Do partner apps offer the same level of privacy protection? The case of wearable applications

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

Harry Manifavas
Computer Science Department, University of Crete
Foundation for Research and Technology, Hellas
Crete, Greece
harryman@ics.forth.gr

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

***Abstract*—We analyze partner health apps compatible with the Fitbit fitness tracker, and record what third parties they are talking to. We focus on the ten partner Android applications that have more than $50,000$ downloads and are fitness-related. Our results show that most of the them contact "unexpected" third parties. Such third parties include social networks; analytics and advertisement services; weather APIs. We also investigate what information is shared by the partner apps with these unexpected entities. Our findings suggest that in many cases personal information of users might be shared, including the phone model; location and SIM carrier; email and connection history.**

***Index Terms*—privacy, security, fitness trackers, wearable devices.**

I. Introduction

Fitness trackers have seen a substantial increase in sales over the past years. "Office lifestyle" and continuous Coronavirus lockdowns are likely to further boost the demand for wearables in the nearest future. At present major wearable companies offer a number of devices from primitive smartbands to advanced smartwatches. Naturally these devices collect and process vast amount of private health data, including heart rate, number of steps, amount of sleep, etc. Many of the companies that produce wearable devices have partnerships with various other services. Customers can choose to synchronize their health data and activities with these compatible applications of their choice. Such partners include various health services, major retailers, service applications, and even voice assistants. Smartbands' users are able to allow these apps to access various categories of their personal data that are collected by wearable devices, in order to improve the quality of service or to go after a richer experience. Partner apps allow users to connect with real-life coaches, enable convenient tracking of workouts, and even reward users for active lifestyle. Once users agree to share their fitness information with the partner apps, after each synchronization it is sent to the permanent storage of affiliated companies.

On the negative side, however, the increasing use of wearables contributes to the growing concerns with respect to the privacy they provide. While major vendors, including Fitbit, Apple, Garmin, Xiaomi, Huawei, etc. are challenged to protect privacy of their users, the partner apps often do not receive the same attention from privacy activists. In this paper we set to investigate whether these partner apps offer high standards of privacy protection. In particular, we focused on Fitbit - one of the major wearable companies. At present Fitbit affiliates with more than 40 partner apps[1]. We studied 10 partners that offer Android apps, provide health service, and have at least $50,000$ downloads in Google Play. In particular, we investigated the following questions:

> What entities are talking to these partner apps as part of their operation (or vice versa)? Who are these third parties and what data are being shared with them?

In this paper we investigate third parties that are contacted by the services compatible with Fitibit. The

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.

[1]https://www.fitbit.com/global/us/technology/partnership

contributions of this paper can be summarized as follows:

- We identify the entities that talk to ten partner apps of Fitbit.
- We analyze the content that is being shared to the detected third parties.
- We show that several of the apps talk to unexpected services including social networks, weather sites, analytics, sites, etc. revealing personal information about their users.

To our knowledge this is the first work to investigate the privacy aspects of the partner smartband applications in *practice*.

II. Related Work

Previous studies discussed the data that are shared with third parties, analyzed privacy of wearable devices, and investigated privacy policies of the IoT services.

Privacy of fitness trackers. Ubiquitous data collection by IoT devices has raised great privacy concerns recently. Hilts et al. analyzed the privacy and security of eight popular wearable fitness tracking devices [1]. Ball et al. studied big data in context of IoT [2]. Both works have raised attention to the potential mass surveillance of users. Vitak et al. and Raij et al. investigated levels of concern for users about their data been shared [3], [4]. Peppet investigated how the IoT market is regulated from the standpoint of privacy and consent [5]. Crawford et al. found that users have little control over their personal information once it has been collected [6].

Sharing data. The process for sharing personal data of users is regulated by privacy policies. A company's privacy policy is obligated to mention what personal data can be shared to which third parties. However, making it possible to accept the policy without reading it, drastically decreases the number of users who study privacy agreements. Meinert et al. established that less than 50% of users had ever read a privacy agreement [7]. Moreover, when users can skip through a privacy policy, they are less motivated to understand it [8], [9]. Besides, companies often deliberately draft terms and conditions in a specific way. Balebako et al. found that privacy policies tend not to be clearly written [10]. Vague policies authorize companies to uncontrollably gather and share (sell) private data of users.

