IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received November 30, 2017, accepted January 16, 2018, date of publication January 29, 2018, date of current version March 13, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2799522

Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice

ACHILLEAS PAPAGEORGIOU[1], (Member, IEEE), MICHAEL STRIGKOS[1], EUGENIA POLITOU[1], (Member, IEEE), EFTHIMIOS ALEPIS[1], (Member, IEEE), AGUSTI SOLANAS[2], (Senior Member, IEEE), AND CONSTANTINOS PATSAKIS[1], (Member, IEEE)

[1]Department of Informatics, University of Piraeus, 18534 Pireas, Greece
[2]Department of Computer Engineering and Mathematics, Rovira i Virgili University, 43003 Tarragona, Spain

Corresponding author: Constantinos Patsakis (kpatsak@gmail.com)

This work was supported by the European Commission under the Horizon 2020 Programme (H2020), as part of the OPERANDO project (Grant Agreement no. 653704) and the CRYPTACUS COST action (COST Action IC1403).

ABSTRACT Recent advances in hardware and telecommunications have enabled the development of low cost mobile devices equipped with a variety of sensors. As a result, new functionalities, empowered by emerging mobile platforms, allow millions of applications to take advantage of vast amounts of data. Following this trend, mobile health applications collect users health-related information to help them better comprehend their health status and to promote their overall wellbeing. Nevertheless, health-related information is by nature and by law deemed sensitive and, therefore, its adequate protection is of substantial importance. In this paper we provide an in-depth security and privacy analysis of some of the most popular freeware mobile health applications. We have performed both static and dynamic analysis of selected mobile health applications, along with tailored testing of each application's functionalities. Long term analyses of the life cycle of the reviewed apps and our general data protection regulation compliance auditing procedure are unique features of the present paper. Our findings reveal that the majority of the analyzed applications do not follow well-known practices and guidelines, not even legal restrictions imposed by contemporary data protection regulations, thus jeopardizing the privacy of millions of users.

INDEX TERMS Communication system security, mobile security, application security, data privacy.

I. INTRODUCTION

The generalization of smartphones has radically changed our interaction with mobile devices and the information we exchange. This shift has been amplified by the existence of numerous embedded sensors harnessed by developers to provide their apps with context-aware capabilities. In the medical domain particularly, there is a noticeable growth of health-related apps offering intelligent tools and services to support healthcare interventions according to the users' condition. In practice, these apps deal with implicit or explicit data originating from both users and their environment. Sophisticated mobile health (m-health) apps are able to sense changes in environmental and human body measurements in order to assess users' health and to generate alerts relevant to their condition. Moreover, due to smartphones advanced processing capabilities, most apps often store and process not only health-related data but other sensitive information as well, such as user's location, lists of contacts and personal photographs.

Even though enforcing security and privacy requirements in mobile apps is admittedly not an easily achievable task [1], when sensitive data are at stake one would expect m-health applications to follow well-known security and privacy guidelines and legally binding data protection provisions to guarantee data privacy and safety. However, many popular apps (not only m-health apps), which process sensitive data often fail to provide even basic protection to users' privacy due to either inappropriate implementations or poor design choices [2]–[6].

In this article we investigate user's privacy exposure in m-health apps that, as they handle sensitive personal data, are expected to be equipped with data protection mechanisms. Due to the Android's Operating System (OS) popularity, we decided to test Android apps retrieved from Google Play. We have selected the apps according to quality, popularity and content-related criteria. Furthermore, we have studied the spread of users' personal data and, mainly, the final parties receiving these data. In our in-depth analysis we have evaluated 20 popular m-health apps in terms of their provided data security and privacy. We have come to the alarming conclusion that the majority of the analyzed apps does not meet the expected standards for security and privacy, thus endangering their users' sensitive personal data.

Our study is innovative and has unique features with respect to previous articles in this area. We provide an analysis of security and privacy concerns in m-health apps through long term evaluation, monitoring and recording of the full life cycle of the apps (from January 2016 to August 2017), assessing the quality of all communication channels. Moreover, we investigate the way that app developers responded to the security reports we submitted them. Finally, we perform a GDPR compliance auditing procedure to determine whether the reviewed apps conform to the new EU legal requirements.

The rest of the article is structured as follows: First, in §II we provide the reader with background information and related work in the field of m-health security and privacy. Next, in §III we describe and justify our data collection and assessment methodologies. Further, in §IV we report and analyze the results of our research. Finally, the paper concludes in §V by briefly discussing the impact of our findings and by pointing out some of the necessary mitigation strategies. For the sake of completeness we include some explanations on personal data protection terminology in Appendix.

II. BACKGROUND AND RELATED WORK

Over the last few years we have witnessed a mobile computing outburst and its progressive adoption in people's daily activities. A whole new software market of mobile apps is flourishing with each mobile OS vendor willing to have its own independent marketplace. Undoubtedly, one of the most popular software categories within these on-line stores is that of "health and well-being" and, developers and publishers are increasingly populating the m-health apps market [7].

There is an emerging shift towards the "connected health" model [8], where the goal is to achieve flexible, effective and affordable healthcare services by following the notion of the context-aware smart health (s-health) paradigm [9]. In this technological context, while many devices share common OS platforms, mobile apps are frequently considered to be part of the IoT ecosystem [10], [11] and, hence, they may potentially suffer from similar shortcomings. Yet, a growing number of healthcare professionals are shifting towards the use of mobile apps to better communicate with and manage the health information of their patients. Convenience, better clinical decision making, improved accuracy, increased efficiency and enhanced productivity [12] are some of the benefits that mobile apps provide to health professionals. As a result, there is an increased interest for mobile accessible Personal Health Records (mPHRs) that allow healthcare providers to better share information with patients [13].

This noticeable growth of the m-health market, nonetheless, comes along with a growing concern for the security and privacy readiness of mobile devices (*e.g.*, smartphones, wearables) and their installed apps. A report of the European Commission about citizens' data protection within the 28 EU Members States [14] affirms that over half of the respondents in 16 of the surveyed countries stated that they were concerned about the recording of their everyday activities via mobile phone use or mobile applications. Responding to people's worries about the inadequate and fuzzy protection of their personal data in the era of ubiquitous computing, the European Commission adopted in 2016 a new stringent legal framework for protecting individuals' personal data, the General Data Protection Regulation (GDPR) [15] which will replace the existing 1995's Data Protection Directive [16] and will become directly applicable to all EU Member States on May 2018, harmonizing thus the various national regulations across the EU. The GDPR enforces new legal requirements to data controllers operating within the EU territory and foresees severe sanctions for compliance failure to its provisions regarding personal, and specially sensitive, data protection. Although, the regulation provoked prolonged controversy and intense discussions regarding its applicability in the age of big data and the IoT [17], it anticipates for some radical changes in the data protection regime - among others, the introduction of pseudonymisation and the data portability right.

Yet, concerns about m-health applications are not restricted within the EU domain. On the other side of the Atlantic for instance, there is a lot of skepticism about the applicability of the national US standards of Health Insurance Portability and Accountability Act (HIPAA) that defines policies, procedures and guidelines for maintaining the privacy and security of individually identifiable health information. Notably, some scholars argue that m-health apps fail to be aligned with the regulatory protection of the HIPAA [18].

The fast growing market of m-health apps fostered an emerging interest in studying the security and privacy impact on users. In [19] 20 apps (both Android and iOS) were evaluated in terms of their security by identifying possible risks and desirable features, based on eight analysis criteria, with the aim to assist users in selecting m-health apps. In [20] an m-health threat analysis comprising possible attack scenarios was presented. The analysis, which revealed the security and privacy vulnerabilities of 154 selected diabetes and hypertension apps, was based on four axes: a static analysis applied to all apps, a dynamic analysis applied only to the 72 most frequently downloaded, an assessment of web server's security and, a privacy policy inspection applied to 20 of the selected apps. Additionally, in [21] Knorr *et al.* summarized their findings for the top 20 downloaded apps with a score based on the identified privacy and security issues.

