Università degli Studi di Padova

Dipartimento Matematica

Master Thesis in Cybersecurity

Privacy and Security Analysis of mHealth Apps

Master Candidate

Eleonora Mancini

Supervisor

Prof. Mauro Conti

Academic Year
2021/2022

To Giovanni,
who taught me to work hard
for my goals while enjoying life

Abstract

The widespread availability of Mobile Health (mHealth) applications has been significantly accelerated by the outbreak of the COVID-19 pandemic. While bringing many benefits, from self-monitoring to medical consultations, mHealth apps process many sensitive health-related user data. Therefore, they are subject to privacy regulations set by government, such as General Data Protection Regulation (GDPR) in the EU and Health Insurance Portability and Accountability Act (HIPAA) in the USA, as well as privacy guidelines of the app store (e.g., Google Android). In this work, we analyze the privacy, compliance, and security of 232 mHealth apps in the Android ecosystem, mainly focusing on the most popular free apps (199), but also considering a sample of paid apps (25) and healthcare provider/clinician apps published on the US Centers for Disease Control and Prevention (CDC)'s website (8). For our analysis, we leverage both static approaches, such as privacy policy and APK analysis, and dynamic approaches, like network traffic inspection and analysis of in-app consent acquisition. Our findings reveal that 85.4% of the free mHealth apps do not properly inform the users about all the aspects of the data processing required by the regulations. In addition, they often contain conflicting or incomplete information: only 2.51% of them are completely consistent. Moreover, 55.8% of these apps process user data without explicit consent. Our analysis shows that, when compared to free apps, paid ones are less careful in writing the privacy policy, while containing a lower number of trackers and dangerous permissions on average. We found that 76% of these apps fail in obtaining explicit consent and 84% of them process some types of data without informing the user. Concerning the CDC-endorsed apps, while we did not detect a pervasive presence of trackers, dangerous permissions or sensitive data in the network traffic, our results show that all of them have incomplete privacy policies and fail to ask for explicit consent before accessing their services. As we consider apps with a mean of 8 millions downloads each, our study impacts a lot of end-users and helps creating awareness of mHealth apps' privacy importance among both users and developers.

Contents

List of Figures

List of Tables

List of Acronyms

GDPR General Data Protection Regulation

HIPAA Health Insurance Portability and Accountability Act

CDC Centers for Disease Control and Prevention

PHI Protected Health Information

e-PHI Electronic Protected Health Information

mHealth Mobile Health

APK Android Package Kit

MobSF Mobile Security Framework

PHR Personal Health Record

MITM Man In The Middle

SSL Secure Sockets Layer

HTTP Hypertext Transfer Protocol

HTTPS Hypertext Transfer Protocol Secure

IP Internet Protocol

IMEI International Mobile Equipment Identity

AAID Android Advertising ID

UDID Unique Device Identifier

GSF ID Google Services Framework ID

MD5 Message Digest Method 5

SHA-1 Secure Hash Algorithm 1

CBC Cipher Block Chaining

EBC Electronic Code Book

AES Advanced Encryption Standard

SQL Structured Query Language

GOT Global Offset Table

RELRO Relocation Read-Only

OS Operating System

GUI Graphical User Interface

DAC Discretionary Access Control

GPS Global Positioning System

SMS Short Message Service

MMS Multimedia Message Service

EU European Union

USA United States of America

SSN Social Security Number

1

Introduction

Mobile Health (mHealth) applications are software applications that run on mobile platforms and offer functionalities related to personal healthcare, wellness and medical information management [42]. They provide body measurement recording, health and fitness tracking, sleep tracking, services to get medical appointments or access medical records and many other features [57, 62]. The COVID-19 pandemic played a critical part in the rise of the mHealth area, with a 65% increase in the downloads during 2020 globally [13]. The mHealth market size grew from 45.31 billion USD in 2022 to 56.77 billion USD in 2023, and the prediction is that its value will reach 136.64 billion USD in 2027 [38].

mHealth apps can obtain health-related data through various means, including the use of built-in sensors on wearable devices and smartphones or through manual input by the user or a medical practitioner, as seen in medical appointments and electronic medical record applications. The collected data are then stored and transferred for additional purposes such as enhanced visualizations for the user or the availability of historical data for analysis. Besides, they can also process other personal information not related to health, such as location, contacts, personal files and photos [45]. Since they deal with all these sensitive data, they must comply with privacy regulations such as GDPR [21] and HIPAA [31], as well as the privacy guidelines of the app store, such as Google's privacy guidelines [23].

Complying with privacy regulations and guidelines provides transparency to the end user; however, an insecure mHealth app can still put user data at risk, if it does not implement proper security measures or share data with unauthorized parties. Malicious actors can use these data for nefarious purposes, such as location tracking, bypassing authentication checks, or compromising the device. Additionally, unauthorized parties may use the health data for targeted advertisements without the user's consent [50]. To avoid any sensitive data being leaked to third parties, mHealth apps need to implement security measures such as data encryption and secure communication.

Prior to our work, there has been a body of research in the literature investigating mHealth apps. Papageorgiu et al. [45] showed that the majority of mHealth apps do not follow well-known guidelines and rules, while another study [14] reveals that mHealth apps about menstrual cycle are developed with low-security standards. Many works [27, 33, 43, 47, 44, 10, 35, 28, 26, 62, 45, 14, 29, 61, 5, 4] analyzed compliance with GDPR or HIPAA and another study [60] investigated whether Android apps' privacy policies comply with Google's privacy guidelines. However, none of these prior studies performed a comprehensive analysis of mHealth apps in terms of privacy, compliance and security.

In our work, we inspect the most popular free mHealth apps in the Android ecosystem in terms of their privacy and security. With these apps counting an average of more than 8 million downloads each, our findings will impact a large number of end-users. For the privacy analysis, we first examine their compliance with the privacy regulations of the EU and USA. Then, we observe how the apps implement consent acquisition and analyze their permissions and trackers through APK inspection. After that, we analyze their network traffic to detect Personal Health Information (PHI) data-sharing practices. Finally, we conduct an inconsistency analysis by comparing four different sources of data: 1) the data safety section of the Google Play store, 2) the privacy policy, 3) the permissions declared in the APK source code and 4) the network traffic collected while using the app. For the security analysis, we examine the mHealth apps to understand whether they have vulnerabilities that can put the user's personal data at risk. For this, we employ `MobSF` [40] to perform static APK analysis, `SSL Labs` [54] to evaluate the security of SSL configurations and `drozer` [15] to interact with apps' components.

Our analysis reveals that the privacy policies provided by mHealth apps do not always succeed in mentioning all the relevant information regarding the data processing that is required by the privacy rules. For example, 21.6%

of the apps do not include the user's rights and, in 36.4% of cases, these are only mentioned for users of certain locations (e.g. the EU, California), possibly creating confusion in other users, who may not understand which rights they have and how they can exercise them. It is also common to find inconsistent information between the privacy policy and data safety section, which makes it difficult for the users to understand how their data will be handled: only 2.51% of the apps are consistent in all aspects. These two sources of information should notify the user about what kind of data the app processes; however, 36.2% of the apps process data that they do not mention in at least one of these sources. Furthermore, 55.8% of free mHealth apps do not obtain explicit consent from the user before letting them use their services.