Relevance of wearable data. Prior works have suggested that fitness information collected by wearable devices can be utilized for predicting several health-related parameters, such as heart diseases [11], colorectal cancer [12], quality of sleep [13], and even COVID-19 pandemic trend [14].

III. Methodology

In this section we describe the studied partner apps; as well as the procedure for establishing the contacted third parties, and data shared with them.

A. Detecting Third Parties.

To detect what third parties are contacted by partner apps we employed a three-steps pipeline:

Detecting contacted domains and IP addresses. Since partner apps encrypt the communicated data, we intercepted the traffic between the app and the cloud with a Man in the middle (MITM) setup. Essentially MITM (i) decrypts the IP packets, (ii) shows the traffic contents,(iii) re-encrypts the traffic, and (iv) dispatches IP packets to their destination. We obtained both the full URLs and IP addresses of third parties from this setup. We employed the Burp Suite[2] implementation of MITM. Note that most of the studied apps employ certificate pinning to prevent MITM. We utilized the Xposed[3] framework to disable it.

Identifying the data shared with third parties. Since MITM decrypts the IP packets, we were able to check the contents of traffic that is sent from the partner apps to third parties. Once we had access to the plain text data that are shared with third parties, we searched for any private information inside. Contrary to popular belief, personal information can be sent via *both* POST and GET requests. In some rare instances third parties used custom encoding before applying the TLS encryption. In such cases we were unable to identify the content of the transmitted packets. We distinguish between fitness data that are collected by a smartband, and other private information, including IP, location, phone characteristics, etc.

Learning about third parties. During this step we tried to establish what is the nature of contacted third parties, i.e. what service they provide. This step turned out to be the most challenging one. A number of domain names for detected third parties (e.g. `d34yn14tavczy0.cloudfront.net`) do not instantly reveal who owns them or what they focus on. To learn the physical location of third parties we utilized Geoip[4]. To investigate the nature of third-party services, we employed Whois[5], and web search in general.

To summarize, for each partner app we detect:

- The contacted third parties.
- If/what sensitive data are being shared.
- Origins and physical location of their servers.

[2]https://portswigger.net/burp
[3]https://repo.xposed.info/module/de.robv.android.xposed.installer
[4]https://geoip.com
[5]https://www.whois.com/whois/

B. Partner Apps

We consider only the partner apps that are listed on the official Fitbit website. We chose only official Android apps that count more than $50,000$ downloads in Google play, and offer additional health service. E.g. we did not study official retail partners like Walgreens or Dick's Sporting Goods that offer discounts based on how active a person has been. We also did not rigorously analyze the apps that require special equipment. Many of the studied apps support other wearable trackers. We present partner apps sorted by the number of downloads in descending order.

MyFitnessPal. A prominent health app that tracks many health aspects of users. It collects a number of burned calories from Fitbit to modify daily calories goal. The app was downloaded more than 50 million times, and is one of the most popular health apps available.

Strava. A well-known fitness tracker app. Workouts recorded by Fitbit can be synchronized with the Strava application. It has $10+$ million downloads.

MapMyRun, RunKeeper and Endomondo. These apps are tracking running activities. Synchronization with Fitbit allows them to pull workouts recorded by the smartband. All three of the apps were downloaded more than 10 million times.

MINDBODY. Is the training app that allows users to sign up for the classes in their local area. Mindbody pulls the training data from a Fitbit smartband. It counts more than 1 million installs as of October 2020.

Weightloss Running. Is the app that offers personal training plans for its users. The application pulls the training data from Fitbit. It was downloaded 1 million times.

Hidrate Spark. A health app that tracks water consumption. It receives the steps information from Fitbit and adjusts the daily water consumption goal. The app counts 100 thousand downloads.

Wokamon. Wokamon is a mobile game that encourages adopting a healthy lifestyle. It accounts step data from a Fitbit tracker for in-game rewards. The app was downloaded more than 100 thousand times.

Nudge Health Tracking. Is a health app that enables users to connect with real-life coaches. The Nudge app pulls various health snapshots from the Fitbit account. As of October 2020 the application counts 50 thousand installs.

We conduct our research from Europe. That makes a difference, because a number of third parties own dedicated EU servers. The results of our findings might differ for other locations.

IV. Results

In this section we describe the third parties that are contacted by Fitbit's partner apps. Table I depicts what sensitive data third parties receive from the partner apps. Table II depicts the detailed description of the third parties and the Internet Service Providers (ISPs) that host their servers.