Similarly, a report regarding the security and privacy issues of 43 health and fitness apps, both for iOS and Android, was presented in [22]. The researchers found that 40% of the apps imply high risk to user's privacy, 32% of the apps imply a medium to high risk, 28% of the apps low to medium risk whereas none of the apps was found with no risks at all. Three main technical causes of privacy risks in mobile health and fitness apps were identified: unencrypted traffic, embedded advertisements and third-party analytics services. In another article [18], He *et al.* classified 160 m-health apps offered by Google Play to formulate a list of seven attack surfaces that need to be taken into consideration when evaluating apps' security and privacy status: the Internet, third party services, Bluetooth, logging, SD card storage, exported components and side channels. Random samples of additional apps were tested and analyzed with respect to these seven attack surfaces, and in particular to the Internet and the third party services. According to the results, 63.6% of the sampled apps were sending unencrypted data over the Internet and 81.8% were using third party storage and hosting services such as the Amazon's cloud services. Another study [23] assessed the extent to which certified m-health apps were compliant with the data protection principles mandated by the UK NHS Health Apps Library. The analysis performed on a list of 79 apps, certified by the UK NHS as clinically safe and trustworthy, showed systematic gaps in compliance with data protection principles, revealing thus security and privacy issues.

A review of 24,405 health-related apps, both for iOS (21,953) and Android (2,452) devices, was presented in [24]. The apps have been assessed in terms of security and privacy implications based on their access to medical or other sensitive user information, their potential damage through information leaks, information manipulation or information loss, and their access to information valuable to third parties. Since the installation and testing of all the apps under review was practically infeasible, the researchers focused on the applications' information provided by the online stores. After filtering and clustering the original sample, the results showed that 95.63% of the apps pose at least some potential damage through information security and privacy infringements, whereas 11.67% of them estimated to impose the highest potential damages.

The above studies illustrate the major concerns arising from the way each m-health app collects, manages and/or shares user's private information. For instance, there will always be a matter of trust when an app collects more information than is needed to provide its services, thereby violating the data minimization and purpose limitation principles specified in all contemporary data protection regulations. In terms of their secure connectivity, today it is more than usual for users to interact with their apps on a not fully trusted network, *i.e.* at a shop or a restaurant, and therefore information leakages cannot be physically constrained to specific networks.

The work that we present in this article is an extension of the above referenced articles concerning the security and privacy assessment of m-health apps available in on-line marketplaces. In this respect, we investigate the privacy and security risks in the 20 most popular m-health apps by focusing in the area of privacy and personal data protection when sharing sensitive health information with third party entities. By evaluating how the apps request, handle and disseminate the sensitive personal information we can ultimately assess the required countermeasures for protecting it.

TABLE 1. Inclusion criteria.

Criterion 1	The app must be free.
Criterion 2	The app's content must be in English.
Criterion 3	The app must require health and/or personal data input in order to be functional and based on its description is expected to transmit the users´ data to a remote host.
Criterion 4	The app must have at least 100.000 downloads and a minimum rating of 3.5/5 stars on Google Play.

III. OUR METHODOLOGY

In this section we firstly present our apps collection criteria and secondly the assessment methodology being followed for investigating the security and privacy features offered by each app. The initial tests were performed from January to February 2016 by using Android devices and apps downloaded from the official Android marketplace (*i.e.,* Google Play). A year later, and after notifying each app's vendor on the initially identified issues, we ran a re-evaluation process from July to August 2017, based on dynamic analysis tests, in order to verify any conformance to the previously discovered findings.

In addition to provide a bug/findings report, we performed a GDPR compliance auditing procedure to determine whether the reviewed apps conform to the new legal requirements.

A. COLLECTION METHODOLOGY

With the aim to perform an initial screening of possible candidate applications, we collected a set of 1080 of the most popular apps from the "Medical" and "Health and Fitness" sections of Google Play. We analyzed the scope and features of each app (one by one) and, as a result, many were discarded because they did not allow any monitoring or recording of users' biomedical data. Moreover, another large number of apps from the "Health and Fitness" category was also excluded because they only provided fitness-related functionalities, whereas in our research we have decided to focus on apps that provide m-health managing functionalities regarding health conditions or specific medical diseases.

To identify, collect and evaluate a manageable number of m-health apps that provide users with metrics and interventions according to their inputs, we have determined the inclusion criteria shown in Table 1. By applying the aforementioned inclusion criteria we ended up selecting 20 apps, which can be categorized into three major areas: (i) pregnancy and baby growth, (ii) personal/family members' health agenda and symptoms assistants/checkers, (iii) blood pressure and diabetes support. Due to legal issues we cannot disclose the names (or other identifiers) of the analyzed apps. Hence, we refer to them as *App. I, App. II, . . . App. XX*. The number of downloads (up to 01/2016) of those apps are shown in Table 2.

B. ASSESSMENT METHODOLOGY

The methodology adopted for assessing the 20 collected m-health apps aims at answering the following three main research questions:

TABLE 2. Number of downloads of the analyzed applications.

Downloads	App. Number
100.000 - 500.000	II - IV - V - VI - X - XX
500.000 - 1.000.000	IX - XVI - XVII
1.000.000 - 5.000.000	I - III - VII - VIII - XII - XIII - XIV - XVIII - XIX
5.000.000 - 10.000.000	XI - XV

- Which parties have access to personal data from the app?
- What exact data can each party access?
- How safe is each communication channel?

In order to be able to provide meaningful answers to these questions, we followed the eight steps below:

1) The first and foremost step was to register the needed personas in each app. To this end, we created fake emails and/or Facebook accounts that would allow for each app a user account to be created. Moreover, we carefully read the scope and objectives of each app to accurately emulate a typical user's behavior.
2) After installing each application, we collected its permissions and inspected its privacy policies, if they existed on Google Play, something that became mandatory since the early 2017 by Google for the apps that request or handle sensitive user or device information.
3) This step involved automated static code analysis. To achieve this, we analyzed the APK of each app using MobSF (http://opensecurity.in/mobile-security-framework/) to detect possible vulnerabilities. Despite the fact that some of the reported issues might be considered trivial or false alarms (*e.g.,* reports regarding the use of randomness libraries) most identified issues are rather important and they are presented in scale analysis under the corresponding section.
4) In this step we performed dynamic analysis for each app using *Fiddler* (https://www.telerik.com/fiddler), a well-known web debugging proxy set up. Every app was installed and tested in a cleanroom environment to achieve the most accurate results of each app's behavior during its dynamic analysis. Moreover, we studied and manually analyzed every single communication between each app and third parties. This was achieved by intercepting all communications as illustrated in Figure 1. Additionally, we documented all the domains that the apps were communicating with and we examined their ownership status and their regulating authority. For each captured communication, we listed the type of transmitted data and we analyzed the kind of each data exchange request in terms of its encryption (*plaintext* vs *ciphertext*) and its method (*e.g.,* GET vs POST) in order to evaluate the potential risk of exposure.
5) Once the communication channels were determined, we analyzed the web server configuration to assess the security level of the HTTPS data transmission. To accomplish this, we used a well-known free on-line service *SSL Labs* (https://www.ssllabs.com/ssltest/) from Qualys that enables the remote testing of web server's security against a number of well-known vulnerabilities, such as *Heartbleed* or *Drown*.
6) Having an overview of the quality of each communication channel from the previous steps, we inspected each packet to determine the contents exchanged in each message. This step was essential to identify and evaluate whether the exchanged information was necessary for the intended application purpose, and what kind of data third parties may have access to.
7) In this step we summarized our findings for each app vendor and we informed them accordingly, keeping track of each response in reference to its content, response time and attitude towards changes.
8) Finally, based on the legal demand needs for compliance with the upcoming GDPR regulation, we performed a number of checks in order to estimate each apps' readiness against the GDPR's requirements.

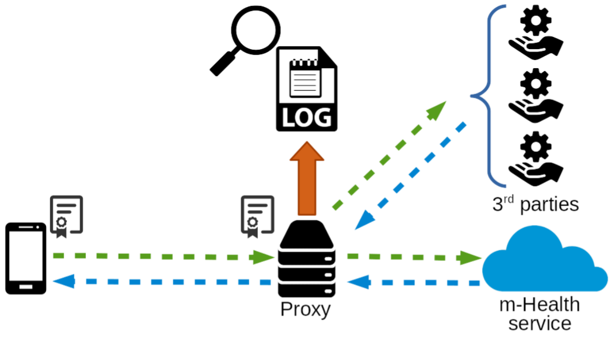


FIGURE 1. Scheme of the interception setup.

Based on the aforementioned steps, we hereafter present our findings and analyze several patterns in terms of coding style and development process. Our ultimate goal, in addition to improving the security and privacy features of the m-health apps under review by providing their developers with extended feedback on their shortcomings, is to highlight common pitfalls in the application development life-cycle that may jeopardize the privacy rights of millions of users.

