks.

Therefore, we set out to investigate whether a *simpler* solution that can be adopted by regular users exists. As a baseline we consider browser content filtering extensions, better known as adblockers. It is estimated that 763.5 million people utilized them in 2019 [23]; besides being easy to install and use, these extensions appear to be extremely effective at blocking the advertisement and trackers

IoT '22, November 7–10, 2022, Delft, Netherlands

ACM ISBN 978-1-4503-9665-3/22/11…$15.00
https://doi.org/10.1145/3567445.3567457

without "breaking" the visited websites. Furthermore, many of the blocklists are continuously maintained, and, hence, the included filtering rules are carefully considered, reducing the possibility of false positive entries. In this work we analyze the third parties that are being contacted by the Fitbit-associated apps. We examine two popular blocklist collections: uBlock Origin [25] – one of the most popular browser content filtering extensions – and Firebog [5] – another well-known collection of maintained domain lists. We study whether blocking such unwanted destinations disrupts the functionality of the official Fitbit apps and its partners.

We consider the following research questions:

> (Q1) What third parties are being contacted by the Fitbit-associated applications? (Q2) Does blocking domains from the well-regarded blocking lists affect the essential functionality of the devices? (Q3) Which are the most "unwanted" third parties and the highest hitting blocklists?

Our key contributions can be summarized as follows:

- We identify what external entities the Fitbit-associated apps talk to.
- We show that 88.7% of the contacted third parties are unnecessary and are contained in rigorously maintained blocklists.
- We empirically demonstrate that such unnecessary destinations can be disabled without breaking the fitness-related functionality of the applications.
- We establish the most contacted unnecessary third parties and rank the blocklists for the wearable fitness trackers.
- We propose an easy-to-set-up blocking framework for the average Fitbit users.

To our knowledge we are the first to study blocking of the unwanted traffic for wearable applications. Unlike previous works on disabling unnecessary IoT communications, our approach does not get impacted by the changes in network traffic of the studied apps, since the blocking rules rely solely on existing blocklist collections. Furthermore, this method can be easily employed by the regular users of the devices, e.g., via mobile filtering applications (i.e., adblockers), and does not require specific network equipment.

2 RELATED WORK

Previous works have investigated the third-party communications of the IoT devices, whether such connections can be safely disabled, and studied the privacy of wearable devices in general.

Ubiquitous data collection in wearables. The possibility to ubiquitously collect data of users became a real concern with the advent of mobile phones endowed with a wide variety of sensors that are always enabled, and in very close proximity of the owner [20]. It appears that fitness trackers represent the second coming of the problem, since they are literally worn 24/7 and may have even higher modality of collected data. Ball et al. investigated the possibility of mass surveillance of users, utilizing on-body sensors. In [3] the authors established that owners of wearables lack control over the data collected on them. The privacy concerns of users in regards to the data collected with fitness trackers were researched in [4, 17, 27].

Third-party communications of IoT. Prior research has studied what entities are being contacted by IoT devices as part of their operation. A recent paper explored what third parties are being contacted by 7 popular fitness trackers [9]. The "unwanted" connections for the partner applications of Fitbit were studied in [10]. The work established that a number of sensitive attributes may be leaked to undesired third parties. Ren et al. studied the Internet communications of 81 IoT devices [18]. They identified severe privacy leaks and potential exposure of sensitive information. Varmarken et al. studied the Internet connections of two popular smart TV ecosystems Roku and Amazon Fire TV and identified a significant number of advertising and tracking third parties [26]. A number of previous papers have managed to identify IoT devices based on the contacted domains and third parties [8, 15], and the various parameters of network traffic [1, 13, 14, 19, 21].

Blocking unnecessary network traffic. The possibility for blocking non-vital communications of IoT devices has been previously investigated. Varmarken et al. [26] found that DNS-based blocklists may not be very effective at blocking all tracking and advertisement entities for the Smart TV ecosystems. Mandalari et al. proposed a framework for automated testing and analysis of third parties that are communicated by IoT device [12]. They implemented the above framework in [11], where the blocking rules are dynamically developed for different categories of the IoT devices. The authors established that most of the studied devices contact non-required destinations that can de disabled without hindering the essential functionality. Smith et al. [22] presented a classifier to predict if a filtering rule (e.g., a new domain in a blocklist) breaks a website.

3 METHODS

In this section we describe our setup for discovering and blocking unnecessary traffic of the apps, the conducted experiments, and the employed blocklist collections. We also discuss the studied partner applications of Fitbit that synchronize fitness data collected by wearables.

3.1 Setup

In our experiments we utilize two Fitbit Versa 2 fitness trackers and two Xiaomi Redmi 7 phones that run the official Fitbit companion application and studied partner apps. The Internet connection for the phones is set up via a WiFi hotspot of a laptop computer.