Since contacting Fitbit as a third party is expected for every app, we do not mention it in this section. We report the most "interesting" findings about the studied partners. We also break down the most significant data leaks, and percentages of apps that contact particular third-party services.

TABLE I
DATA THAT ARE SHARED WITH THE THIRD PARTIES DURING RUNTIME OF THE FITBIT'S PARTNER APPS. **PHONE DATA** ACCOUNTS FOR THE MANUFACTURER,MODEL, OS, AND SCREEN RESOLUTION.

App	Shared Data	Third Party
MyFitnessPal	Phone model	Facebook
	Location	Facebook
	Phone Data	Branch
	Connection Data	Amplitude
	Phone Data	Amazon
	Phone Details	Google
Strava	Connection Data	Branch
	Phone Data	Branch
	Phone Details	Bugsnag
MapMyRun	Phone Data	Branch
	Phone Data	Amplitude
RunKeeper	Phone Data	Facebook
	Location	Facebook
	Email	Iterable
	Phone Data	Iterable
	Phone Data	Amplitude
	location	Amplitude
	Phone Details	Google
Endomondo	Phone Data	Facebook
	Location	Facebook
	Location	Amplitude
	Phone Data	Amplitude
MINDBODY	Email	Mparticle
	Connection Data	Branch
	Phone Data	Branch
	Connection Data	Newrelic
Weightloss	Phone Model	Facebook
	Location	Facebook
	Sim Carrier	Facebook
	App Data	Appsflyer
	Phone Details	Google
	Phone Data	Facebook
HidrateSpark	Phone Data	Facebook
	Location	Facebook
	App Details	Facebook
	Phone Details	Google
Wokamon	Phone Data	Supersonicads
	Connection Data	Supersonicads
	Sensor Data	Facebook
	Phone Data	Facebook
Nudge	Phone Data	Facebook
	Location	Facebook
	Sim Carrier	Facebook
	Connection data	Branch
	Phone Data	Branch

TABLE II

THIRD PARTIES THAT ARE CONTACTED BY THE PARTNER APPS. **ORIGIN** REPRESENTS THE HEADQUARTERS LOCATION OF ISPS. THE **SITE** COLUMN REFERS TO THE *physical* LOCATION OF THE CONTACTED SERVERS. **ROLE** DESCRIBES SERVICES THAT THIRD PARTIES PROVIDE.