IV. RESULTS

Based on the aforementioned methodology, the experiments were carried out accordingly for all the 20 m-health apps under evaluation. Before reporting the results of the static and dynamic analysis for each app, we discuss the results of their manual analysis, which covers the inspection of their privacy policies and permission requests.

A. MANUAL ANALYSIS

1) PRIVACY POLICIES

Prior to our initial experiments, Google had not taken any action against the amount of apps not providing valid privacy policies, even though they are handling sensitive information. In fact, our initial results on February 2016 showed that 10% of the analyzed apps didn't have any reference to a

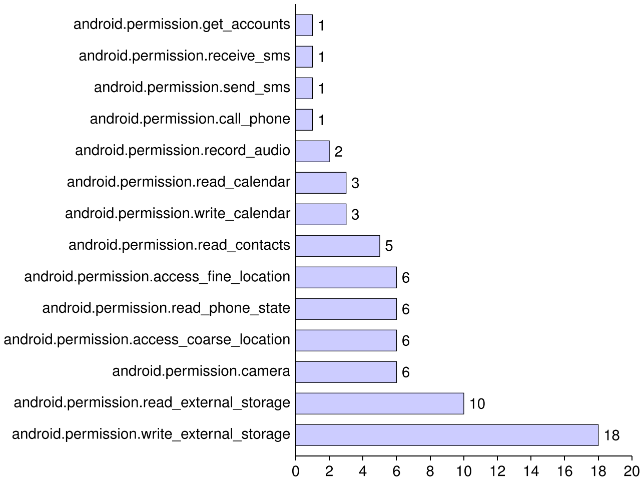


FIGURE 2. Summary of dangerous permission requests.

TABLE 3. Results of the static code analysis.

Code Analysis	Percentage
The App logs information. Sensitive information should never be logged.	100
The App uses an insecure Random Number Generator.	95
Files may contain hardcoded sensitive informations like user names, passwords, keys etc.	85
App uses SQLite Database. Sensitive Information should be encrypted.	85
App can read/write to External Storage. Any App can read data written to External Storage.	85
This App may have root detection capabilities.	45
Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	30
Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole.	30
Insecure WebView Implementation. WebView ignores SSL Certificate Errors.	15
Remote WebView debugging is enabled.	10

privacy policy page whereas 5% of the apps had a link to a URL that claimed to host their application privacy policy but responded with a 404 error page. Finally, 5% of the apps had a link to a privacy policy page that wasn't translated into English, even though the contents of the application were. Furthermore, some of the apps under review did provide some kind of privacy policy, albeit of dubious validity since the quality and the relevance of their policy were not up to the required ones for protecting users from privacy issues, such as malicious or unintentionally data leakage. In compliance with [21] and [25], we have also found that the problem of missing or invalid privacy policies mainly affects the less popular apps. However, the mindset of the development community towards this practice has been arguably shifting due to the recent Google's reaction (*i.e.,* since the early 2017 Google has sent notifications to developers for not providing a valid privacy policy). Yet, an updated study on the existence, relevance, quality and overall validity of the provided privacy policies by the apps is deemed necessary.

2) PERMISSIONS ANALYSIS

To analyze the permission requests of the apps under examination, we collected the permissions listed in the *Manifest* files of the apps´ APKs using python scripts. Based on the dangerousness of the permissions [26], permissions in Android could be divided into "normal" and "dangerous". Figure 2 summarizes the requested dangerous permissions and the number of apps that did so. Upon closer examination of the results, several findings stand out as they imply other parallel usage, beyond applications' scope. For instance, while only two apps required access to the microphone, one more was also requesting it without any obvious reason. While none of the apps in the study required any Bluetooth functionality or connectivity to a paired device, oddly, two applications requested this permission. To the best of our understanding, this permission was requested to fulfill the requirements of ad libraries which exploit Bluetooth devices to track user's location [27], [28]. Notably, Google since *Marshmallow* required apps that performed scanning for hardware identifiers, like via WiFi or Bluetooth, to request the location permission, leaving out though other indirect approaches for obtaining location information [29]. Nonetheless, six of the studied apps requested permissions to access location and coarse location.

While only one app needed access to the calendar, two more asked for it and five requested access to the contacts list (*i.e.,* another well-known ad library tactic). One application requested access to SMS in order to both read and write, while another requested access to dial phone numbers. Remarkably, none of these apps exhibited any functionality justifying such requests. Almost all apps requested access to the devices' external storage, a permission not adequately justified since developers, instead of arbitrary accessing the storage, may use intents to get stored photos from the gallery or take a new photo for the user's profile. Last but not least, six of the apps requested access to the camera, again an action that could be avoided, through proper Android intents utilization.

B. STATIC CODE ANALYSIS

To evaluate the security of the apps in detail, we examined each APK independently using MobSF. The analysis of the tested APKs revealed several security issues summarized in Table 3. While some of these issues, such as the use of insecure random number generators, appear quite often, they are not all qualified as significant since, most of the times, the use of random number generators is not necessarily related to security or privacy violations. On the contrary, MobSF showed that many apps do not connect using HTTPS and have several issues concerning Android WebViews components. MobSF also revealed that 45% of the apps tried to determine whether the device was rooted – a feature irrelevant to their goals.

C. DYNAMIC ANALYSIS

In our dynamic analysis, we evaluated the apps in terms of their security and privacy attributes when they transmit sensitive and personal data over the Internet. Next, we

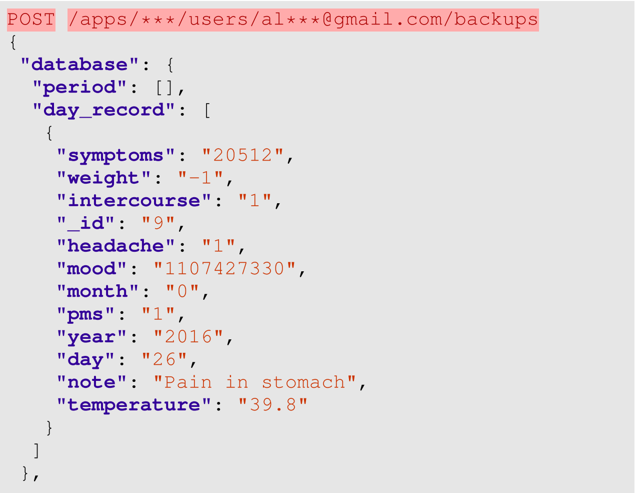
TABLE 4. Health data transmission.

App No.	Sent to Vendor	Sent to Vendor over HTTP	Share data with third party	# 3rd party domains	# 3rd party domains over HTTP
App. I	✓			0	0
App. II	✓	✓	✓	1	1
App. III	✓	✓		0	0
App. IV			✓	1	0
App. V	✓	✓	✓	1	1
App. VII	✓			0	0
App. IX	✓			0	0
App. X	✓	✓		0	0
App. XII			✓	1	0
App. XIII	✓			0	0
App. XV			✓	2	1
App. XVI	✓			0	0
App. XVII			✓	1	1
App. XVIII	✓			0	0
App. XIX	✓	✓	✓	1	1
App. XX	✓	✓	✓	1	1

discussed our findings grouped according to the kind of data that apps transmitted, namely health-related data, multimedia, location information, registration and log-in data, e-mails, devices Id., search queries, OS information, and chat sessions.

1) HEALTH-RELATED DATA

In order to identify the transmitted health information while the user interacts with the app, we captured all keywords and/or phrases related to the health status or the medical condition of the user by using the Fiddler web debugging tool. Our experiments showed that 80% of the analyzed apps transmit users' health-related data, while 20% store them locally on the device. In terms of security, only 50% of those apps transmit health-related data over HTTPS connections for all of their communication. Table 4 summarizes our findings. The second column *"Sent to Vendor"* displays whether the app sends the collected health-related data to the vendor's domain, while the third column *"Sent to vendor over HTTP"* specifies which of the apps that sent health-related data to the vendor's domain did so over HTTP. The fourth column *"Share data with third party"* indicates whether the app shares health-related data with a third party domain, whereas the fifth column *"# 3rd party domains"* reflects the number of third party domains to which the app sends data. Finally, the sixth column *"# 3rd party domains over HTTP"* displays the number of third party domains that receive health-related data over HTTP. Figure 3 shows an example of a JSON response to a POST request over HTTP of one of the tested apps, resulting from us using the appś back-up function in order to send data to our email address. It can be observed that 50% of the apps send data to third parties. These third parties can be classified into two main categories: i. Marketing related platforms that provide mobile analytics or performance related data, and ii. Cloud based back-end solutions used to configure applications' functionalities. Oddly enough, one app was found to sent health-related data to an IP for which it wasn't possible to identify any authority based on on-line resources. Finally, from the apps transmitting data to remote hosts, 7 of them transmit health-related data to their vendors using GET requests, whereas 4 send information to third parties using GET requests. All these apps transfer their users' health data through URLs. Practically, this means that identifiers and sensitive users' data are open to everyone having access to the URLs. In the plain HTTP case, the threats are obvious and independent of GET/POST requests. However, even if HTTPS is used, the data is stored in the log files of the web server, which can potentially expose this data to unauthorized entities.



```
POST /apps/***/users/al***@gmail.com/backups
{
 "database": {
  "period": [],
  "day_record": [
   {
    "symptoms": "20512",
    "weight": "-1",
    "intercourse": "1",
    "_id": "9",
    "headache": "1",
    "mood": "1107427330",
    "month": "0",
    "pms": "1",
    "year": "2016",
    "day": "26",
    "note": "Pain in stomach",
    "temperature": "39.8"
   }
  ]
 },
```