Discovering Third Parties. We employ the Man-in-the-Middle (MITM) approach to identify all entities that are being contacted by the studied applications. We set up MITM between the applications and the cloud. MITM essentially pretends to be the target destination of data and allows to view the encrypted traffic in plain text. We do not rigorously examine what data are shared with third parties since it has been done in previous works [10]. Instead, we specifically monitor packets that synchronize Fitbit fitness information, including number of steps, calories, workouts, etc. For MITM we utilize the Burp suite scanner [16]. Some of the studied apps employ certificate pinning – a mechanism to prevent traffic interception by endowing server's certificate credentials inside the application. We leverage the EdExposed framework to bypass it[1].

Blocking Domains. In order to block unnecessary third parties, we modify the *hosts* file for every studied application. This file is produced by the operating system and maps domain names to the

[1] https://www.xda-developers.com/edxposed/

IP addresses. Since hosts file is examined before the Domain Name System (DNS), it allows to resolve the unwanted domains as a localhost (127.0.0.1), preventing packets from traversing the global web. Since the phone Internet connection comes via a WiFi hotspot, all the traffic essentially passes thought the laptop. Therefore, disabling domains on the computer restricts the phone from connecting to them likewise. We keep separate lists of blocked domain names for each application.

Employed Blocklist Collections. Our initial idea was to verify that it is feasible to block the domains that are being contained in the adblockers' filtering rules without breaking the wearable applications. We decided to utilize the content blocker uBlock Origin (henceforth Ublock for convenience), since it is one of the most popular solutions that is used by more than 10 million Chrome[2] and almost 6 million Firefox[3] users. At present Ublock supports more than 50 domain-based filtering lists that are actively maintained by developers and researches. Ublock's blocklist categories include: the default, anti-advertisement, anti-tracking, anti-malware, "annoyancess", and the regional sets. Overall, Ublock supports up to 600K blocking rules. It is remarkable that despite a quite significant number of traffic filters, the continuous maintenance of the blocklists results in a negligible number of false positives and breaking of the websites. Similarly to the previous works on content blocking [11, 26], in this paper we consider another blocklist collection the Firebog (Firebog) [5]. It coalesces various categories of rules, including malicious, advertising, suspicious, and tracking & telemetry lists, with a total of 60 blocklists. Excluding the non-recommended blocklists, Firebog contains more than 5, 300K domains.

It is worth noting that some blocklists are present in both collections, e.g., actively supported *EasyList* and *EasyPrivacy*.

3.2 Experiment

In this section we describe the directed experiments on blocking unwanted third parties.

Official Fitbit app. The aim of the conducted experiments is to learn whether disabling undesired third parties impacts the workflow of the application/devices and fitness data. However, since wearable fitness trackers are much more complex than most of the other IoT devices, it is quite challenging to verify that every aspect of the application/device remains unchanged. For instance, for a smart bulb it is trivial to identify malfunction (if it stops turning on/off). However, wearable devices collect a wealth of various multimodal data and do not have a single most prominent functionality. In this context a natural question to ask is what if the third-party communications affect some of the fitness data that has been gathered. For example, what if disabling `test.com` causes taken steps to be recorded erroneously. Therefore, we set to empirically verify that fitness data which are collected by wearables do not get impacted by the filtering rules.

We set up two identical Fitbit accounts, where we provided the same values of gender, weight, height, age, etc. We paired each of these accounts with a separate copy of Fitbit Versa 2. In our experiment a test subject, who is one of the authors for this work, *simultaneously* wore two fitness trackers on the same hand. For the one of the trackers we disable all the unwanted third parties that has been found in the blocklists; for the other we do not block/intercept anything and use it in the off-the-shelf mode. We compare the values of the collected data to detect any malfunctions. Naturally, since the devices are not worn at the exact same spot, the collected fitness data are likely to differ. Therefore, we conduct a second round of experiment where the test subject wears both devices without blocking anything, in order to assess the baseline difference due to wrist placement, errors, etc. Finally, we compare 2 *differences* for both rounds to conclude if blocking contacted domains significantly alters the discrepancy between the simultaneously worn trackers. Both rounds lasted 5 days, Monday to Friday. The test subject was encouraged to maximize wearing of the devices, and perform as many various trackable activities as possible, including various workouts, sleep, measuring heartbeat, etc.

A user study by Chong et al. [2] found that users of wearable devices consider tracking their steps, sleep, and exercise the primary factors when purchasing a wearable. Therefore, we consider the same metrics when comparing results for 2 devices.

Partner apps of Fitbit. Naturally, it is infeasible to rigorously analyze all of the functionality when blocking third parties for every studied app. Therefore, we simply verify that the data which have been imported from Fitbit match the correspondent values in the Fitbit cloud.

3.3 Partner Apps

We consider some of the partner apps[4] for Fitbit that were studied in [10]. We choose the applications that allow users to synchronize their Fitbit activity data in order to verify whether it is feasible to disable unwanted connections. We utilize the latest available versions of the applications which are specified in Table 1. Below we briefly describe the apps and what Fitbit data are being synchronized.