In addition to the most popular free apps, we also study a sample of paid mHealth apps. Our results show that the latter, when compared to the free apps, do not put additional care into protecting the user's privacy. We detected that, while they generally use a lower number of trackers and dangerous permissions, their privacy policies and data safety sections lack completeness. All the paid apps in our dataset fail to provide a complete privacy policy, i.e., they either do not provide a privacy policy or provide an incomplete one. We did not find the data safety section for 20% of them and 56% have an incomplete one, meaning that they lack some information required by Google's privacy guidelines. Additionally, only 4% of paid apps put consistent statements in these two sources. Furthermore, 84% of them violate those statements in at least one of the sources. Finally, paid apps process user data without explicit consent in 76% of cases.

We perform a study on mHealth apps endorsed by the US Centers for Disease Control and Prevention (CDC), which shows that half of them do not have a data safety section and all of them have incomplete privacy policies. Furthermore, these two sources are never consistent with each other. Interestingly, none of the CDC apps obtains explicit user consent. On the other hand, we detected a lower presence of trackers and permissions, as well as a lower amount of user data sent over the Internet, especially to third-party trackers.

Contributions. The main contributions of this study are as follows:

- We performed a comprehensive analysis of the privacy, compliance and security of the most popular mHealth Android apps, considering both GDPR and HIPAA privacy rules.
- We investigated for the first time whether mHealth apps comply with

Google's requirement to fill in the data safety section on Google Play. Moreover, we highlighted for the first time the inconsistency issues between the data safety section, the privacy policy and the actual network traffic.

- We performed studies on paid and CDC-endorsed mHealth apps, finding out that many of them have missing details in their privacy policies and fail to comply with Google's requirements, besides not following the rules on consent acquisition.

The results and findings of our study emphasize the importance of creating awareness among both users and developers of mHealth applications dealing with such sensitive data. In this manner, this can serve as a useful guide for both.

Organization. The rest of the thesis is structured as follows: Chapter 2 introduces the background on the Android operating system and on the privacy rules that we focus on. Chapter 3 illustrates the mHealth dataset that we used throughout the analysis and the methodology used to carry out the app inspection. Chapter 4 describes the results; in particular, Section 4.1 discusses the privacy and compliance results and Section 4.3 the ones about security. The findings for CDC-endorsed and paid mHealth apps are discussed in chapters 5 and 6. Chapter 7 takes into account the limitations of our study and Chapter 8 describes the related work on privacy and security of mobile apps. Lastly, we conclude with some final considerations in Chapter 9.

2
Background

This chapter introduces the technical background on Android applications and on the privacy rules that we will consider in our work.

2.1 Android Operating System

Android, developed by Google, is an open-source mobile Operating System (OS) based on the Linux kernel. Launched in 2008, it has gained more and more popularity, becoming the leader of the most used operating systems worldwide [52, 49, 2]. However, high popularity also constitutes increasing risks and threats that the OS needs to face, making it difficult to find a balance between security, privacy and usability [37].

2.1.1 Android applications

Android applications are mostly developed in Kotlin, Java or Flutter and they consist of an archive containing files and folders with an `.apk` (Android Package Kit) extension. It is also possible to develop part of the app in native code with C, C++ or Rust programming languages [51]. An important file contained in the `apk` archive is the Android Manifest, which specifies the app's meta-data such as package name, components, permissions, libraries and version supported [17]. An android app is composed of multiple components, which are as follows:

- *Activity:* a component that provides a Graphical User Interface (GUI) to interact with the user. Each screen of the app corresponds to an activity and the *Main Activity* is displayed when the app is launched.

- *Service:* a component that performs operations in the background, without a GUI.
- *Broadcast receiver:* a component that allows the app to register for events so that it can receive notifications about those events by the system or by other apps when they occur.
- *Content provider:* an interface that allows access to structured data from inside or outside the app. Data can be stored in a database or files or over a network.

An app component can be accessed from other apps if it is marked as exported. Apps may need to export their components if they need other apps to interact with them. However, if this is not done with the proper restrictions, it can also lead to security issues [14, 51].

2.1.2 Android security

To protect the security of each app and prevent it to be accessed by others, the Android kernel implements Linux Discretionary Access Control (DAC), in which each app is assigned a unique id and runs in a sandboxed environment. Two different apps may share the same sandbox only if they are signed with the same certificate [17].

2.1.3 Android Permissions

The android platform employs a permission-based mechanism to protect users' privacy by restricting apps from accessing privacy-sensitive resources like GPS, contacts, SMS, location, etc. To access those resources, the developer has to request them by adding the `<uses-permission>` tag in the `AndroidManifest.xml` file [17, 36]. Based on the type of permission, the OS might grant it automatically or prompt the user to allow the request. The different types of permissions are defined by Android according to four protection levels [27, 1]:

- *"normal"*: lower-risk permissions that are automatically granted by the system at installation time;

Category	**Data type**
Location	Approximate location, precise location
Personal info	Name, email address, user IDs, address, phone number, race and ethnicity, political or religious beliefs, sexual orientation, other info
Financial info	User payment info, purchase history, credit score, other financial info
Health and fitness	Health info, fitness info
Messages	Emails, SMS or MMS, other in-app messages
Photos and videos	Photos, videos
Audio files	Voice or sound recordings, music files, other audio file
Files and docs	Files and docs
Calendar	Calendar events
Contacts	Contacts
App activity	App interactions, in-app search history, installed apps, other user-generated content, other actions
Web browsing	Web browsing history
App info and performance	Crash logs, diagnostics, other app performance data
Device or other IDs	Device or other IDs

Table 2.1: Google's categorization of data types [23].

- *"dangerous"*: higher-risk permissions that can give access to resources that could harm the user, therefore the system might ask for confirmation before granting them;

- *"signature"*: the system grants these permissions only if the requesting application is signed with the same certificate as the application that declared the permission;

- *"signatureOrSystem"*: permissions that the system grants only to applications that are in a dedicated folder on the Android system image or that are signed with the same certificate as the application that declared the permission.

2.2 Google privacy guidelines

Google Play is the largest and most accessible market platform for users to download android applications with over 2 million apps [35, 2]. To protect users' privacy, Google Play published the "Privacy, Deception and Device Abuse" document [46], which the developers are required to comply with. According to Google's guidelines, developers should be transparent in how they handle user data by informing the user about the access, collection, use and sharing of the data, and limiting the use of the data to the purposes disclosed [59]. In particular, all developers who published an app on Google Play must complete the "data safety form", a section that describes to the users how the app handles their data. The data safety section includes:

- types of data collected and whether they are optional or required,
- types of data are shared,
- whether the app uses encryption to transfer data,
- whether the user can request to have their data deleted,
- whether the app has committed to following the Play Families Policy,
- whether the app has been independently validated against a global security standard,
- a privacy policy.

To indicate the type of data collected and shared, the developers are asked to use the categorization that Google provides, as shown in Table 2.1. Starting from July 20, 2022, to publish new apps or app updates the developers must complete the data safety form and provide a valid privacy policy and, starting from August 22, 2022, non-compliant apps may face enforcement actions such as the removal of the app's store listing from Google Play [23].

2.3 Privacy regulations

mHealth apps deal with many personal and health data. This kind of sensitive information is protected by regulations to avoid privacy violations. In this thesis we focus on European Union and United States laws, i.e. GDPR and HIPAA.