App	Domain name	IP address	ISP	Origin	Site	Role
MyFitnessPal	z.moatads.com	104.107.144.129	Akamai tech	USA	Greece	Ads
	ads.mopub.com	192.48.236.12	MoPub	USA	USA	
	cdn.branch.io	52.85.158.100	Amazon	USA	Greece	
	api2.branch.io	52.85.158.120	Amazon	USA	Greece	
	aax-eu.amazon-adsystem.com	52.95.123.41	Amazon	USA	Ireland	
	s3.amazonaws.com	52.216.132.85	Amazon	USA	USA	
	api.amplitude.com	35.160.169.182	Amazon	USA	USA	Analyts
	crashlyticsreports-pa.googleapis.com	216.58.212.163	Google	USA	USA	
	api.ua.com	52.85.158.128	Amazon	USA	Greece	API
	config.88-f.net	104.19.161.19	Cloudflare	USA	Canada	
	d34yn14tavczy0.cloudfront.net	52.85.158.22	Amazon	USA	Greece	Photo
	graph.facebook.com	69.171.250.15	Facebook	USA	USA	Social
Strava	app.adjust.com	185.151.204.13	Adjust GmbH	Germany	Netherlands	Analytics
	sessions.bugsnag.com	35.190.88.7	Google	USA	USA	
	firebaseinstallations.googleapis.com	216.58.206.74	Google	USA	USA	API
	api2.branch.io	52.85.158.114	Amazon	USA	Greece	
	api.iterable.com	52.205.72.116	Amazon	USA	USA	
	dgalywyr863hv.cloudfront.net	52.85.155.138	Amazon	USA	Greece	Photo
	graph.facebook.com	31.13.84.8	Facebook	USA	Austria	Social
MapMyRun	ads.mopub.com	192.48.236.12	MoPub	USA	USA	Ads
	hub.samsungapps.com	34.254.23.31	Amazon	USA	Ireland	
	pubads.g.doubleclick.net	216.58.206.34	Google	USA	USA	
	pagead2.googleadservices.com	216.58.209.34	Google	USA	USA	
	cdn.branch.io	52.85.158.100	Amazon	USA	Greece	
	api.amplitude.com	54.203.10.108	Amazon	USA	USA	Analyts
	api2.branch.io	52.85.158.120	Amazon	USA	Greece	API
	graph.facebook.com	31.13.84.8	Facebook	USA	Austria	Social
RunKeeper	id-prod-age.prod.asics.digital	34.197.96.234	Amazon	USA	USA	Ads
	launches.appsflyer.com	18.203.26.15	Amazon	USA	Ireland	Analytics
	api.amplitude.com	52.40.97.110	Amazon	USA	USA	
	crashlyticsreports-pa.googleapis.com	216.58.206.67	Google	USA	USA	
	api.iterable.com	52.55.152.71	Amazon	USA	USA	API
	graph.facebook.com	31.13.84.8	Facebook	USA	Austria	Social
Endomondo	api.amplitude.com	52.40.97.110	Amazon	USA	USA	Analyts
	graph.facebook.com	31.13.84.8	Facebook	USA	Austria	Social
MINDBODY	cdn.branch.io	52.85.158.72	Amazon	USA	Greece	Ads
	mobile-collector.newrelic.com	151.101.2.110	Fastly	USA	USA	Analytics
	identity.mparticle.com	151.101.242.133	Fastly	USA	Italy	API
	sdk.iad-03.braze.com	151.101.17.208	Fastly	USA	USA	
	api2.branch.io	52.85.158.37	Amazon	USA	Greece	
	logx.optimizely.com	52.4.25.221	Amazon	USA	USA	
Weightloss	t.appsflyer.com	79.125.107.112	Amazon	USA	Ireland	Ads
	ads.mopub.com	192.48.236.9	MoPub	USA	USA	
	ads.verv.com	5.9.122.176	Hetzner Online	USA	Germany	
	cb.mopub.com	192.48.236.12	MoPub	USA	USA	
	firebase-settings.crashlytics.com	172.217.16.163	Google	USA	Germany	Analytics
	api.rockmyrun.com	52.89.196.53	Amazon	USA	USA	API
	graph.facebook.com	69.171.250.15	Facebook	USA	USA	Social
	www.facebook.com	69.171.250.35	Facebook	USA	USA	
	api.darksky.net	52.21.90.77	Amazon	USA	USA	Weather
HidrateSpark	reports.crashlytics.com	54.243.164.158	Amazon	USA	USA	Analytics
	graph.facebook.com	69.171.250.15	Facebook	USA	USA	Social
Wokamon	a.appbaqend.com	104.17.72.8	CloudFlare	USA	Canada	Ads
	outcome-ssp.supersonicads.com	52.85.158.20	Amazon	USA	Greece	
	gum.criteo.com	178.250.0.157	Criteo SA	France	France	
	devs.data.mob.com	116.211.155.227	ChinaNET	China	China	Analytics
	api.share.mob.com	118.212.233.191	China Unicom	China	China	API
	graph.facebook.com	69.171.250.15	Facebook	USA	USA	Social
Nudge	cdn.branch.io	52.85.158.64	Amazon	USA	Greece	Ads
	stats.pusher.com	52.90.41.11	Amazon	USA	USA	Analytics
	exp.host	104.197.216.164	Google	USA	USA	API
	d1wp6m56sqw74a.cloudfront.net	52.85.155.179	Amazon	USA	Greece	
	api2.branch.io	52.85.158.37	Amazon	USA	Greece	
	graph.facebook.com	69.171.250.15	Facebook	USA	USA	Social

MyFitnessPal. This app communicates with Facebook, and sends location and phone model information. Same information is sent to the amazon-owned European ad service. To enable personalized advertisement, MyFitnessPal communicates actions taken by users with the deep linking API Branch. It also shares the phone parameters, including the screen resolution, model and OS version. Another third-party API that communicates with MyFitnessPal is Amplitude. It tracks users' actions inside the app. Moreover, it receives information about mobile network operators and whether WiFi is used. The application also utilizes Crashlytics[6], and sends wealth of information about the specifics of the phone (battery level, ram/disk usage, etc.) to Google.

Strava. Similarly to MyFitnessPal, Strava talks to the Branch API, communicating the phone data and location to the third party. Moreover, Strava utilizes error monitoring API Bugsnag. The app shares the screen resolution, and phone info (name, OS version, etc.)