- *MyFitnessPal* (App2). A health tracking application that requests calories and the step count from Fitbit.
- *Strava* (App3). An app to track one's running/cycling activities (e.g., workouts that can be placed on a map). It allows users to synchronize their GPS Fitbit workouts.
- *Runkeeper* (App4). A running application that extracts Fitbit workouts.
- *Weightloss Running* (App5). Another running application that allows users to synchronize their workouts and step count with Fitbit.
- *Wokamon* (App6). A mobile game where progress is based on the number of steps that are record with a Fitbit device. Additionally synchronizes the burned calories.
- *Nudge* (App7). A health application to connect with coaches and obtain personalized training. It extracts the number of steps, heartbeat, and workouts.

4 RESULTS

In this section we display our results and answer the research questions put forth in the introduction.

[2] https://chrome.google.com/webstore/detail/ublock-origin/cjpalhdlnbpafiamejdnhcphjbkeiagm

[3] https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/

[4] The detailed description of the apps and the supported interactions with Fitbit can be found here: https://staticcs.fitbit.com/partnership

	App and version	All Third Parties	# Blocked
	Fitbit v3.18	graph.facebook.com, api.mixpanel.com, decide.mixpanel.com, cdn.optimizely.com, m.stripe.com, mcbs1myt8rhvg1jhw6dlgdpy4fly.device.marketingcloudapis.com, s7.device.marketingcloudapis.com, app-measurement.com, logx.optimizely.com, firebase-settings.crashlytics.com, settings.crashlytics.com, in.appcenter.ms	10/12
Partner Apps	MyFitnessPal v22.15.0	graph.facebook.com, sdk.iad-06.braze.com, z.moatads.com, api2.branch.io, firebase-settings.crashlytics.com, crashlyticsreports-pa.googleapis.com, cdn.branch.io, sdk.split.io, api.segment.io, aax-eu.amazon-adsystem.com, c.amazon-adsystem.com, mads.amazon-adsystem.com, api2.amplitude.com, ads.mopub.com, googleads.g.doubleclick.net, pubads.g.doubleclick.net, auth.split.io, streaming.split.io, events.split.io, d34yn14tavczy0.cloudfront.net, pagead2.googleadservices.com	20/21
	Strava v267.9	graph.facebook.com, sessions.bugsnag.com, api2.branch.io, cdn.branch.io, app.adjust.com, api.iterable.com, events.mapbox.com, api.mapbox.com	7/8
	Runkeeper v13.4	graph.facebook.com, api.iterable.com, launches.appsflyer.com, api2.amplitude.com, crashlyticsreports-pa.googleapis.com, beacons.gcp.gvt2.com	6/6
	Weightloss Running v6.8.13	graph.facebook.com, launches.appsflyer.com, ads.mopub.com, api2.amplitude.com	4/4
	Wokamon v2.17.5	graph.facebook.com, api.share.mob.com, c.data.mob.com, api.exc.mob.com, m.data.mob.com , ms.applovin.com, rt.applovin.com, connect.tapjoy.com, a4.applovin.com, d.applovin.com, rpc.tapjoy.com, placements.tapjoy.com, googleads.g.doubleclick.net, pagead2.googleadservices.com, data.flurry.com	15/15
	Nudge v6.3.3	exp.host, sentry.io, ws-mt1.pusher.com, sockjs-mt1.pusher.com, sock252-mt1.pusher.com	1/5

Table 1: Third parties contacted by the studied apps. The domains that are not contained in the blocklists are in teal; the rest are unnecessary and can be disabled. We report the blockable/total number of contacted third-party destinations per application. Fitbit is not listed as a third party for partner apps.

4.1 Analysis of Third Parties

In order to answer Q1, we start by describing what third parties Fitbit and its partner apps talk to. Table 1 depicts all the third parties that are being contacted by the apps as part of their operation. We do not report Fitbit API as a third party for the partner apps, since it is an expected destination in order to request fitness data. It is evident that both the official Fitbit application and the partner apps contact a significant number of external domains. Moreover, 3/7 studied applications contact *only* undesired third parties. The obtained results suggest that the unwanted entities are mostly advertisement providers, analytics/tracking services, and various content delivery network. It is worth noting that 6/7 applications send data to Facebook, even if users do not attempt to log in via the social network.

We further investigate what are the most contacted unnecessary destinations for wearable applications. Figure 1 depicts the data flows between the studied applications and the unwanted third parties. There we aggregate third parties to the organizations that run them. For example, Google is represented by not only Google advertisement but also Crashlytics – an analytics provider owned by Google. In the figure, the width of a flow is proportional to the number of second-level domains. For example, since the apps that contact Branch communicate with both api2.branch.io and cdn.branch.io, the correspondent flow is twice the size of Iterable, which is represented by a single domain (api.iterable.com). It is evident that the most prevalent third-party organizations are Facebook (Meta) and Google: they are contacted by 6/7 and 4/7 applications accordingly. Furthermore, a number of companies, including Google, Amazon, and Branch, provide more than a single second-level domain per their service. We further depict the individual third parties that are being contacted by multiple applications in Table 2, where most of domains are being contacted by 2 apps.