2.3.1 GDPR

The General Data Protection Regulation (GDPR) was first introduced in 2016 and enforced in May 2018. It regulates the protection of natural persons with regard to the processing of personal data and the free movement of personal data across the European Union. The regulation applies to all natural persons established in the EU, regardless of whether the processing takes place in the Union or not [21, 22].

Personal data GDPR applies when the processing involves information that can be categorized as *personal data*. Personal data is defined as *"any information relating to an identified or identifiable natural person"* meaning that an individual is distinguishable from others by means of that information [18].

GDPR subjects There are four different types of subjects considered by this regulation. These are the *data subject*, the natural person to whom the data relates; the *data controller*, the individual or company that decides the purposes and means of the processing; the *data processor*, the person or company that processes the data on behalf of the controller; and the *data protection officer*, who ensures that the processing is compliant to the rules [21].

GDPR principles GDPR is based on seven principles that represent guidelines to ensure the protection of data [21]:

- *Lawfulness, fairness and transparency*: the processing should be fair, the user should be informed about its details and there has to be at least one legal basis for it. The legal basis for processing can be based on consent, contract, legal obligation, vital interests, public task, or legitimate interests. If the legal basis is user consent, it must be freely given, specific, informed and evidenced by clear affirmative action.

- *Purpose limitation*: data should only be processed according to a specific purpose.

- *Data minimization*: only the minimum data needed to meet the purpose should be processed.
- *Accuracy*: data should be accurate and up to date.
- *Storage limitation*: data should be retained no longer than needed).
- *Integrity and confidentiality*: appropriate technical or organizational measures should be used to keep the data secure, protecting them against unauthorized or unlawful processing and against accidental loss, destruction or damage.
- *Accountability*: the controller should be responsible for compliance with the principles [21, 22].

Data subject rights Under GDPR, the data subject has the right to be informed about the processing, to access the data being processed, to rectify the incorrect data, to have their data erased, to restrict the processing, to object to the processing, to appeal against automated decision making and profiling and to data portability [21].

2.3.2 HIPAA

Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a United States law that establishes standards for the protection of sensitive patient health information [31]. It sets up safeguards to protect the privacy of protected health information and limits the disclosure of these data without the user's consent. The rule is composed of four parts [56]: the privacy rule, the security rule, the breach notification rule and the enforcement rule. HIPAA applies to the so-called *covered entities* [56], which include health plans, healthcare clearinghouses and all health care provider who transmits electronic health information.

Protected Health Information Protected Health Information (PHI) includes all the *individually identifiable health information*, which is data that can be used to identify an individual and relates to:

- the individuals past, present or future physical or mental health or condition,

- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual.

HIPAA does not put any restrictions on data that neither identifies nor provides a reasonable basis to identify an individual (de-identified health information) [56, 32].

HIPAA privacy rule The HIPAA privacy rule aims to protect the privacy of PHI by limiting the circumstances in which it can be used or disclosed by the covered entities, while at the same time allowing the flow of health information to safeguard the individual's health [32, 56]. In addition to establishing the conditions that have to be met in order to share PHI, the privacy rule also requires the covered entities to use, disclose and request only the minimum amount of PHI needed to accomplish the intended purpose (i.e., *minimum necessary* principle).

Covered entities are also required to use the appropriate measures 1) to prevent intentional or unintentional use or disclosure of PHI, 2) to have a procedure for individuals to lodge a complaint and to provide a privacy policy describing the ways in which PHI may be used or disclosed and 4) the rights that the individuals can exercise. Moreover, except in case of emergency, they should obtain the patient's acknowledgment of receipt of the privacy policy [56].

Individuals rights Under the HIPAA privacy rule, the individuals have the following rights [56]:

- *access*: individuals can request a copy of their PHI;
- *amendment*: individuals have the right to rectify inaccurate or incomplete PHI;
- *disclosure accounting*: individuals have a right to an accounting of the disclosures of their PHI except for special cases;
- *restriction*: individuals have the right to request to restrict the use or disclosure of PHI;
- *confidential communication requirements*: covered entities must provide the possibility to request a different means for receiving communications.

HIPAA security rule HIPAA security rule applies to *electronic protected health information* (e-PHI) and it requires all the covered entities to ensure the confidentiality, integrity and availability of all e-PHI; detect and safeguard against anticipated threats to the security of the information; protect against anticipated impermissible uses or disclosures that are not allowed by the rule; certify compliance by their workforce [31].

3

Dataset and methodology

This chapter describes our selection and categorization of Android mHealth apps and the methodology used to analyze them.

The steps that we followed are depicted in Figure 3.1, which consists of three main phases. Phase Ⓐ corresponds to the extraction of the data that we can find on Google Play, namely the apps, the privacy policies and the data safety sections. This phase also includes the categorization of the apps based on their functionalities. In phase Ⓑ, we set up the environment to collect other datasets on which we conduct a preliminary analysis, while in phase Ⓒ we conclude the assessment by using the results of the previous stages to perform comparisons and further inspect mHealth apps.

3.1 Data extraction

This section corresponds to phase Ⓐ of Figure 3.1. It describes the app selection, in which we downloaded 199 mHealth Android apps from Google Play, followed by their functionalities' categorization. Lastly, it illustrates the other data that we gathered in order to be able to proceed with the actual analysis.

3.1.1 App selection

To conduct our analysis, we searched in Google Play for the categories "Medical" and "Health and fitness" by typing the following URLs:

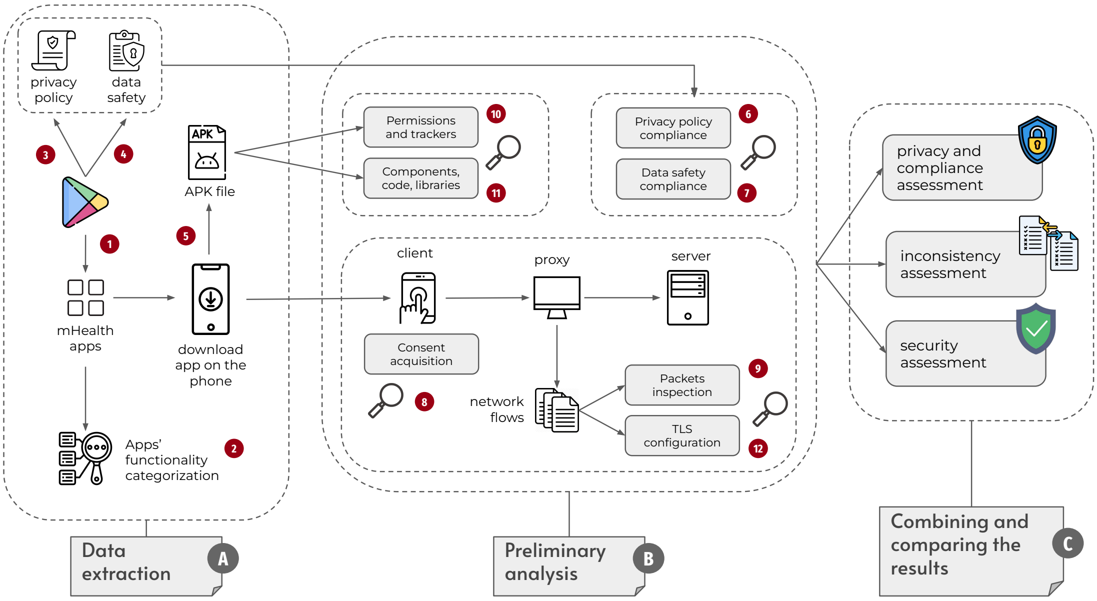


Figure 3.1: Analysis methodology pipeline.