MapMyRun. MapMyRun contacts Branch and amplitude APIs. Both third parties receive the data about the phone that runs the app.

RunKeeper. RunKeeper also communicates with Facebook services regardless whether users connect their accounts with it. Facebook obtains data about the phone and the location for users of RunKeeper. Similar data is shared with the Amplitude tracker. Another tracking API contacted by RunKeeper is Iterable. The API collects the data about the phone, and the email that users used to register in RunKeeper.

Endomondo. Sends the phone and location data to Facebook and the Amplitude API.

MINDBODY. Communicates the phone details, and the SIM carrier (whether WiFi is used) with Branch. Moreover, Mindbody sends the email address to the advertisement provider Mparticle. The app also utilizes the security provider Newrelic. Minbody communicates performance data, including wireless carrier's name and the phone model to this service.

Weightloss. The app shares the phone information, location and sim carrier with Facebook. Weightloss also utilizes Crashlytics: Google receives data about the phone model, battery level, amount of ram and disk space used. Furthermore, Weightloss communicates with the ads provider AppsFlyer. It receives statistics about the usage of the application to provide "customer-centric" service.

HidrateSpark. The app shares private information with Facebook. In particular HidrateSpark sends out the phone name and model. Moreover, the social network receives details about the app usage. That info accounts for the time that the app is running, and time between app sessions. To reduce the number of bugs, HidrateSpark utilizes Crashlytics. A number of various sensitive phone information are sent to Google services as a result. That data include battery level, amount of ram and disk space used, timestamps, and many more.

Wokamon. This app also contacts Facebook without user's consent. Apart from phone info and location, it also shares the gyroscope x, y, z axes data with the social network.

Nudge. Nudge communicates the phone information, location and sim carrier with Facebook. It also shares phone model and Wireless carrier with Branch.

A. Data leaks and third parties

Here we report how many of the studied apps leak data to various companies.

Facebook. 9/10 (90%) of the studied apps share sensitive data with the Facebook social media. These apps allow user to register/sign in with their Facebook profile. It is natural to assume that in that case, the social network will be contacted. However, we established that Facebook is contacted, and the data are shared regardless whether a user is registered in the social media or attempting to sign in with her Facebook credentials. Hence, the social network is able to gather data about customers beyond its userbase. The partner apps mostly contact the `graph.facebook.com` domain - a convenient way for the application to interact with the Facebook social graph. However, sensitive data of users are inevitably shared in the process. In particular, Facebook records every session of each partner app, receiving information about the phone manufacturer, localization, timezone, location (country), Sim carrier, and in some cases even gyroscope parameters.

Crashlytics/Google. Google owns Firebase - a platform for creating Android applications that is contacted by 5/10 applications. In particular, 40% of the studied partner apps contact a crash report service Crashlytics - a subsidiary of Firebase. A very convenient way to troubleshoot applications, Crashlytics collects, analyzes and organizes app crash reports. On the negative side, however, as part of its operation Crashlytics records an unprecedented amount of app-related information. Essentially it records every action that user takes inside the app, and the state of the phone parameters during that step. Such parameters include battery level, battery velocity, presence of proximity, screen orientation, used ram and disk space.

Branch. 5/10 (50%) investigated apps employed a deep linking service Branch. Deep linking enables users to better navigate within the application. However, aside from providing its service the Branch API also send a vast amount of private data to its servers. The collected

[6]Crashlytics - the crash reporter from Google. https://firebase.google.com/docs/crashlytics

data include the phone model and manufacturer, screen dpi and resolution, OS version and architecture, install and update time.

V. Discussion

Most of the studied applications are shipped with a privacy policy. However, it appears that many of the policies are vaguely written, and enable third parties to collect any type of sensitive information that can be retrieved from users. Clients are mandated to accept user agreements in order to use partner applications. Once that is done, users lose control over their own data. An ability to link multiple identities to a single user characterizes a so-called "permanent record". Third parties that have not been granted an explicit permission from users to collect and permanently store their data are able to access and process sensitive data of people who own fitness trackers. Even if the shared data alone do not seem to be of utmost importance, the fact that information is collected from every client of these partner apps should be quite concerning for privacy-conscious consumers. An average number of downloads for the studied apps is around $10,000,000$. The same number for the official Fitbit app is 50 million. If a third party has access to the fifth of Fitbit's userbase, the scale of mass profiling that it can launch is immense. In practice, not every user of a partner app links her Fitbit account. Nevertheless, the number of affected users is concerning. Andrade et al. found that users are more likely to grant access to their personal data to the companies with a credible reputation [15]. Since Fitbit is universally accepted as the company that greatly cares about privacy, it is likely that its credibility would "convey" to the affiliated apps as well.