Third Party	Apps
graph.facebook.com	1,2,3,4,5,6
firebase-settings.crashlytics.com	1,2
crashlyticsreports-pa.googleapis.com	2,4
pagead2.googleadservices.com	2,6
googleads.g.doubleclick.net	2,6
*.branch.io	2,3
api2.amplitude.com	2,4
launches.appsflyer.com	4,5
ads.mopub.com	2,5
api.iterable.com	3,4

Table 2: Unnecessary domains contacted by multiple apps. The applications are numbered according to their order in Table 1 and as indicated in Section 3.3.

To get a better understanding of what proportion of all contacted entities for wearable applications needs to be disabled, we report

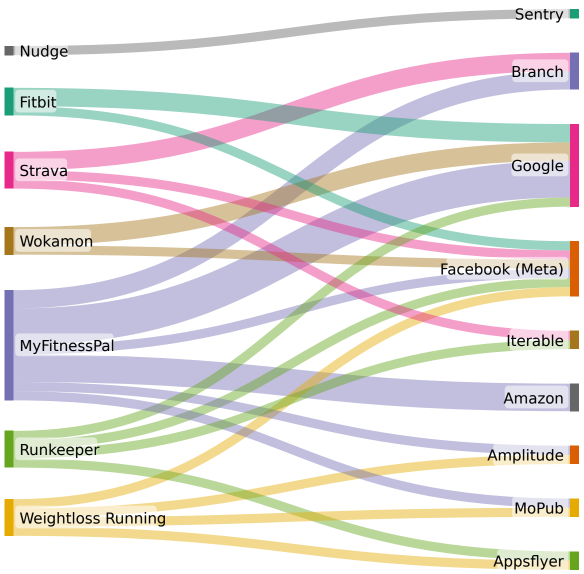


Figure 1: Mapping of the Fitbit-associated apps to the companies that host unnecessary third parties. The widths of the flows correspond to the number of second level domains per organisation. The most contacted organisations are shown.

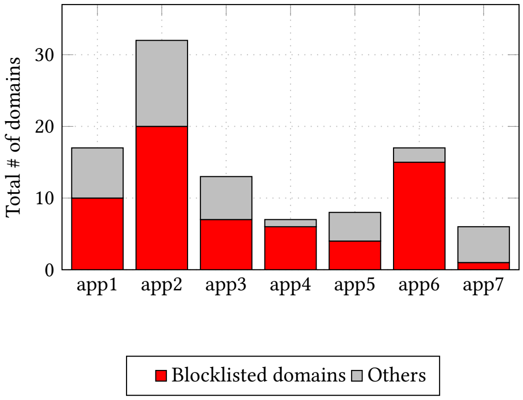


Figure 2: The percentage for unnecessary third party connections of all the contacted domains (including first parties). The Apps are numbered according to their order in Table 1 and as indicated in Section 3.3.

the individual results for every app in Figure 2. We consider *all* the connections, including first parties, Fitbit API and all other entities that are omitted from Table 1. It is evident that for almost all applications the number of unwanted connections exceeds 50%. In other words, at least half of the contacted destination may be unnecessary or even harmful for wearable applications.

Overall, the obtained results indicate that more than 88% of the third parties are unwanted.

Again, in this study we *do not focus* on the data sent to the third parties. For in-depth details please refer to our previous work [10]. Nevertheless, in Table 3 we report high-level insights that are leaked. Such information includes Android Advertising ID (AAID), details on the Phone characteristics, approximate and exact location, connection specifics (WiFi or cellular), email, and even demographics.

For example, a unique cross-app AAID is being shared with graph.facebook.com which is contacted by almost all the apps, enabling the social network to monitor individuals beyond its userbase. Latitude/longitude are sent to events.mapbox.com every second. Massive bulks of private data are sent to api.segment.io, sharing email, gender, age, lifestyle and many more. Naturally, such data are extremely sensitive and can be utilized for mass profiling.

Data	Apps
Phone manufacturer, model, etc.	ALL
AAID	1,2,3,4,5,6
EMAIL	1,2,3,4
Connection details	1,2,4
Location	2,3,5
Demographics	2

Table 3: Sensitive information shared by studied apps with third parties. Applications are numbered according to their order in Table 1 and as indicated in Section 3.3. For each app the data are shared with at least one of the unwanted third parties from Table 1.

4.2 Blocking Unnecessary Traffic

In this section we report the results obtained from our experiments, answering Q2. In Table 4 we disclose all the raw daily cumulative data for both rounds of experiment. We detail daily steps, distance and calories, as well as various type of sleep. Again, the test subject simultaneously wears both devices on one hand. In the first round both wearables contact all the default third-party connections in order to establish the baseline difference due to varying position of the trackers. For the second round we disable all the unnecessary connections that are shown in Table 1. Visually, it appears that there seem to be no significant difference between the discrepancy between rounds. It seems that concurrently worn trackers sometimes may interchange REM and light sleep minutes. However, the total nightly sleep seems to be recorded consistently.