- `https://play.google.com/store/apps/category/HEALTH_AND_FITNESS`
- `https://play.google.com/store/apps/category/MEDICAL`

For each category, Google Play shows the list of the top 45 free and top 45 grossing apps. By changing the `gl` parameter in the URL, we were able to display these chart for different countries. Therefore, we selected the top 45 free and grossing apps of USA and Italy, for both "Medical" and "Health and fitness" categories. The last step was removing the duplicates, the apps that required payment and the ones that were not available for our device, yielding a total of 199 apps (step 1 in Figure 3.1). The collection phase was carried out between October and November 2022. The apps that we selected are the most popular ones available in Google Play, with a mean number of more than 8 million downloads per app in total, meaning that privacy violations would impact a huge number of users.

3.1.2 App Functionality Categorization

The developers can choose to assign a category to their app among the ones available on Google Play. The "Medical" category is described by Google as containing apps related to "*Drug and clinical references, calculators, handbooks for healthcare providers, medical journals and news*", while the apps in "Health and fitness" should be about "*Personal fitness, workout tracking, diet and nutritional tips,* *health and safety*" [9]. We noticed that these categories are broad and may not always be efficient to communicate the app functionalities to the user. Moreover, we observed that the "Medical" and "Health and fitness" sections may overlap. For example, "My Calendar Period Tracker" [41] belongs to the "Medical" category but it offers similar functionalities to "Flo Ovulation & Period Tracker" [19], which is instead under the "Health and fitness" category. To overcome this issue and to be able to correlate the results with the app functionality, we define additional sub-categories to further divide the apps based on their functionalities:

- *Personal Health Record (PHR) Management and Appointments*. These apps allow the user to find doctors, schedule appointments, view visit details, access lab reports and medical health reports, connect with healthcare portals and similar actions.

- *Consultation*. These apps require the users to input their personal information and provide personalized advice on a certain topic. It can be about personalized workouts or diets, medical advice, psychological help, advice to adopt healthy habits, or about the menstrual cycle and getting pregnant. Most of these apps can record other personal information such as weight and height, food and calories consumed during the day, water drunk, symptoms and mood experienced within the day, etc. to log the progress over time.

- *Activity Trackers*. These apps allow the user to track various activities such as running, walking, sleeping, riding, etc. Some of them also provide an option to add the records of an activity manually instead of tracking it through the built-in sensors.

  The main difference from the consultation apps is that with the latter it is usually not possible to record the activity while it is happening: the users have to manually enter the data they want to track.

- *Patient Trackers*. These apps are similar to activity trackers but they are related to medical measurements such as blood pressure, body temperature and heart rate.

- *Treatments and Drug Guide*. These apps are related to the treatment of certain symptoms or diseases. They can also give the users advice about the medications and treatments to follow as well as function as a diary in which the users can log important information about their disease or condition.

- *Medical reference and education*. This subcategory contains apps that are meant to help students and medical personnel in their job. They can be medical guides, drug lookup databases, simulations of real case scenarios, or quizzes and exercises for students.
- *Purchasing Medications*. Purchasing Medications apps allow users to search for pharmacies, drugs and stores, or to make purchases or orders online.
- *Disability Assistance*. The goal of these apps is to assist users with a certain disability. They are used together with an external device other than the smartphone.
- *Covid*. These apps include contact tracing and similar apps developed to fight the Covid-19 pandemic.
- *Emergencies*. These apps notify users about emergencies occurring near them or if the user is in danger, automatically send their position to emergency services. They also allow to storage of personal data and contacts that the rescuers might need.

Finally, one of the apps, "Body Editor Photo Editor" [7], does not fall under any of the mentioned subcategories, since it is a photo editor in which users can modify their bodies to look fitter and healthier.

Overall, the app dataset contains 199 apps, of which 109 belong to the Medical category and 90 to Health and Fitness. The functionality distribution is given in Table 3.1. In the end, we have 50 apps in Consultation, 41 in Activity Trackers, 39 in PHR management and appointments, 31 in Medical reference and education, 10 in Treatments and Drug Guide, 9 in Patient Tracking, 8 in Purchasing Medications, 5 in Covid, 3 in Disability Assistance, 2 in Emergencies and 1 in Body Photo Editor.

This categorization corresponds to step 2 of Figure 3.1.

3.1.3 Data collection

From the 199 mHealth apps that we collected, we extracted further information to conduct our analysis. As also depicted in Figure 3.1, we continued our analysis with the following steps:

Subcategory	**Apps %**	**Category distribution**	
		Medical	Health & Fitness
Consultation	20.1% (50/199)	7	43
Activity Trackers	17.1% (41/199)	4	37
PHR Management and Appointments	16.4% (39/199)	36	3
Medical Reference and Education	13.5% (31/207)	31	0
Treatments and Drug Guide	4.78% (10/199)	10	0
Patient Tracking	4.33% (9/199)	4	5
Purchasing Medications	3.86% (8/199)	8	0
Covid	2.45% (5/199)	5	0
Disability Assistance	1.49% (3/199)	3	0
Emergencies	0.995% (2/199)	1	1
Body Photo Editor	0.5% (1/199)	0	1
Total	**100% (199)**	**109**	**90**

Table 3.1: Subcategories distribution across the collected apps.

- (③) *Privacy Policy Extraction:* We first checked each app's Google Play link for the privacy policy. If we cannot find it there, we search for it within the app. We were able to collect the privacy policy of all the mHealth apps except for 5 of them, which either did not provide one or provided a broken link.
- (④) *Data Safety Extraction:* We extracted the information contained in the Google Play data safety section for 184 apps out of 199 (the remaining 15 did not provide it). This includes information about the collected and shared data, the use of encryption, the possibility to delete the data and the developer's privacy policy.
- (⑤) *APK Extraction:* We downloaded all the APKs from the Google Play store either using `googleplay` [24] or by extracting the APK file from the phone.

3.2 Methodology

In this section, we present the methodology used to analyze mHealth apps. Our goal is to assess the privacy and security of mHealth Android applications through the stages depicted in Figure 3.1. For the steps requiring a phone, we used a rooted Pixel 4 running Android 13, along with a Google account created for this experiment. A rooted phone allows us to obtain privileged control over the device and perform actions with administrator-level permissions. We fist started with a preliminary analysis (phase Ⓑ) and then compared and discussed the results obtained in the different areas (phase Ⓒ).

In the rest of the section, we further explain the details of the analysis methodology we followed for phase Ⓑ.

3.2.1 Privacy Policy

(⑥) In this step, we manually inspected each app's privacy policy page by examining how they address the aspects required by the regulations. In particular, we checked if the privacy policy page contains information about the type of data collected, the purposes of the data collected, the recipients of data, the user rights and the data protection measures. Another important aspect of the privacy policy is to provide a contact for the user to lodge a complaint.

Finally, we checked if the policy considers the case in which the data belongs to minors.

3.2.2 Data Safety Section

(❼) All the apps are required by Google to fill out the data safety form [23]. In this step, we analyze the data safety section of the apps to understand whether the developers disclose the required information about the collected data, data sharing, the use of encryption, the possibility to delete data and the link to the privacy policy.