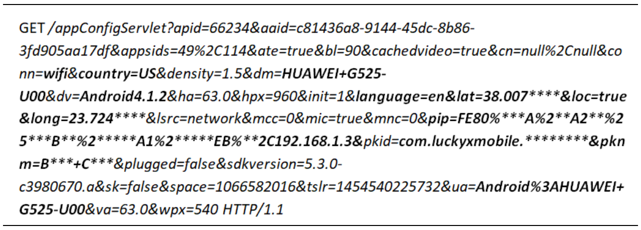
FIGURE 3. Part of a JSON response to a POST request over HTTP containing health-related data.

2) MULTIMEDIA DATA TRANSMISSION

Multimedia content in the m-health apps could be classified into the following categories: i. multimedia content the app needs in order to be functional and aesthetically pleasing to the user, ii. multimedia content a user submits in the process of creating his/her account, *e.g.,* his/her photo, and iii. multimedia content the app requests for health related purposes, *e.g.,* scans of x-rays images. Although in the first case a possible transmission seems innocent, as personal data are not involved, still an eavesdropper can very easily monitor the content and reach conclusions about the nature and the scope of each app a user installs or uses. In the second and third cases, however, the data under process concern sensitive personal data. Our experiments showed that a number of apps, in addition to the transmission of text data over the network, disseminate user submitted multimedia files closely related to his/her health condition without always providing the necessary protection security mechanisms. Also, the majority of these apps do not transmit their core multimedia content over the HTTPS. More precisely, 20% of the apps ask users to submit personal photos (from categories ii and iii). Only half of those send health-related multimedia content over HTTPS for all of their transmissions, whereas most of the spread multimedia content (N = 3) was transferred to third

TABLE 5. User's location transmittion.

App No.	Sent to Vendor	Sent to Vendor over HTTP	Share data with third party	# 3rd party domains	# 3rd party domains over HTTP
App. I	✓		✓	1	0
App. II	✓	✓	✓	1	0
App. VII	✓			0	0
App. VIII			✓	2	2
App. XVII			✓	1	1
App. XVIII	✓			0	0
App. XIX	✓	✓		0	0



```
GET /appConfigServlet?apid=66234&aaid=c81436a8-9144-45dc-8b86-
3fd905aa17df&appsids=49%2C114&ate=true&bl=90&cachedvideo=true&cn=null%2Cnull&co
nn=wifi&country=US&density=1.5&dm=HUAWEI+G525-
U00&dv=Android4.1.2&ha=63.0&hpx=960&init=1&language=en&lat=38.007****&loc=true
&long=23.724****&lsrc=network&mcc=0&mic=true&mnc=0&pip=FE80%***A%2**A2**%2
5***B**%2*****A1%2*****EB%**2C192.168.1.3&pkid=com.luckyxmobile.********&pkn
m=B***+C***&plugged=false&sdkversion=5.3.0-
c3980670.a&sk=false&space=1066582016&tslr=1454540225732&ua=Android%3AHUAWEI+
G525-U00&va=63.0&wpx=540 HTTP/1.1
```

FIGURE 4. Location transmission via a GET request over HTTP to an Ad service.

parties' cloud-based solutions. Moreover, most multimedia links provided by the apps were static links, which is a major privacy issue [30].

3) LOCATION PRIVACY

Seven of the analyzed apps requested and transmitted location information, that under certain data protection regulations is considered, not only personal, but sensitive as well. The findings about transmitted users' location information are shown in Table 5. More precisely, 35% of the apps transmitted users' geolocation information or their postal address either to their vendors or to third parties. Moreover, 4 of the assessed apps send their users' location to 5 distinct third party domains, while 3 of them are doing so over HTTP. Furthermore, our analysis showed that 5 out of the 7 apps that transmit users' location ask for it with a GET request. Especially, one of the apps, although did not offer any special geolocation service to its users, two of its third party ad services asked for users geolocation at a rate of almost one request every 3 seconds within a timeframe of approximately 12 minutes. Apart from draining the battery, the app transmitted the user's location to third party domains over HTTP connections via GET requests. Figure 4 shows an example of a GET request that leaked location information (latitude, longitude) over HTTP. Additional identifiable information was also leaked in the same request (*i.e.*, mobile device model, OS, device version, local IPv6 Aaddress).

4) USER'S REGISTRATION AND LOG IN SECURITY

Many of the m-health apps required a profile to be created and, in many cases, a password as well. We focused on examining each app's registration and login security. Therefore, we captured the registration process and we repeatedly tested the login procedure of each app in order to check: whether the app transfers its user login data over the HTTP, and whether the app requests user login data via GET requests. The outcome of this analysis revealed that 55% of the apps asked for and transmited users' passwords, while 27% of those do not use a secure connection (HTTPS) for its dissemination. Also, 45% of the apps that transmit users' passwords used GET requests, which is not considered a good practice in terms of security.

5) EMAIL AND DEVICE ID TRANSMISSION

According to our tests, while 75% of the apps transmit user email addresses to at least one of their connected domains, 33% of those apps use an insecure connection for this transmission to at least one of their connected domains, and 60% of those apps share users' emails addresses with third parties. Moreover, one of these apps transmits user's email address to an unknown IP whose owner couldn't be identified.

Regarding device identifiers, we searched for unique IDs related to the device used in our experiments. More specifically, we searched for the IMEI, the GSF ID and the Secure ID and, we found that 45% of the apps transmit at least one of the device's unique IDs to at least one of their connected domains. Yet, only 44% of these apps make use of HTTPS. Based on our experimental results, we observe that each time a domain requests one of the GSF ID or the IMEI, the app sends also the Secure ID. Further, 89% of these apps shared their users' device Secure ID with third parties. Thus, by snooping and uniquely binding the device unique ID to an individual, users' sensitive health data privacy may be compromised.

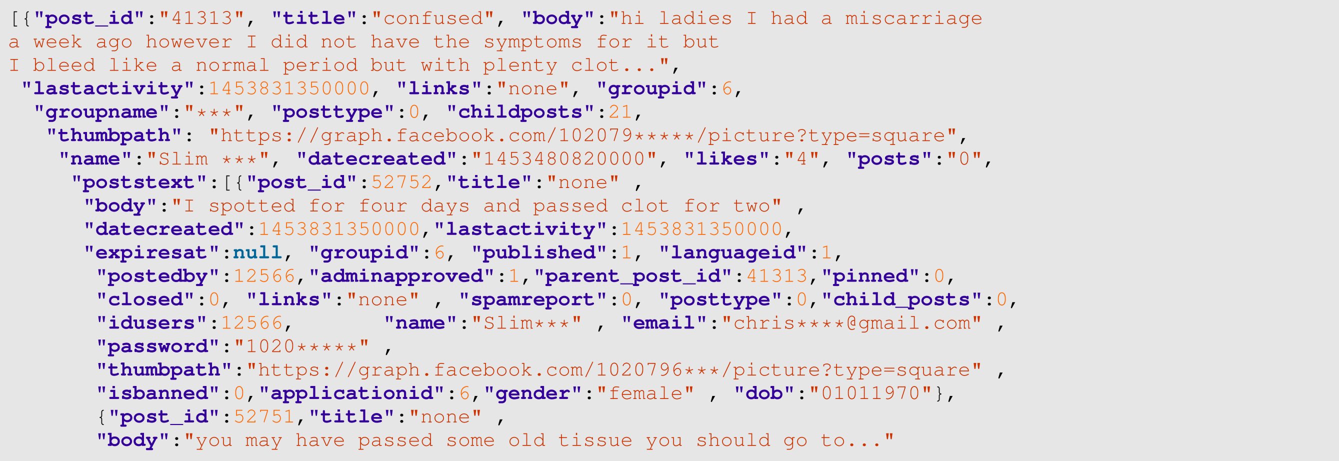
6) USERS' SEARCH QUERY PRIVACY AND OS TYPE

Based on our findings, 25% of the apps are found to transmit users' search queries over the network, but only 20% of these apps use a secure connection (HTTPS) when doing so. While all the apps transmitting search queries send them to their vendor's domain, 80% of them send this information to third parties as well, and two apps send their users' queries to 16 different third party domains. The most dangerous behavior, though, is that all of these apps are found to transmit users' search queries by using the GET request. As expected, it is more than easy for an eavesdropper to collect this information and infer user's health condition.