Nevertheless, to be more formal, we report the statistical differences between the errors of two rounds. As a matter of fact, standard statistical tests, including t-test or Kolmogorov–Smirnov test can only reject the null hypothesis of the datapoints coming from the same distribution. In other words, it is unfeasible to accept the null hypothesis and claim that the data from both rounds are similar (even though they are coming from identical devices on the same hand). Therefore, we report the statistical values that can be interpreted for our case in Table 5. We display the Root Mean Square Error (RMSE) and Normalized RMSE (NRMSE) for the daily values of activities between the devices. We separately calculate RMSE/NRMSE for both rounds and then estimate the difference between the errors. It appears that the highest NRMSE difference is observed for light/REM sleep, and the lowest for the total duration of sleep. The obtained results suggest that there is no significant discrepancy between the identical and modified pairs of the devices.

Activity	Band	Round 1					Round 2				
		Day 1	Day 2	Day 3	Day 4	Day 5	Day 1	Day 2	Day 3	Day 4	Day 5
Steps	1	2184	4869	2960	5140	7685	2077	6670	4888	2859	3194
	2	2110	4862	3019	5035	7706	2023	6660	4759	2799	3032
Distance	1	1650	3700	2120	3900	7710	1530	7190	3710	2160	2390
	2	1600	3690	2060	3820	7060	1500	6420	3610	2120	2300
Sleep Total	1	425	546	408	429	449	427	407	452	470	390
	2	424	538	418	447	462	426	399	432	467	403
Light Sleep	1	294	317	283	277	303	287	276	319	268	285
	2	289	353	274	257	312	276	310	314	252	289
REM Sleep	1	98	162	65	71	98	88	71	93	116	60
	2	102	113	78	103	106	103	44	78	140	68
Deep Sleep	1	33	67	60	81	48	52	60	40	86	45
	2	33	72	66	87	44	47	45	40	75	46

Table 4: A complete listing of the obtained results. Both bands are simultaneously worn on the same hand. For the second device in round 2 the unnecessary third parties were disabled. Distance is measured in meters; sleep in minutes.

Activity	RMSE R1	RMSE R2	NRMSE R1	NRMSE R2
Steps	64	99.5	0.011	0.021
Distance	295	350.3	0.048	0.062
Sleep Total	11.5	11.3	0.083	0.141
Light Sleep	19.4	17.7	0.202	0.264
REM Sleep	27.1	19.1	0.279	0.199
Deep Sleep	4.8	8.7	0.089	0.189

Table 5: Comparison of Root Mean Square Error (RMSE) and Normalized RMSE (NRMSE) for round 1 (R1) and 2 (R2).

Regarding partner apps, we verified that blocking unnecessary destinations does not affect the Fitbit data from being correctly imported, since all the values that have been observed for the partners replicate the original ones in the Fitbit cloud. Overall, it appears that blocking unwanted destinations does not impact the workflow of the official Fitbit application and studied partner apps.

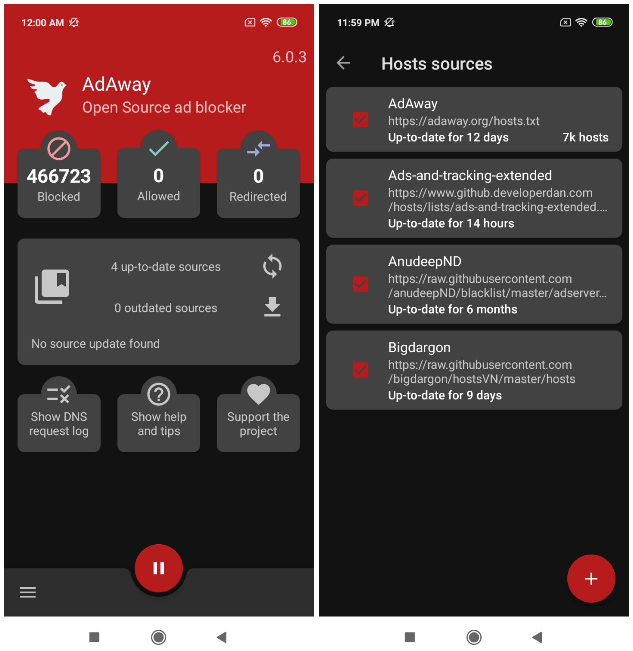
4.3 Examination of Blocklists

Once we verified that the domain-based filtering rules do not break the essential functionality of the wearable apps, we set to answer Q3, i.e., which third parties are the "most undesirable".