3.2.3 Consent Acquisition

(❽) Each app should obtain explicit user consent before processing data, as this is required by both HIPAA and GDPR. Under HIPAA, a covered entity *"must obtain the individuals written authorization for any use or disclosure of PHI"* [56]. GDPR defines consent as *"any freely given, specific, informed and unambiguous indication of the data subjects wishes"*, which must be a *"clear affirmative action"* with which the user agrees to the processing of their personal data [6].

To understand if mHealth apps comply with this, we installed and opened each of them to see whether it is necessary or not to click on a button to agree before proceeding to the services.

3.2.4 Network Traffic

(❾) The network traffic of the apps can contain very useful information regarding the collected and shared data. To analyze it, we intercepted each request made by the apps with `mitmproxy` [39], which is an interactive HTTPS proxy that gives us a Man In The Middle (MITM) position. To be able to see the traffic in cleartext, we registered `mitmproxy` as a trusted Certificate Authority with the device, so that it could generate interception certificates on the fly. With this setup, we started each app and granted all the permission requested. When possible, we logged in or created a new account by providing all the information needed. Finally, we browsed the app for a few minutes and tried as many functionalities as possible. The recorded traffic was saved locally for further analysis. We did not automatically run the apps to make sure we knew what data was given in input to them (email address, name, health data, etc.) and that all the viable UI paths were covered.

The network traffic was successfully captured for 124 mHealth apps, while the remaining 75 detected the inspection environment or required specific and sensitive personal information to work, which we were not able to provide. After capturing the network flows, we scanned each packet sent by the apps searching for personal data and PHI. We looked in each HTTP packet's query string and body for values that we knew in advance, such as device information (e.g., identifiers, device's location, IP address), or health and personal information that we entered while testing the app. In particular, the data that we tried to match are:

- Device unique identifiers, such as International Mobile Equipment Identity (IMEI), Android Advertising ID (AAID), Unique Device Identifier (UDID), Google Services Framework ID (GSF ID), Android Device ID and Device Build Fingerprints;
- Location and online identifiers: latitude, longitude and IP address;
- Personal information, which includes first name, last name, email, phone number, username, password and address;
- Data that we entered during the testing, in particular personal health-related information, drug and disease information, blood type, weight, height and diet information.

We also considered simple transformations of these strings, such as MD5, SHA-1 and Base64 encoding.

Next, we are interested in identifying to which domains mHealth apps send personal data and PHI and, in particular, if they belong to a tracker company. To this end, for each web server encountered in the network analysis, we selected the root domain and used `exodus` [16] to detect if it is among the known trackers. This analysis only reveals the well-known trackers, so we were not able to classify the ones not included in the `exodus` list.

3.2.5 Permissions and Trackers

(10) A pervasive presence of permissions and trackers in the app may contribute to privacy threats. Through permissions, in particular the dangerous

ones, the app can access sensitive resources that could hinder users' privacy. Similarly, the app may send sensitive data to tracker companies without the users knowing. The analysis of permissions and trackers was performed using `exodus` [16].

3.2.6 Vulnerability Analysis

(11) This step consists of a static analysis of the APK files in order to identify potential vulnerabilities. To this purpose, we used the APK dataset defined in Section 3.1.3 as input to Mobile Security Framework (`MobSF`) [40], which is one of the most complete and up-to-date analysis tools. Additionally, we used `drozer` [15] to further analyze some potential issues, since it allows us to interact with the app's components.

3.2.7 Network Security Analysis

(12) In this last step, we assessed the security level of the webservers to which mHealth apps are sending personal data and PHI. For this, we used `SSL Labs`' online sever test [54], which is a free assessment tool to check SSL server configurations. The tool inspects the certificate, the protocol support, the key exchange and the cipher strength; then it gives a score to the configuration based on the features found [53].

4 Results

This chapter summarizes the results that we obtained after the steps described in the previous one. Section 4.1 illustrates the privacy and compliance assessment, which is carried out by analysing the outcomes of the steps in Section 3.2. Section 4.2 compares the results to detect potential inconsistencies, while Section 4.3 gives a description of the security assessment of our dataset of mHealth apps.

4.1 Privacy and Compliance Assessment

In this section, we present the results of our privacy and compliance analysis of mHealth Android apps. In the following sub-sections we follow the same steps that we described in Section 3.2.

4.1.1 Privacy Policy

Most of the apps in our dataset have a privacy policy located in Google Play or within the app itself, while we were not able to find it only for 5 apps. The analysis of the available privacy policies was carried out by considering the requirements of both GDPR and HIPAA, in particular by answering the following research questions:

- *Q1:* Does the policy mention the kinds of data processed by the app and for which purposes?

- *Q2:* When do the apps share data with third parties, does the policy mention the recipients of the data?
- *Q3:* Does the policy inform the users about their rights?
- *Q4:* Does the policy talk about the security measures taken for protecting the data?
- *Q5:* Does the policy provide the contact information to file a complaint?
- *Q6:* Does the policy address the case in which the processing concerns data belonging to children?

Results of Q1&Q2: Out of 194 apps with a privacy policy, only 12 do not mention the data types and 9 of them do not specify the purpose of the processing. Regarding data sharing, 152 apps claim that they will share user information with third parties; however, 97 of them do not disclose the recipients of the data even though this is required under both GDPR and HIPAA. Furthermore, among the apps that disclose the recipients, 42 of them do not explicitly name third parties, meaning that they refer to "healthcare providers" or "service providers and advisors" or others, but they do not mention who these actually are.

Results of Q3: The privacy policy should inform the users about the rights they have under the rule that the app complies with. Our analysis reveals that 50 apps fail to include user rights in their privacy policy. Interestingly, we also found that 38 apps only mention the rights of the Californian or the EU users despite the fact that we ran all the apps in another state. Under both GDPR and HIPAA, the subject has the right to withdraw the authorization or consent and, under both rules, the user must be informed about this right before giving consent [58]. Our analysis shows that 101 apps do not mention this in their policy, 20 apps only mention it related to EU data subjects and three apps only in relation to Californian users. Another right that should be present under both GDPR and HIPAA is the right to rectification or amendment [58]. Among the apps in our dataset, we identified 41 of them that do not mention it and 22 that only mention it for EU or Californian users.

Results of Q4&Q5: Both GDPR and HIPAA require the processor or the covered entities to protect the security of the personal data being processed. 159

apps in fact include in their policy a section about the measures taken to secure the data. Another requirement is to offer a way for individuals to lodge a complaint and, according to our evaluation, all of the apps except 3 provide contact information to do so.

Results of Q6: A special case of data processing is when it involves personal data or PHI belonging to minors. Recital 38 of GDPR [48] states that *"children merit specific protection with regard to their personal data as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data"*. HIPAA allows the parents to be the personal representatives of their children and to exercise individual rights on their behalf, even though there are exceptional cases in which parents are not allowed to do so [56]. Thus, we investigated whether or not the privacy policies mention how the data belonging to children is being processed. We found that 69 apps do not say anything about minors in their privacy policy, while 7 of them only recommend the user not to use their services if they are minors or under a certain age.

Takeaway-1. The results of our privacy policy analysis show that 98% of mHealth apps' policies provide a way to file a complaint, 94% disclose the data types collected and 79% of them mention a way to secure the data. However, a significant number of privacy policies fail to name the recipients of the data they share, properly disclose the user rights and offer information on the data processing involving minors. In total, 170 apps (85.4%) have at least one missing requirement in their privacy policy.