Moreover, our examination revealed that the information of the OS type was transmitted at least once to at least one domain per app and at least one of the connections was insecure. As a result, an eavesdropper could easily figure out whether a user makes use of an Android device and, in most of the cases, the version of the device software. This could lead to privacy issues when a user makes use of an app, *e.g.*, within a specific place or area, because an eavesdropper having access to the same area can easily match the logs of his activity with the user.

7) CHAT SESSIONS TRANSMISSION

Chats are not very common within the analyzed m-health apps. Nevertheless, we had the opportunity to test two apps



```
[{"post_id":"41313", "title":"confused", "body":"hi ladies I had a miscarriage
a week ago however I did not have the symptoms for it but
I bleed like a normal period but with plenty clot...",
 "lastactivity":1453831350000, "links":"none", "groupid":6,
  "groupname":"***", "posttype":0, "childposts":21,
   "thumbpath": "https://graph.facebook.com/102079*****/picture?type=square",
    "name":"Slim ***", "datecreated":"1453480820000", "likes":"4", "posts":"0",
     "poststext":[{"post_id":52752,"title":"none" ,
      "body":"I spotted for four days and passed clot for two" ,
      "datecreated":1453831350000,"lastactivity":1453831350000,
      "expiresat":null, "groupid":6, "published":1, "languageid":1,
       "postedby":12566,"adminapproved":1,"parent_post_id":41313,"pinned":0,
       "closed":0, "links":"none" , "spamreport":0, "posttype":0,"child_posts":0,
       "idusers":12566,       "name":"Slim***" , "email":"chris****@gmail.com" ,
       "password":"1020*****" ,
       "thumbpath":"https://graph.facebook.com/1020796***/picture?type=square" ,
       "isbanned":0,"applicationid":6,"gender":"female" , "dob":"01011970"},
       {"post_id":52751,"title":"none" ,
       "body":"you may have passed some old tissue you should go to..."
```

FIGURE 5. Part of a transmission of private information of users chatting over HTTP.

offering this function. Our results indicate that an insecure chat implementation can lead to several privacy risks for all its participants. One major issue is the non-use of HTTPS connections. Additionally, insecure database queries can lead to unnecessary transmission of personal, sensitive and health information even together in only one request. Figure 5 shows a part of a response we collected through a GET request over HTTP. The request, in addition to leaking private information from the user, discloses data from other users participating in the chat. More specifically, the request leaks email addresses, passwords, names, images and health related questions. For privacy reasons we have blinded out part of the users' sensitive information in Figure 5.

D. SSL WEB SERVER CONFIGURATION

In the fifth step of our methodology we analyzed the web server configuration to determine the security level of HTTPS data transmission. In order to analyze the SSL web configuration of each captured domain, we used the SSL Server Test service from Qualyss SSL labs. This service tests and rates the SSL web server configuration of each domain with a letter grade scale (A, B, C, D, E, F, M, T). Tests include: i. the assessment of the certificate to verify that it is valid and trusted, ii. the inspection of the server configuration in three categories: a. protocol support, b. key exchange support and c. cipher support.

We divided our findings into HTTPS connections to domains that are owned by the apps' vendors and HTTPS connections to third party servers. The number of HTTPS connections to servers owned by vendors for each app per SSL grade result is presented in Table 6. Apps that do not establish at least one HTTPS connection to its vendor's server are excluded from the table. Additionally, the number of HTTPS connections to third parties for each app per SSL grade result is presented in Table 7. Moreover, the total number of HTTPS connection for each data category per SSL grade result is presented in Table 8.

TABLE 6. Number of HTTPS connections to Vendors' domains per SSL grade result.

	Grade						
App No.	A	B	C	D	E	F	T
App No. I	1	0	0	0	0	0	0
App No. II	0	1	0	0	0	0	0
App No. VII	1	0	0	0	0	0	0
App No. IX	1	0	0	0	0	0	0
App No. XIII	0	0	0	0	0	0	2
App No. XVI	0	2	0	0	0	0	0
App No. XVIII	0	0	1	0	0	0	0
App No. XIX	1	0	0	0	0	0	0
App No. XX	1	0	0	0	0	0	0
N	5	3	1	0	0	0	2

E. RESPONSE TO OUR SECURITY AND PRIVACY REPORTING

As described in our methodology's final step, we provided each app vendor with a report of our findings using the vendor's email address provided in Google Play. By the date we performed our re-evaluation process, one of the apps had been withdrawn from the Google Play and therefore, from now on, we do not include it in our tests and results.

1) PRIVACY POLICY

Since our initial evaluation in 2016, app vendors that did not have a published on-line privacy policy on Google Play had, at least, two major reasons to add one. First, as we already mentioned, since early 2017 Google has sent notifications to app developers asking to provide a valid privacy policy. Second, we reported the issue to each app's vendors when we informed them of our initial evaluation results. Hence, one would have expected that by the 5th of July 2017 (*i.e.*, the date we performed our re-evaluation process regarding the existence of a privacy policy link on Google Play)

TABLE 7. Number of HTTPS connections to third party domains per SSL grade result

App No.	Grade A	B	C	D	E	F	T
App No. I	4	5	0	0	0	0	0
App No. II	1	2	0	0	0	0	0
App No. III	0	4	0	0	0	0	0
App No. IV	0	1	0	0	0	0	0
App No. V	0	2	0	0	0	0	0
App No. VI	0	2	0	0	0	0	0
App No. VII	6	4	0	0	0	0	1
App No. VIII	0	2	0	0	0	0	0
App No. IX	0	1	0	0	0	1	0
App No. X	0	2	0	0	0	0	0
App No. XI	0	5	0	0	0	0	0
App No. XII	0	1	0	0	0	0	0
App No. XIII	0	5	0	0	0	0	0
App No. XIV	0	1	0	0	0	0	1
App No. XV	1	0	0	0	0	0	0
App No. XVI	0	1	0	0	0	0	0
App No. XVII	7	9	3	0	0	0	1
App No. XVIII	2	2	0	0	0	1	0
App No. XIX	7	8	4	0	0	2	0
App No. XX	5	8	3	0	0	2	0
N	33	65	10	0	0	6	3

TABLE 8. Total number of HTTPS connections for each data category per SSL grade.

Grade	Email	Password	Location	Health data	Search queries	Unique ID
A	3	2	1	4	0	0
B	7	5	2	2	2	2
C	1	1	0	1	0	0
F	2	0	0	0	0	2
T	0	1	1	1	0	1

all the apps would have a proper link to their privacy policy. Surprisingly, one of the apps kept missing a privacy policy, another app provideed a link to an error page and, another app kept having a link to a privacy policy page not translated into English.

2) SECURE TRANSMISSION OF USER DATA

In this section we report the results obtained after repeating the fourth step of our methodology. More specifically, we re-evaluated the apps by re-running the dynamic analysis on their updated versions in order to check whether the reported issues were solved or still remained. For the sake of clarity, we have categorized our findings into minor and major issues, and we analyze how many of them (in each category) remain in the re-evaluated version of the apps. It should be noted that in our results we count the number of minor or major issues and not the frequency at which these issues occur. Table 9 provides some examples of minor and major issues.

TABLE 9. Example cases of major or minor issues.