We rank third parties based on the number of blocklists that include the correspondent domains in Table 6. Essentially, we identify as "most unwanted" those entities that have been incorporated in many blocklists designed for *various* kinds of unwanted content. We find Google's DoubleClick and Amazon's AdSystem to be the highest hitting entities that are all contained in more than 10 various filtering lists. Furthermore, all such domains are disabled by the default installation of Ublock that runs on millions of computers around the globe. Another interesting finding is that only 8 unnecessary third parties are present in the blocklists of exclusively Firebog, with the rest being contained in both collections. Hence, simply employing a popular adblocker would immensely help regular users to protect their privacy, with their wearable devices still being fully operatable.

Further addressing Q3, we study what are the most effective blocklists for disabling unwanted connections of wearable applications. The obtained results are depicted in Table 7, and, unsurprisingly, the "winners" are the filtering lists that focus on mobile tracking and advertisement. In fact, 2 of the most prominent and well-maintained lists *EasyList* and *EasyPrivacy* contain only 4 unnecessary domains. That is likely due to the fact that they are mostly employed to address web advertising and tracking instead.

We further stress that the proposed approach can be set up by an *average* Fitbit user via ad blocking apps, as shown in Figure 3.



12:00 AM

6.0.3

AdAway
Open Source ad blocker

466723 Blocked
0 Allowed
0 Redirected

4 up-to-date sources
0 outdated sources
No source update found

11:59 PM

Hosts sources

☑ AdAway
https://adaway.org/hosts.txt
Up-to-date for 12 days — 7k hosts

☑ Ads-and-tracking-extended
https://www.github.developerdan.com/hosts/lists/ads-and-tracking-extended....
Up-to-date for 14 hours

☑ AnudeepND
https://raw.githubusercontent.com/anudeepND/blacklist/master/adserver...
Up-to-date for 6 months

☑ Bigdargon
https://raw.githubusercontent.com/bigdargon/hostsVN/master/hosts
Up-to-date for 9 days

Figure 3: An open-source Android ad blocker AdAway[5]with 4 highest hitting blocklists for wearables as per Table 7.

# Occurrences	Third Parties	Collection	Ublock Default
18	googleads.g.doubleclick.net	UF	Yes
16	pubads.g.doubleclick.net	UF	Yes
15	aax-eu.amazon-adsystem.com	UF	Yes
14	c.amazon-adsystem.com	UF	Yes
13	ads.mopub.com, mads.amazon-adsystem.com	UF, UF	No, Yes
11	z.moatads.com	UF	Yes
10	app-measurement.com	UF	No
9	api.mixpanel.com, pagead2.googleadservices.com, data.flurry.com	UF, UF, F	No, Yes, No
8	decide.mixpanel.com, launches.appsflyer.com, d.applovin.com	UF, UF, UF	No, No, No
7	api2.branch.io, api2.amplitude.com, events.mapbox.com,	UF, UF, UF	No, Yes, Yes
	m.data.mob.com, api.exc.mob.com, api.share.mob.com,	UF, UF, UF	No, No, No
	ms.applovin.com, rt.applovin.com, *.tapjoy.com	UF, UF, UF	No, No, Yes
6	settings.crashlytics.com, api.segment.io,	UF, UF	Yes, No
	events.split.io, cdn.branch.io, c.data.mob.com	UF, F, UF	Yes, No, No
5	logx.optimizely.com, sdk.iad-06.braze.com,	UF, UF	Yes, No
	crashlyticsreports-pa.googleapis.com, app.adjust.com	UF, UF	Yes, Yes
4	cdn.optimizely.com, firebase-settings.crashlytics.com,	F, UF	No, Yes
	sessions.bugsnag.com, api.iterable.com	UF, UF	No, Yes
3	sdk.split.io, auth.split.io, beacons.gcp.gvt2.com, a4.applovin.com	F, F, UF, UF	No, No, Yes, No
2	graph.facebook.com	F	No
1	*.device.marketingcloudapis.com, streaming.split.io, sentry.io	F, F, F	No, No, No

Table 6: Ranking of the unnecessary third parties based on the number of blocklists containing them. We show whether a third party is detected by a collection of blocklists (U = Ublock, F = Firebog, UF = both). We also report if a third party is blocked by a default installation of uBlock Origin.

Blocklist	# Blocked	Collection
bigdargon	38	Firebog
ads-and-tracking-extended	38	Firebog
adaway	36	Firebog
anudeepND	32	Firebog
VeleSila	17	Firebog
AdGuard Mobile Ads	14	Ublock
Peter Lowe’s list	14	Ublock
someonewhocares	12	Firebog
RooneyMcNibNug	10	Firebog
jdlingyu	10	Firebog
Dan Pollock’s list	10	Ublock
AdGuard Tracking Protection	10	Ublock
neohostsbasic	9	Firebog
winhelp2002	9	Firebog
Perflyst android-tracking	8	Firebog
KOR: List-KR	6	Ublock
POL list	5	Ublock
EasyPrivacy	4	Firebog Ublock
EasyList	4	Firebog Ublock

Table 7: Ranking of blocklists based on the number of unnecessary third parties of wearables. Only lists that contain at least 4 different domains are included.