4.1.2 Data Safety Section

Even though it is required by Google, 16 apps out of 199 do not display any information in the data safety section. Among the remaining ones, three of them provide a broken link to the privacy policy and 10 of them do not include all the details required by Google.

4.1.3 Consent

Explicit user consent is required under both GDPR and HIPAA before processing personal data. In addition, under GDPR, it should be verifiable and

PHI	Trackers	Others	Domains #
AAID	✓	✓	65
Device build fingerprints	✓	✓	31
Email	✓	✓	53
First name	✓	✓	65
Last name	✓	✓	41
Username	✓	✓	12
Password	✓	✓	29
Phone number	✓	✓	3
Address		✓	3
Longitude	✓	✓	37
Latitude	✓	✓	37
Personal health info	✓	✓	51
Drug info	✓	✓	4
Personal notes		✓	3
IP address	✓	✓	4
Logged food	✓	✓	2
udid		✓	1
IMEI		✓	1

Table 4.1: PHI and personal data detected during network analysis along with the types and number of domains to which they are sent to.

evidenced by a clear affirmative action [56, 22]. We found that only 61 apps ask the user to check a box to obtain consent before proceeding, while 95 apps provide a way for accessing the privacy policy page, but they do not require the user to actually read it or accept it before continuing. We did not find any link to view the privacy conditions within 16 of the apps. The remaining 27 either did not work on rooted devices, or crashed, or we could not get to the point at which the privacy policy should be prompted.

4.1.4 Network Traffic

Network traffic analysis can have many useful implications regarding users' data privacy: it can give insights about the data shared with third-party domains, the trackers used and the other recipients of the shared data.

Table 4.1 shows the PHI and personal data detected during network analysis

Domain	App #	Domain	App #
crashlytics.com	72	appsflyer.com	25
facebook.com	58	amazonaws.com	20
doubleclick.net	49	amplitude.com	20
googleadservices.com	35	adjust.com	18
googletagservices.com	27	google-analytics.com	17

Table 4.2: Summary of the 10 most popular trackers found during the network traffic analysis.

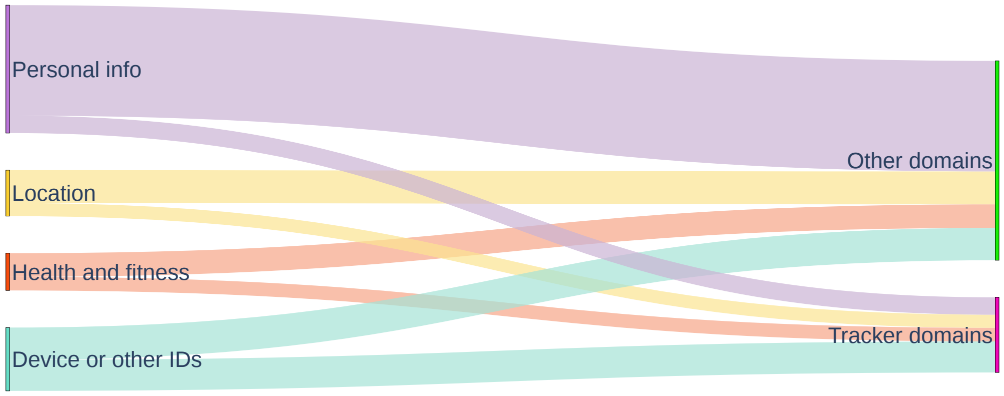


Figure 4.1: Different categories of data detected during the network traffic analysis, along with the domain they are being sent to (tracker domain or other).

along with the types of domains to which they are sent. In total, we detected 14 different types of information being sent over the internet. It is interesting to note that trackers receive many categories of PHI and personal data, including very sensitive ones such as personal health information or password. The 10 most popular tracker domains to which mHealth apps connect are listed in Table 4.2. Most of them are advertisement trackers, while others are used for analytics, profiling and crash reporting purposes.

Our network analysis reveals that at least 46.7% of apps share data with third-party domains, in particular with trackers, although we expect this number to be higher in reality, because `exodus` only covers well-known trackers. Before sharing user data with trackers, apps should obtain explicit consent. However, the majority of them (64 out of 93) do not comply with this requirement.

Figure 4.1 gives an overview of the categories of data detected during the analysis of the network packets. For each of them, it shows the amount of data being shared with tracker domains and with other domains (i.e. the ones that are not well-known trackers according to `exodus`' classification).

Takeaway-2. The results of our network traffic analysis show that PHI and personal data are being transmitted over the Internet. 46.7% of the mHealth apps share user's data with third-party trackers for analytics, profiling and crash reporting purposes. Notably, we observed that 68.8% of them do not ask for explicit consent before sharing the data.

4.1.5 Permissions and Trackers

We first investigated how many permissions the mHealth apps request and how many of them are dangerous. Then, for each dangerous permission, we manually checked if it is related to the functionalities of the app or if there is no obvious reason why it was requested, based on the app's description and screenshots on Google Play. Similarly, we also extracted the trackers for each app using `exodus`.

We identified a total of 165 unique permissions requested by the apps in our dataset, of which 38 are dangerous. The number of permissions, dangerous permissions and trackers for the apps in each subcategory is given in Figure 4.2. Our results show that Activity Tracker apps request the highest number of dangerous permissions, followed by PHR Management and Appointments and Consultation; while the lowest number of dangerous permissions is requested by Patient Tracking, Covid and Emergencies apps. Activity Trackers subcategory also counts the higher number of trackers and permissions in general, compared to the rest of the subcategories.

The most popular dangerous permissions among mHealth apps are `WRITE_EXTERNAL_STORAGE` and `READ_EXTERNAL_STORAGE`, which are mostly requested by the apps that belong to PHR management and appointments, Consultation and Activity Trackers subcategories. These apps may in fact need those permissions to allow the user to export activity reports, lab results and medical records, or to upload documents. Also, `CAMERA` and the location-related permissions are among the most requested ones. Many apps in fact give the user the possibility to scan QR codes, send photos to receive a consultation, make video