Example of major and minor issues	Major	Minor
Transmission of Device IDs or Personal or Health data (in any way) to 3rd parties	✓	
Transmission of Device IDs or Personal or Health data insecurely to Vendor (i.e. over HTTP via GET or POST request)	✓	
Transmission of Device IDs or Personal or Health data to Vendor via GET request over HTTPS		✓
Transmission of anonymous behavioral data to 3rd parties		✓

We use the term *"major issue"* to refer to those that may lead to the identification of the user when sensitive information is transmitted to third parties, even when the appropriate secure measures are in place, as well as when sensitive information is disseminated to vendors without safeguarding the appropriate secure mechanisms. Alternatively, we use the term *"minor issues"* to refer to cases where leakages of non-personal information (*e.g.,* behavioral data) may occur. Also, we consider minor issues those cases in which best practices are not implemented and lead to sensitive information leakage.

Figure 6 shows the number of major issues found before and after we notified the app vendors. We observe that for most of the apps there is a clear improvement. On the other hand, the improvement is almost non-existent in terms of minor issues as shown in Figure 7. Only 5 out of the 12 apps with minor issues have partially or completely solved the reported problems.

F. GDPR-READINESS ASSESSMENT

Apart from our previously described re-evaluation process, we have also proceeded to an additional evaluation process in order to check whether the apps meet the legal data protection requirements specified in the GDPR's provisions. Inevitably, the analysis of some requirements defined in the regulation would require access to each vendor's infrastructure in order to be checked for compliance (*e.g.,* the requirement for Data Protection Impact Assessment (Art 35)) – a precondition rather unrealistic in our case. In addition, the technical implementation of some GDPR's requirements is not yet crystal-clear in all of its technical details (*e.g.,* the Right to be Forgotten (Art. 17)). Hence, only those requirements that can be efficiently and unambiguously checked against each app's implementation have been chosen to be evaluated in this study.

In this section, we do not include results for non-functional security requirements of GDPR, such as secure transmission or/and strong authentication, for which the reader might refer to Sections 4.2 and 4.3 of this article. Additionally, while we have repeatedly checked for the existence of a

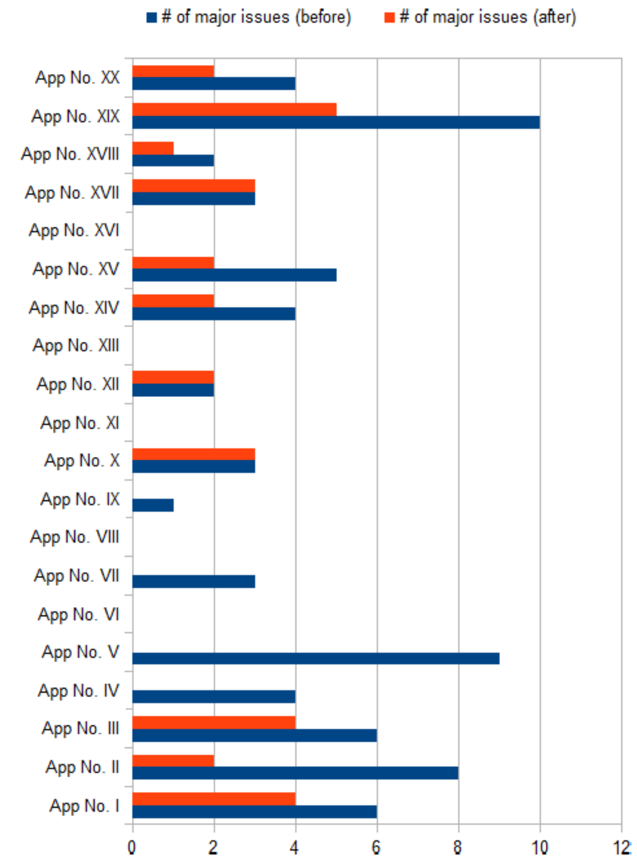


FIGURE 6. Number of major issues per app before and after our reportings.

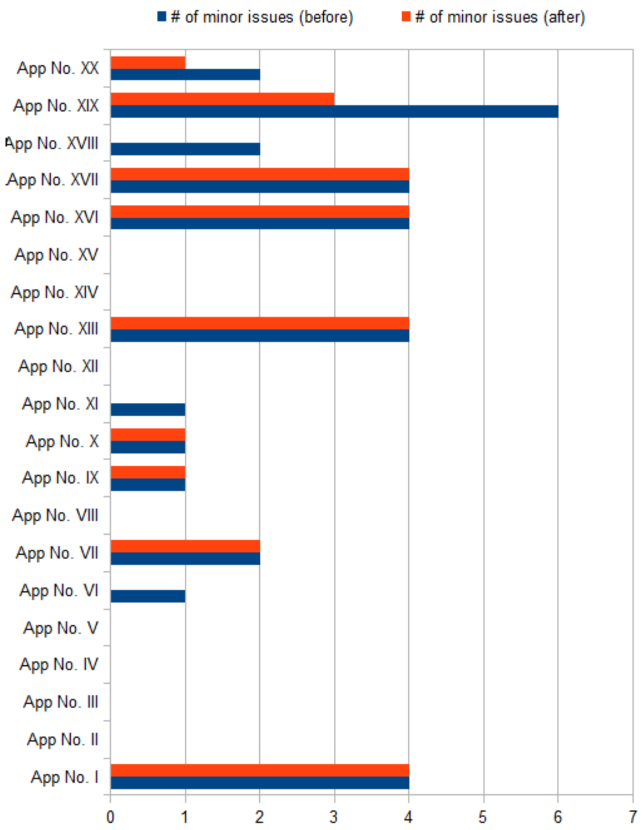


FIGURE 7. Number of minor issues per app before and after our reportings.

link to a privacy policy on Google Play, in this section and according to GDPR requirements we will thoroughly check if this section, with the required content, exists while the user navigates inside the app. Note that many of our checks are limited to the existence of the minimum elements to satisfy the GDPR requirements, such as the existence of a functional element that provides information regarding the collection of the user's personal data up front his registration.

Below, we present our results for the 19 apps under review that are currently available on-line. For the sake of clarity, we present our findings divided into two categories, namely "functional requirements" and "non-functional requirements" of the GDPR.

1) FUNCTIONAL REQUIREMENTS

- Consent (I): 11 out of the 19 apps provide, at least, an introductory information regarding their privacy policy or/and term of use before registration.
- Consent (II): Only one of the apps is found to ask for user consent up front each time the user provides additional information.
- Consent (III): None of the apps require users to answer specific questions, in electronic form, about their willingness to participate.
- Right to withdraw consent: 7 out of the 19 apps provide users with an option to withdraw their consent, and thus allow for the erasure of any previously consented information. Nevertheless, in 1 out of the 7 apps providing this option, the deletion functionality doesn't seem to work. Three of 12 apps state that user data can be deleted only by sending appropriate email requests to the app's vendor. Yet, two out of 12 apps offer users the possibility to delete their records individually, one at a time, and not all at once. Furthermore, one app refused to delete users data with the excuse that: "Sometimes we were asked about deleting all records, to start a new series of measurement. But there is no reason to do this. The time range can be changed to view only the wanted part of all records. So old readings can stay". We let the readers judge this response by themselves.
- Right to data portability: 7 out of the 19 apps provide users with a mechanism to send, upon request, their personal data to another entity in a machine readable format (*e.g.*, XML or CSV format), 2 of these 7 apps offer this function via a web-based platform. As for the rest of the 12 apps, one that does not provide such portability mechanism, advertises this functionality in its paid version, while another sends the data only as text in the body of an email. Another app offers the data only after a request by email, while another enables users to share their dashboards with their preferred users, but not the actual data. Finally, one app provides a sharing

mechanism by email for each of its sections individually, but not for the whole amount of user data in a single request.

2) NON-FUNCTIONAL REQUIREMENTS

- Data Protection Officer: In terms of the *Data Protection Officer* requirement, all apps fail to provide any contact details for such a role. Nevertheless, 12 out of the 19 apps offer a point of contact for support purposes.
- Profiling and marketing: Information on collection and processing of user data for profiling purposes was provided by 11 out of the 19 apps. This profiling information is available, in most cases, in the apps' privacy policy section.
- Transfer to third countries: 8 out of the 19 apps notify their users in advance, even before their registration, that they are sharing data with third parties. Half of these 8 apps implements this notification in a functional manner (*e.g.,* a checkbox or a pop up window), while the other half notifies their users by including a relevant statement into the privacy policy or "terms of use" sections.

V. CONCLUSION

Mobile health (m-Health) apps have gained momentum and currently they are widely spread among cellphone users. Despite the warm welcome from users, m-health apps have raised concern regarding their management of private information. Indeed, m-health apps have to deal with health-related data, which are consider very sensitive and are highly protected by national and international regulations such as the GDPR.