5 DISCUSSION

Since all studied applications contact unnecessary third parties, we believe the problem of disabling undesired communication for wearables to be of utmost importance. Since any contact with a third party may leak potentially (or very) sensitive information, it is in users’ best interest to disable such communications.

Smart Kettle vs Smartband. While for some simple IoT devices it is relatively straightforward to verify that essential functionality is preserved, it is a much harder task for the compound smartwatches. As indicated previously, there is no single button or task that distinctly defines the device. Therefore, it requires much more effort and time in order to study its entire functionality. Furthermore, even if blocking third parties does not hinder the collected activity data, it is entirely possible that some other aspects of the application, e.g., chats, fitness communities or global leaderboards may be impacted. In order to claim that disabling third parties does not affect its functionality, one has to rigorously verify every single aspect of the app (which may be unfeasible). Nevertheless, we believe our approach to be appropriate, since we specifically test the aspects that are essential for the vast majority of users.

Domain-based filtering. Previous works have indicated that readily available blocklists may not be the ideal solution for some of the IoT devices [11] and smart TVs [26]. Mainly, the authors argue that such collections do not include a considerable number of unnecessary third parties, resulting in low recall. However, trying to block everything increases the chance of encountering false positive domains and can cause improper functioning of the devices/applications. In our case we strife to ensure that the apps

[5] https://adaway.org/

remain working correctly even at a cost of missing potentially "blockable" entities. Furthermore, since a significant number of researches and maintainers are studying unwanted mobile connections, domain-based blocklists are likely to include many more unwanted third parties for wearables compared to other types of IoT devices that do not connect via companion apps. The results obtained in this work indicate that, indeed, utilizing exclusively existing filtering lists seems to be appropriate for fitness trackers.

Limitations and future work. As a matter of fact, one cannot claim that blocking the traffic destinations envisioned by the developers will *never* result in "breaking" the applications. However, this issue is inherent for all works in the field of content filtering and it is always a tradeoff between increasing the recall of unnecessary connections and a chance to compromise the functionality.

Potential directions for future research include studying other wearable fitness trackers and partner applications. We also consider running longer experiments on wearables to not only obtain better statistical insights but also to study how blocking undesired third parties impacts the battery levels, CPU consumption, and the volume of network traffic. Finally, we plan to eventually release our own personal blocklist to disable unnecessary communications of wearable devices and applications.

6 CONCLUSION

In this work we show that it is feasible to disable the undesired connections of Fitbit devices without hindering the functionality of the associated applications and spoiling the collected fitness data. We propose an approach that enables analysis of the unnecessary destinations for the wearable applications and allows to block the unwanted traffic. We demonstrate that more than 88% of the identified third parties are contained in the credible blocklist collections and can be disabled without breaking the apps or devices. We show that even a default installation of uBlock Origin which is used by millions of people around the globe would have blocked more than half of the contacted destinations. Most of the found unnecessary third parties include advertisement services, tracking and analytics providers, and even social networks. We find Facebook, Google and Amazon to be the most contacted unnecessary destinations, with Google and Amazon being also the most "blockable" organizations. Our approach can be easily utilized by the end-users of the Fitbit devices via various mobile content filtering applications.

ACKNOWLEDGMENTS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 813162. The content of this paper reflects the views only of their author (s). The European Commission/ Research Executive Agency are not responsible for any use that may be made of the information it contains.

REFERENCES

[1] Ahmet Aksoy and Mehmet Hadi Gunes. 2019. Automated iot device identification using network traffic. In *ICC 2019-2019 IEEE International Conference on Communications (ICC)*. IEEE, 1–7.

[2] Kimberly PL Chong, Julia Z Guo, Xiaomeng Deng, and Benjamin KP Woo. 2020. Consumer perceptions of wearable technology devices: retrospective review and analysis. *JMIR mHealth and uHealth* 8, 4 (2020), e17544.

[3] Kate Crawford, Jessa Lingel, and Tero Karppi. 2015. Our metrics, ourselves: A hundred years of self-tracking from the weight scale to the wrist wearable device. *European Journal of Cultural Studies* 18, 4-5 (2015), 479–496.

[4] Kaja Fietkiewicz and Aylin Ilhan. 2020. Fitness tracking technologies: Data privacy doesn't matter? The (un) concerns of users, former users, and non-users. In *Proceedings of the 53rd Hawaii International Conference on System Sciences*.

[5] The Firebog. 2022. *The Big Blocklist Collection*. Retrieved August 25, 2022 from https://firebog.net/

[6] Freemyband. 2021. *Free my band*. Retrieved August 25, 2022 from https://www.freemyband.com/

[7] Gadgetbridge. 2022. *Gadgetbridge*. Retrieved August 25, 2022 from https://gadgetbridge.org/

[8] Hang Guo and John Heidemann. 2020. Detecting iot devices in the internet. *IEEE/ACM Transactions on Networking* 28, 5 (2020), 2323–2336.