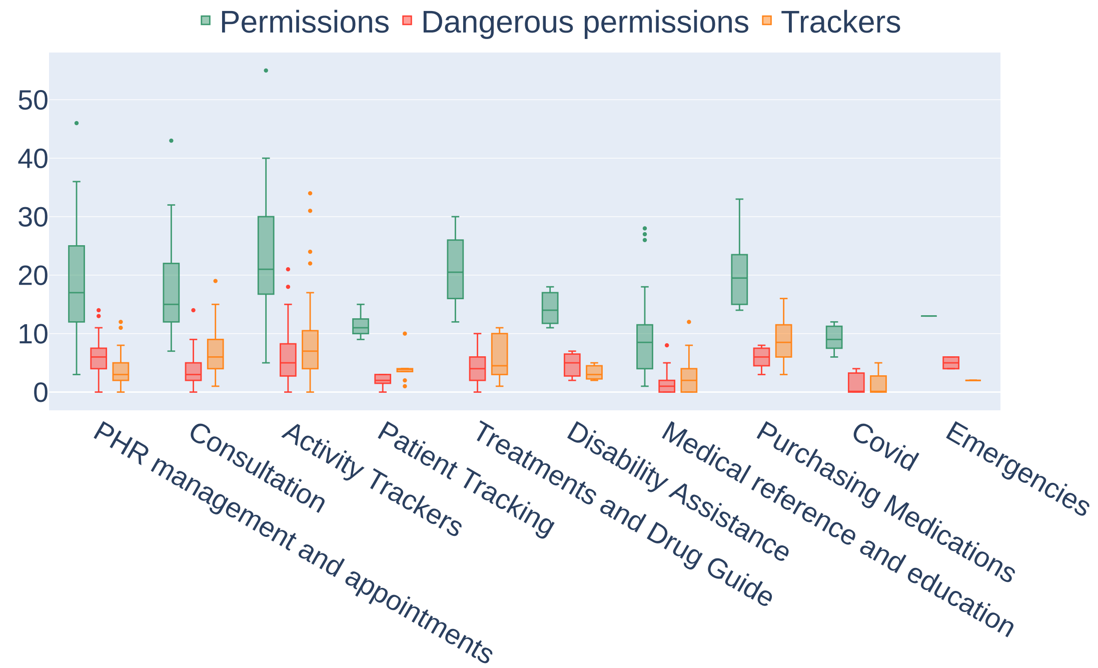


Figure 4.2: The number of permissions, dangerous permissions and trackers for apps in each subcategory in our dataset.

calls with physicians, find doctors or pharmacies based on the location and track the running or biking route.

As one would expect, the most popular permissions used by mHealth apps change according to the functionality. For example, Activity Trackers apps request `ACTIVITY_RECOGNITION` more often, while `ACCESS_FINE_LOCATION` is the most requested by apps in Emergencies and Purchasing Medications. However, not all dangerous permissions are requested for an obvious reason, meaning that in some cases there is no evident relation between the permission and the functionalities that the app offers. For example, an app for managing diabetes offers a logging service to monitor food intake, medications and blood sugar level. You can also log exercise time and view reports, charts and statistics. Based on these kind of functionalities, some of the permissions that the app requests, (i.e. camera and location-related permissions) look unnecessary. Our analysis shows that based on the app's description on Google Play, the dangerous permissions that are requested more often without a clear reason are the ones to write and read from external storage, `CAMERA` (which may be not related to the functionalities but may be used to take a picture for the account), `READ_PHONE_STATE`, `RECORD_AUDIO` and the ones to access the location. This means that the app has access to sensitive resources even though they are not actually necessary, potentially leaking private user data.

Takeaway-3. Our permissions and trackers analysis reveals that mHealth apps typically request an average of 17.6 permissions (of which 4.3 are dangerous) and use 5.7 trackers per app. We found that the most popular permissions are related to the apps' functionalities, with Activity Trackers being the category requesting a higher number of permissions and trackers than other categories. While the dangerous permissions are usually linked to the app's functionalities, in some cases, mHealth apps request permissions that may appear unnecessary.

4.2 Inconsistency Assessment

Ideally, the data processing should be consistent across all relevant sources. Developers should declare that they process the same type of data in both the privacy policy and the data safety section. The app should not request permission related to data that is not mentioned there. Similarly, we should not find in the network traffic data that is not declared there. In this thesis, we have the following four sources for each app: 1) the information provided by the app in Google Play data safety section, 2) the app's privacy policy, 3) its APK source code and 4) its network traffic. In this Section, we compare these different sources to assess whether mHealth apps are consistent across them.

Network Traffic vs. Data Safety For this step, we classify the personal information found during the network analysis according to Google's data types categorization [23] (also shown in Table 2.1) in order to be able to understand whether or not the data detected within the packets were mentioned in the data safety section. The results of this analysis show that some of the apps process categories of personal data and PHI that are not mentioned in Google Play's data safety section. In particular, we identified 60 violations. The most popular types of information processed without informing the user are "Device or other IDs" (34 times), followed by "Personal info" (26 times), "Health and fitness" (22 times) and "Location" (8 times).

Next, we focused on the intention to share user data. We found that 53 mHealth apps share data with third parties even though their data safety section says "No data shared with third parties".

Network Traffic vs. Privacy Policy In this step, we used the aforementioned Google data types categorization to classify the data and compare them to the statements of the privacy policies. In total, we found out that 46 apps send over the Internet PHI and personal data that they do not mention among the categories of processed data in their privacy policy. Moreover, 14 apps share user data with third parties but they do not mention or are not clear about this in their privacy policy.

Overall, our analysis shows that 13 mHealth apps share personal data with third parties without informing the user neither in the privacy policy nor in the data safety section. 72 of them process types of data that are not mentioned in at least one of these sources.

Data Safety vs. Privacy Policy We observed that there are many discrepancies between the statements provided by apps in their privacy policy and the ones they provide in Google Play's data safety section. Particularly, 194 apps out of 199 present inconsistencies. In general, developers provide conflicting information concerning:

- the sharing of personal data;
- the types of personal data being processed;
- the use of encryption;
- the possibility of requesting the erasure of personal information.

Topic	Apps
Types of data processed	94% (187/199)
Sharing of personal data	59.3% (118/199)
Erasure	41.7% (83/199)
Encryption	30.2% (60/199)

Table 4.3: Number of apps having inconsistencies between the privacy policy page and the data safety section.

Table 4.3 summarizes the number of inconsistencies that we found in relation to the aforementioned areas. Our analysis showed that only 5 apps do not have discrepancies at all, while 45 have only 1 discrepancy, 68 have 2 of them, 54 present 3 discrepancies and 27 apps display discordant information in all four areas.

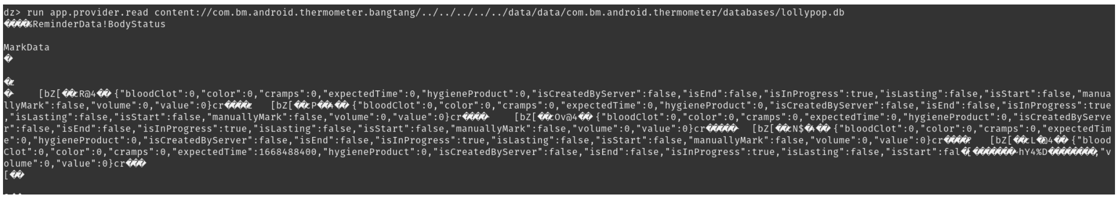
Permissions vs. Privacy Policy An interesting aspect to investigate is whether the privacy policies mention the use of dangerous permissions, or if at least they mention the personal data related to them among the types of processed data. Among the apps in our dataset, only 11 of them explicitly talk about dangerous permissions. However, 108 apps refer to the data accessed by them in the privacy policy and 56 only mention some of the data (not for all dangerous permissions requested). Of the remaining apps, 29 of them do not talk about permissions at all and for 5 of them, we were not able to find a privacy policy page.

	Explicitly	**Among processed data**	**Partially**	**Do not mention**
Privacy Policy	5.56%	49%	28.3%	14.6%
Data Safety	0%	40.6%	31.7%	20.1%

Table 4.4: Percentage of the apps that mention data accessed by the dangerous permissions among the processed ones, in both privacy policy and data safety.

Permissions vs. Data Safety A similar investigation was carried out also for Google Play's data safety section. Table 4.4 shows the results for both the data safety section and the privacy policy page.