Despite most of the popular third-party companies offer their service free of charge, the real price that the partner apps pay is the data of their users. That is, partner apps utilize the data of their users to "pay" for the convenience and service. Hence, it is an individual user who contributes data to fund a better application experience.

VI. Conclusion

It appears that many Fitbit partner apps utilize a number of various third-party services. Applications employ advertisement providers to boost revenues; APIs and tracking services to enhance the experience of users. A number of apps that allow sign up using Facebook credentials do also contact the social network API. However, Facebook is also contacted even for clients who choose to log in with different methods. Even though we were not able to detect health data being shared with third parties during the runtime, the application still communicates a wealth of other personal information to the "unexpected" third parties. The majority of the studied apps are shipped with a privacy policy that identifies what data can be shared with third parties. On the negative side, however, in most cases any private information is listed in the "shareable" category. This enables partner apps to collect and share all possible personal data without fearing legal prosecution.

We urge owners of wearable devices to rigorously investigate privacy policies of the partner services they are planning to use.

References

[1] A. Hilts, C. Parsons, J. Knockel, Every step you fake: A comparative analysis of fitness tracker privacy and security, Open Effect Report.Available at: https://openeffect.ca/reports/Every_Step_You_Fake.pdf (2016).

[2] K. Ball, M. Di Domenico, D. Nunan, Big data surveillance and the body-subject, Body & Society 22 (2) (2016) 58–81.

[3] J. Vitak, Y. Liao, P. Kumar, M. Zimmer, K. Kritikos, Privacy attitudes and data valuation among fitness tracker users, in: International Conference on Information, Springer, 2018, pp. 229–239.

[4] A. Raij, A. Ghosh, S. Kumar, M. Srivastava, 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, 2011, pp. 11–20.

[5] S. R. Peppet, Regulating the internet of things: first steps toward managing discrimination, privacy, security and consent, Tex. L. Rev. 93 (2014) 85.

[6] K. Crawford, J. Lingel, T. Karppi, 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.

[7] D. B. Meinert, D. K. Peterson, J. R. Criswell, M. D. Crossland, Privacy policy statements and consumer willingness to provide personal information, Journal of Electronic Commerce in Organizations (JECO) 4 (1) (2006) 1–17.

[8] A. Acquisti, J. Grossklags, Privacy and rationality in individual decision making, IEEE security & privacy 3 (1) (2005) 26–33.

[9] N. Steinfeld, "i agree to the terms and conditions":(how) do users read privacy policies online? an eye-tracking experiment, Computers in human behavior 55 (2016) 992–1000.

[10] R. Balebako, R. Shay, L. F. Cranor, Is your inseam a biometric? evaluating the understandability of mobile privacy notice categories, CMU, Tech. Rep. CMU-CyLab-13-011 (2013).

[11] Z. Al-Makhadmeh, A. Tolba, Utilizing iot wearable medical device for heart disease prediction using higher order boltzmann model: A classification approach, Measurement 147 (2019) 106815.

[12] B. Muthu, C. Sivaparthipan, G. Manogaran, R. Sundarasekar, S. Kadry, A. Shanthini, A. Dasel, Iot based wearable sensor for diseases prediction and symptom analysis in healthcare sector, Peer-to-peer networking and applications 13 (6) (2020) 2123–2134.

[13] A. Sathyanarayana, S. Joty, L. Fernandez-Luque, F. Ofli, J. Srivastava, A. Elmagarmid, T. Arora, S. Taheri, Sleep quality prediction from wearable data using deep learning, JMIR mHealth and uHealth 4 (4) (2016) e125.

[14] G. Zhu, J. Li, Z. Meng, Y. Yu, Y. Li, X. Tang, Y. Dong, G. Sun, R. Zhou, H. Wang, et al., Learning from large-scale wearable device data for predicting epidemics trend of covid-19, Discrete Dynamics in Nature and Society 2020 (2020).

[15] E. B. Andrade, V. Kaltcheva, B. Weitz, Self-disclosure on the web: The impact of privacy policy, reward, and company reputation, ACR North American Advances (2002).