[9] Andrei Kazlouski, Thomas Marchioro, Harry Manifavas, and Evangelos Markatos. 2020. Do you know who is talking to your wearable smartband? *Integrated Citizen Centered Digital Health and Social Care* (2020), 142.

[10] Andrei Kazlouski, Thomas Marchioro, Harry Manifavas, and Evangelos Markatos. 2021. Do partner apps offer the same level of privacy protection? The case of wearable applications. In *2021 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*. IEEE, 648–653.

[11] Anna Maria Mandalari, Daniel J Dubois, Roman Kolcun, Muhammad Talha Paracha, Hamed Haddadi, and David Choffnes. 2021. Blocking Without Breaking: Identification and Mitigation of Non-Essential IoT Traffic. *Proceedings on Privacy Enhancing Technologies* 4 (2021), 369–388.

[12] Anna Maria Mandalari, Roman Kolcun, Hamed Haddadi, Daniel J Dubois, and David Choffnes. 2020. Towards automatic identification and blocking of non-critical iot traffic destinations. *arXiv preprint arXiv:2003.07133* (2020).

[13] Yair Meidan, Michael Bohadana, Asaf Shabtai, Juan David Guarnizo, Martín Ochoa, Nils Ole Tippenhauer, and Yuval Elovici. 2017. ProfilIoT: a machine learning approach for IoT device identification based on network traffic analysis. In *Proceedings of the symposium on applied computing*. 506–509.

[14] Markus Miettinen, Samuel Marchal, Ibbad Hafeez, N Asokan, Ahmad-Reza Sadeghi, and Sasu Tarkoma. 2017. Iot sentinel: Automated device-type identification for security enforcement in iot. In *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2177–2184.

[15] Roberto Perdisci, Thomas Papastergiou, Omar Alrawi, and Manos Antonakakis. 2020. Iotfinder: Efficient large-scale identification of iot devices via passive dns traffic analysis. In *2020 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE Computer Society, 474–489.

[16] Portswigger. 2022. *What do you want to do with Burp Suite?* Retrieved August 25, 2022 from https://portswigger.net/burp

[17] Andrew Raij, Animikh Ghosh, Santosh Kumar, and Mani Srivastava. 2011. Privacy risks emerging from the adoption of innocuous wearable sensors in the mobile environment. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 11–20.

[18] Jingjing Ren, Daniel J Dubois, David Choffnes, Anna Maria Mandalari, Roman Kolcun, and Hamed Haddadi. 2019. Information exposure from consumer iot devices: A multidimensional, network-informed measurement approach. In *Proceedings of the Internet Measurement Conference*. 267–279.

[19] Mustafizur R Shahid, Gregory Blanc, Zonghua Zhang, and Hervé Debar. 2018. IoT devices recognition through network traffic analysis. In *2018 IEEE international conference on big data (big data)*. IEEE, 5187–5192.

[20] Katie Shilton. 2009. Four billion little brothers? Privacy, mobile phones, and ubiquitous data collection. *Commun. ACM* 52, 11 (2009), 48–53.

[21] Arunan Sivanathan, Hassan Habibi Gharakheili, Franco Loi, Adam Radford, Chamith Wijenayake, Arun Vishwanath, and Vijay Sivaraman. 2018. Classifying IoT devices in smart environments using network traffic characteristics. *IEEE Transactions on Mobile Computing* 18, 8 (2018), 1745–1759.

[22] Michael Smith, Peter Snyder, Moritz Haller, Benjamin Livshits, Deian Stefan, and Hamed Haddadi. 2022. Blocked or Broken? Automatically Detecting When Privacy Interventions Break Websites. *arXiv preprint arXiv:2203.03528* (2022).

[23] Statista. 2020. *Number of adblock users worldwide from 2013 to 2019*. Retrieved August 25, 2022 from https://www.statista.com/statistics/435252/adblock-users-worldwide/

[24] Statista. 2022. *Wearables unit shipments worldwide from 2014 to 2021*. Retrieved August 25, 2022 from https://www.statista.com/statistics/437871/wearables-worldwide-shipments/

[25] uBlock Origin. 2022. *uBlock Origin - Free, open-source ad content blocker*. Retrieved August 25, 2022 from https://ublockorigin.com/

[26] Janus Varmarken, Hieu Le, Anastasia Shuba, Athina Markopoulou, and Zubair Shafiq. 2020. The tv is smart and full of trackers: Measuring smart tv advertising and tracking. *Proceedings on Privacy Enhancing Technologies* 2020, 2 (2020).

[27] Jessica Vitak, Yuting Liao, Priya Kumar, Michael Zimmer, and Katherine Kritikos. 2018. Privacy attitudes and data valuation among fitness tracker users. In *International Conference on Information*. Springer, 229–239.