With the aim to assess the current state of practice in m-health apps regarding the protection of health-related data, we have analyzed a representative set of apps, for more than a year, and we have studied the diverse facets of their security and privacy policies and practices. Our study highlights numerous major and minor shortcomings of m-health applications. A large portion of the assessed apps has been found to jeopardize user's privacy and security by violating sensitive data protection regulations set to prevent the inappropriate and uncontrollable usage, processing and disclosure of health data to third parties. According to our analysis, a relevant number of popular m-health apps could violate users' privacy by revealing sensitive information such as health conditions, medical symptoms, photos, location, e-mails and passwords.

Lack of encryption, use of GET instead of POST requests for sensitive data transmission, and insecure programming practices, are some of the major security and privacy open issues for developers to solve when building m-health apps. User profiling, either for advertising and marketing purposes or for user behavior monitoring, is an additional privacy concern that needs to be taken into account to guarantee users privacy. Even though the conformance to the current data protection regulations should provide m-health application users with data transparency, it is still a hard to achieve functionality. In particular, the upcoming enforcement of the GDPR in May 2018 within the EU is expected to meet with technical challenges, such as tracking and deleting user disseminated data to third parties, and designing and developing internal procedures satisfying GDPR auditing and data protection requirements.

In light of the above, security experts and privacy advocates raise the alarm about the potential privacy harms that derive from m-health apps processing personal and sensitive data, and urge for suitable countermeasures. As revealed by the European Commission's 2014 m-Health Green Paper [31], European citizens do not trust m-Health apps since 67% of the surveyed population said they would never use any m-health capability of their mobile phone in support of their health. In an effort to build solid foundations and easily implementable privacy standards for the development of m-health applications, and specially for fostering trust among their users, European Commission issued in 2016 a draft "Code of Conduct on privacy for mobile health applications" [32]. Although its final version is yet to be adopted, as it is subjected to the implementation of Article 29 Data Protection Working Party comments [33] and to its conformance to the GDPR's provisions, it is still a good reference point for providing practical guidelines to app developers in order to build reliable applications compliant with data protection standards and principles.

APPENDIX

PERSONAL, SENSITIVE AND HEALTH DATA

Within the EU domain and according to the GDPR, Article 4, personal data are defined as any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. This definition clarifies that personal data are any information that can be used on its own or with other information to identify, contact, or locate an individual. Hence, in the EU, any location information or any device ID which uniquely bind a place or a device respectively to an individual fall under the personal data category. The US however have not adopted yet a comprehensive information privacy law but they are rather having limited sectoral laws in some areas, such as the HIPAA for health related data processing. Hence, there is not a universal definition of personal data across all of the States. Still, the Privacy Shield Framework (https://www.privacyshield.gov) between the EU and the US, specified to foster compliance with data protection requirements when transatlantic transferring of personal data is concerned, defines personal data as data about an identified or identifiable individual that are within the scope of the DPD, and the GDPR by extension. In Canada, where the Personal Information Protection and Electronic

Documents Act (PIPEDA) (https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/) has been active since 2001, personal information means information about an identifiable individual, but does not include the name, title, or business address or telephone number of an employee of an organization.

Even since the DPD era, health data were classified in a special category of personal data, called ''sensitive'', referring to data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. Under the GDPR, the ''genetic data'' and ''biometric data'' have been also expressly added in the sensitive data class, only in the case though that may be used for uniquely identifying a natural person. The sensitive data are generally prohibited from processing unless specific derogations and exemptions apply. For instance, the grounds of processing sensitive data under the GDPR, which are more or less similar to those defined in its predecessor DPD, include, apart from user's explicit consent, some advanced conditions for processing, such as when the data are necessary for the purposes of preventative or occupational medicine, or for reasons of public interest in the area of public health, or necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes (Article 9-2 (a)-(j)). Across the Atlantic and despite the lack of a comprehensive personal data definition, the Federal Trade Commission (FTC), an independent agency of the US government, issued in 2009 a report[1] suggesting that data considered as sensitive should include financial data, data about children, health information, precise geographic location information and social security numbers. Still, every organization in the US should evaluate independently the sensitivity of each individual personally identifiable information [34].

While health data are defined to be sensitive under all data protection regulations, the strict classification of which exact information falls under the category of health-related data has not been provided, up until recently, under any data protection act, leaving room to individual interpretations. The GDPR specifies in broad terms the types of data included in the definition of ''data concerning health'', and only substantially increases what is specified in the DPD.[2] It expressly covers both physical and mental health and explicitly defines that health data are all personal data relating to the physical or mental health of an individual, including the provision of health care services, which reveal information about his or her health status (Rec. 35, 53-54; Art.4(15)).

However, in 2015 the Article 29 Data Protection Working Party [35] (Art. 29 WP) published a letter [36] with an annex [37] clarifying the scope of the key legal term ''health data'' in relation to the lifestyle and wellbeing apps. According to this annex, health data are not certainly limited to ''medical data'' in the strict sense (i.e., data about an individual's physical or mental health status generated in a professional medical context, including data generated by apps or devices used in this context). Instead, they include all data pertaining to an individual's health status, regardless of the context in which they were collected and regardless of whether the information establishes ''ill health''. According to Art. 29 WP position, personal data are health data when: i. the data are inherently/clearly medical data, ii. the data are raw sensor data that can be used in itself or in combination with other data to draw a conclusion about the actual health status or health risk of a person, iii. conclusions are drawn about a person's health status or health risk (irrespective of whether these conclusions are accurate or inaccurate, legitimate or illegitimate, or otherwise adequate or inadequate). Even though the Opinions and Recommendations published by the Art. 29 WP are not legally binding, still they do provide directions for conflict resolutions.

In the US, the HIPAA defines health data as the ''Protected Health Information'' (PHI)[3] that includes all ''individually identifiable health information'' held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. In particular, defines that health information means any information that: (i) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (ii) relates to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual. ''Individually identifiable health information'' is a subset of the PHI[4] which also identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Hence, individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

REFERENCES

[1] C. Spensky *et al.*, ''SoK: Privacy on mobile devices—It's complicated,'' *Privacy Enhancing Technol.*, vol. 2016, no. 3, pp. 96–116, 2016.

[2] S. Fahl, M. Harbach, T. Muders, L. Baumgärtner, B. Freisleben, and M. Smith, ''Why eve and mallory love Android: An analysis of Android SSL (in)security,'' in *Proc. ACM Conf. Comput. Commun. Secur.*, 2012, pp. 50–61.

[3] G. Qin, C. Patsakis, and M. Bouroche, ''Playing hide and seek with mobile dating applications,'' in *Proc. IFIP Int. Inf. Secur. Conf.*, 2014, pp. 185–196.

[4] C. Patsakis, A. Zigomitros, and A. Solanas, ''Analysis of privacy and security exposure in mobile dating applications,'' in *Proc. Int. Conf. Mobile, Secure Programm. Netw.*, 2015, pp. 151–162.

[1] https://www.ftc.gov/news-events/press-releases/2009/02/ftc-staff-revises-online-behavioral-advertising-principles

[2] https://www.whitecase.com/publications/article/chapter-5-key-definitions-unlocking-eu-general-data-protection-regulation

[3] https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

[4] https://www.hipaa.com/hipaa-protected-health-information-what-does-phi-include/

[5] M. Conti, L. V. Mancini, R. Spolaor, and N. V. Verde, "Analyzing Android encrypted network traffic to identify user actions," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 1, pp. 114–125, Jan. 2016.

[6] Y. J. Jia, Q. A. Chen, Y. Lin, C. Kong, and Z. M. Mao, "Open doors for bob and mallory: Open port usage in Android apps and security implications," in *Proc. 2nd IEEE Eur. Symp. Secur. Privacy*, Apr. 2017, pp. 190–203.

[7] (2016). *Developers and Publishers are Flocking to the mHealth App Market, BI Intelligence*. [Online]. Available: http://www.businessinsider.com/developers-andpublishers-are-flocking-to-the-mhealth-app-market-2016-10

[8] A. Solanas, J. H. Weber, A. B. Bener, F. van der Linden, and R. Capilla, "Recent advances in healthcare software: Toward context-aware and smart solutions," *IEEE Softw.*, vol. 34, no. 6, pp. 36–40, Nov./Dec. 2017.

[9] A. Solanas *et al.*, "Smart health: A context-aware health paradigm within smart cities," *IEEE Commun. Mag.*, vol. 52, no. 8, pp. 74–81, Aug. 2014.

[10] C. Kolias, A. Stavrou, J. Voas, I. Bojanova, and R. Kuhn, "Learning Internet-of-Things security 'hands-on,'" *IEEE Security Privacy*, vol. 14, no. 1, pp. 37–46, Jan./Feb. 2016.

[11] R. Want, B. N. Schilit, and S. Jenson, "Enabling the Internet of Things," *Computer*, vol. 48, no. 1, pp. 28–35, 2015.

[12] C. L. Ventola, "Mobile devices and apps for health care professionals: Uses and benefits," *Pharmacy Therapeutics*, vol. 39, no. 5, pp. 356–364, 2014.

[13] N. Bouri and S. Ravi, "Going mobile: How mobile personal health records can improve health care during emergencies," *JMIR mHealth uHealth*, vol. 2, no. 1, p. e8, 2014.

[14] (2015). *Special Eurobarometer 431: Data Protection, Directorate-General for Communication*. [Online]. Available: https://data.europa.eu/euodp/el/data/dataset/S2075_83_1_431_ENG.

[15] Regulation, General Data Protection, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46," *Official J. Eur. Union*, vol. 59, pp. 1–88, 2016. [Online]. Available: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679

[16] European Community, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data on the free movement of such data, 1995. [Online]. Available: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046

[17] P. de Hert and V. Papakonstantinou, "The new general data protection regulation: Still a sound system for the protection of individuals?" *Comput. Law Secur. Rev.*, vol. 32, no. 2, pp. 179–194, 2016.

[18] D. He, M. Naveed, C. A. Gunter, and K. Nahrstedt, "Security concerns in Android mhealth apps," in *Proc. AMIA Annu. Symp.*, 2014, pp. 645–654.

[19] R. Adhikari, D. Richards, and K. Scott, "Security and privacy issues related to the use of mobile health apps," in *Proc. ACIS*, 2014.

[20] K. Knorr and D. Aspinall, "Security testing for Android mhealth apps," in *Proc. IEEE 8th Int. Conf. Softw. Test., Verification Validation Workshops (ICSTW)*, Apr. 2015, pp. 1–8.

[21] K. Knorr, D. Aspinall, and M. Wolters, "On the privacy, security and safety of blood pressure and diabetes apps," in *Proc. IFIP Int. Inf. Secur. Conf.*, 2015, pp. 571–584.

[22] C. M. L. Njie, "Technical analysis of the data practices and privacy risks of 43 popular mobile health and fitness applications," Privacy Rights Clearinghouse, USA, Tech. Rep., 2013. [Online]. Available: https://www.privacyrights.org/

[23] K. Huckvale, J. T. Prieto, M. Tilney, P.-J. Benghozi, and J. Car, "Unaddressed privacy risks in accredited health and wellness apps: A cross-sectional systematic assessment," *BMC Med.*, vol. 13, no. 1, p. 214, 2015.

[24] T. Dehling, F. Gao, S. Schneider, and A. Sunyaev, "Exploring the far side of mobile health: information security and privacy of mobile health apps on iOS and Android," *JMIR mHealth uHealth*, vol. 3, no. 1, p. e8, 2015.

[25] A. Sunyaev, T. Dehling, P. L. Taylor, and K. D. Mandl, "Availability and quality of mobile health app privacy policies," *J. Amer. Med. Informat. Assoc.*,vol. 22, no. 1, pp. e28–e33, 2015.

[26] E. Alepis and C. Patsakis, "Hey doc, is this normal?: Exploring Android permissions in the post marshmallow era," in *Proc. Int. Conf. Secur., Privacy Appl. Cryptograph. Eng.*, 2017, pp. 53–73.

[27] T. Book, A. Pridgen, and D. S. Wallach. (2013). "Longitudinal analysis of Android ad library permissions." [Online]. Available: https://arxiv.org/abs/1303.0857

[28] T. Book and D. S. Wallach, "A case of collusion: A study of the interface between ad libraries and their apps," in *Proc. 3rd ACM Workshop Secur. Privacy Smartphones Mobile Devices*, 2013, pp. 79–86.

[29] E. Alepis and C. Patsakis, "There's wally! location tracking in Android without permissions," in *Proc. 3rd Int. Conf. Inf. Syst. Secur. Privacy (ICISSP)*, Porto, Portugal, Feb. 2017, pp. 278–284. [Online]. Available: https://doi.org/10.5220/0006125502780284

[30] C. Patsakis, A. Zigomitros, A. Papageorgiou, and A. Solanas, "Privacy and security for multimedia content shared on OSNs: Issues and countermeasures," *Comput. J.*, vol. 58, no. 4, pp. 518–535, 2015.

[31] E. Commission. *Green Paper on Mobile Health ('mHealth')*. Accessed: Nov. 30, 2017. [Online]. Available: https://ec.europa.eu/digital-single-market/en/news/green-paper-mobilehealth-mhealth

[32] E. Commission. *Draft Code of Conduct on Privacy for Mobile Health Applications*. Accessed: Nov. 30, 2017. [Online]. Available: http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=16125

[33] H. Graux. *Article 29 Data Protection Working Party*. Accessed: Nov. 30, 2017. [Online]. Available: http://ec.europa.eu/newsroom/document.cfm?doc_id=44371

[34] *Guide to Protecting the Confidentiality of Personally Identifiable Information PII, NIST*. Accessed: Nov. 30, 2017. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf

[35] *Article 29 Working Party*. Accessed: Nov. 30, 2017. [Online]. Available: http://ec.europa.eu/newsroom/just/itemdetail.cfm?item_id=50083

[36] P. Timmers. *Article 29 Data Protection Working Party*. Accessed: Nov. 30, 2017. [Online]. Available: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_en.pdf

[37] *Annex—Health Data in Apps and Devices*. Accessed: Nov. 30, 2017. [Online]. Available: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf

ACHILLEAS PAPAGEORGIOU received the B.Sc. degree in communications, informatics and management from the Techological Educational Institute of Epirus, Greece, and the M.Sc. degree in digital communications and networks from the Department of Digital Systems, University of Piraeus, Greece, where he is currently pursuing the Ph.D. degree with the Department of Informatics. He is the Head of digital strategy at a private company in Greece. His current research interests include security and privacy in personalized health services, smart health, social networks, and Internet of Things.

MICHAEL STRIGKOS received the B.Sc. degree in information management from the Techological Educational Institute, Kavala, Greece, and the M.Sc. degree in digital communications and networks from the Department of Digital Systems, University of Piraeus, Greece. He is a Senior Web Developer. His current research interests include Web security.

EUGENIA POLITOU received the Diploma (BSE) degree in electrical and computer engineering and the M.Sc. degree in digital image processing and Internet databases from Democritus University of Thrace, Xanthi, Greece. She is currently pursuing the Ph.D. degree in informatics with the University of Piraeus, Greece. Her current research interests include human–computer interaction, mobile computing, privacy, and data protection. She has a great experience in research, security, analysis, and design under various national and European large-scale IT projects within the private and public sector.

EFTHIMIOS ALEPIS received the B.Sc. degree in informatics and the Ph.D. degree from the Department of Informatics, University of Piraeus, Greece, in 2002 and 2009, respectively. He has been an Assistant Professor with the Department of Informatics, University of Piraeus, since 2013. He has authored/co-authored over 60 scientific papers which have been published in international journals, book chapters, and international conferences. His current research interests include the areas of object-oriented programming, mobile software engineering, human–computer interaction, affective computing, user modeling, and educational software.

AGUSTI SOLANAS (S'03–M'06–SM'14) received the M.Sc. degree (Hons.) in computer engineering from Rovira i Virgili University (URV) in 2004, the Diploma of Advanced Studies from the Technical University of Catalonia in 2005, and the Ph.D. degree from the Department of Telematics Engineering, Technical University of Catalonia in 2007. He is a Professor with the Department of Computer Engineering and Mathematics and the Head of the Smart Health research group, URV. His current research interests include smart health, health informatics, behavior analysis, multivariate analysis, privacy protection, and computer security. He serves as a Scientific Coordinator at APWG.EU

CONSTANTINOS PATSAKIS received the B.Sc. degree in mathematics from the University of Athens, the M.Sc. degree in information security from Royal Holloway, and the Ph.D. degree in security from the University of Piraeus. He is currently an Assistant Professor with the University of Piraeus. He has several publications in peer-reviewed international conferences and journals and participated in many national and European research and development projects. His main areas of research interests include cryptography, security, privacy, and data anonymisation. He was a Researcher at the UNESCO Chair in Data Privacy and the Trinity College.