Takeaway-4. Our inconsistency analysis reveals that the information that mHealth apps provide about the processing of personal data is often inconsistent across different sources (e.g., privacy policy and data safety section), especially regarding the description of the types of processed data. Moreover, some apps process personal information that they do not mention in the privacy policy or in the data safety section. Finally, we found out that a portion of mHealth apps share data with third parties without informing the user.



```
dz> run app.provider.read content://com.bm.android.thermometer.bangtang/../../../../../data/data/com.bm.android.thermometer/databases/lollypop.db
����%ReminderData!BodyStatus

MarkData
�

�z
�    [bZ[��cR@4�� {"bloodClot":0,"color":0,"cramps":0,"expectedTime":0,"hygieneProduct":0,"isCreatedByServer":false,"isEnd":false,"isInProgress":true,"isLasting":false,"isStart":false,"manua
llyMark":false,"volume":0,"value":0}cr����z   [bZ[��cP��4�� {"bloodClot":0,"color":0,"cramps":0,"expectedTime":0,"hygieneProduct":0,"isCreatedByServer":false,"isEnd":false,"isInProgress":true
,"isLasting":false,"isStart":false,"manuallyMark":false,"volume":0,"value":0}cr����    [bZ[��cOv@4�� {"bloodClot":0,"color":0,"cramps":0,"expectedTime":0,"hygieneProduct":0,"isCreatedByServe
r":false,"isEnd":false,"isInProgress":true,"isLasting":false,"isStart":false,"manuallyMark":false,"volume":0,"value":0}cr�����  [bZ[��cN$�4�� {"bloodClot":0,"color":0,"cramps":0,"expectedTim
e":0,"hygieneProduct":0,"isCreatedByServer":false,"isEnd":false,"isInProgress":true,"isLasting":false,"isStart":false,"manuallyMark":false,"volume":0,"value":0}cr����   [bZ[��cL�4�� {"blood
Clot":0,"color":0,"cramps":0,"expectedTime":1668488400,"hygieneProduct":0,"isCreatedByServer":false,"isEnd":false,"isInProgress":true,"isLasting":false,"isStart":fal�[�������hY4%D��������,"v
olume":0,"value":0}cr���
[��
```

Figure 4.3: Using drozer to verify the exported provider's vulnerability to path traversal.

4.3 Security Assessment

In this section, we present the results obtained after the security assessment of mHealth apps. In particular, Sub-section 4.3.1 illustrates the result of the APK analysis, while Sub-section 4.3.2 discusses the outcomes of the network security inspection.

4.3.1 APK Analysis

The results of the static analysis of the mHealth apps APKs can be broken down into three different areas, described below.

Exported components Component exporting can be dangerous for security if it is not done with proper restrictions. Our static analysis revealed that 191 mHealth apps have at least one exported component. In particular, exported activities were detected in 152 apps, services in 177, receivers in 176 and providers in 25.

Exported activities can allow malicious apps to gain access to internal pages if they are not properly protected with permissions. Similarly, exported services and broadcast receivers can lead respectively to unauthorized access to the functionality that they implement and to broadcast spoofing, if they do not implement any controls. Exported content providers can lead to information leakage, SQL injection, or path traversal attacks, since an external application will be able to query local data [14].

We tested the exported providers against these attacks using `drozer` [15], finding out the one app has an exported content provider that is vulnerable to path traversal. This can cause information leaks, since it allows us to read the app's internal files. As shown in Figure 4.3, we were able to use `drozer` to perform a path traversal attack and read one of the app's private files.

Code vulnerabilities The static analysis with `MobSF` identified many potential issues in the code of mHealth apps such as those related to insufficient cryptography, insecure WebView implementation, SQL injection, insecure implementation of SSL and potential leaking of sensitive information. We found the following potential vulnerabilities:

- *Cryptography:* 15 mHealth apps use encryption algorithms with ECB mode, which is known to be weak, and 80 apps use CBC with PKCS5/PKCS7 padding, which is vulnerable to padding oracle attacks. 11 calls to `Cipher.getInstance("AES")` were detected, which also result in the use of ECB mode and 11 apps use weak encryption algorithms. Moreover, many apps use weak hash functions such as MD5 and SHA-1 (137 and 146 respectively). 177 apps were found to use an insecure random generator, which could lead to security issues if it is used for cryptography or for other critical operations.

- *WebView implementation:* if WebView is not properly used, it can lead to data leaks by exploitation through cross-site scripting [14]. The results of our analysis show that 39 mHealth apps have remote WebView debugging enabled and that 112 apps have an improper implementation of this feature that may cause the execution of user-controlled code in it. Another WebView issue is that 11 apps ignore SSL Certificate errors and accept any SSL Certificate, making the app vulnerable to MITM attacks.

- *SQL injection:* 174 mHealth apps use SQLite Database and execute raw SQL query, which represents a potential threat in case the app puts untrusted user input within the raw query.

- *SSL implementation:* in 22 mHealth apps, `MobSF` detected a MITM vulnerability because SSL is implemented to trust all certificates or accept the self-signed ones.

- *Information leak:* we found that many apps log information, create temp files, copy data to the clipboard and write to the app directory. This can result in information leaks if these operations involve sensitive data. Moreover, 169 apps can read/write to external storage, which can also lead to information leakage since all the apps can read the data on the external storage.

Shared libraries vulnerabilities 4 types of vulnerabilities were found in the shared libraries that mHealth apps use. 16 apps use binaries without stack canaries, which makes them vulnerable to attacks that exploit a stack-based buffer overflow to overwrite the return address of a function and change the program flow. We detected that 4 apps use shared libraries that do not have full RELRO enabled, which means that an attacker may be able to exploit vulnerabilities in the code to overwrite GOT entries and change the program flow. Moreover, 2 mHealth apps have RUNPATH set in the shared object they use and one app has RPATH set. Adversaries can abuse these features for code execution and privilege escalation.

Takeaway-5. Our security analysis detected potential vulnerabilities in mHealth apps' components, code and shared libraries. These could be exploited by malicious apps installed on the same phone. For example, a malicious app running in the background may interact with the exported components, causing an information leakage.

4.3.2 Network Configuration

The captured network traffic was used to identify the domains to which mHealth apps connect and through which protocol. Most of mHealth apps use `https` for their communications. Nevertheless, we detected 84 of them making connections using `http` and, in particular, one using it to send sensitive user data over the internet, such as first name, last name, email and password, which can therefore be seen in cleartext by monitoring the network traffic.

Among 383 unique domains to which the apps connect, 130 of them receive personal data and PHI. For each of them, we tested its SSL configuration using `SSL Labs` [54]. The grades go from A to F (with A+ for exceptional configurations), but it is also possible to get M and T, to indicate a certificate name mismatch or that the site certificate is not trusted, respectively. In the last two cases, the certificate is not trusted, so the other security scores are ignored because attackers can subvert connection security [53].

The results show that the majority of web servers have good SSL configurations, graded with A (43) and B (41). 14 exceptional configurations were detected, with a score of A+. For 19 domains the tool gave us an error and in 5 cases the assessment failed because it was not possible to connect to the server.

One domain did not support any secure protocol, so it could not be analyzed. The remaining 7 webservers got a T grade since the certificate was not trusted, either because of a name mismatch or because it was expired.

Takeaway-6. Although 92.5% of apps use secure protocols to send data, sometimes `http` is used, making it possible for an attacker to eavesdrop on sensitive information. Concerning SSL, most of the domains to which mHealth apps send information have a good configuration, according to the `SSL Labs` tool [54].

5

CDC's Health Care Provider Apps

In this chapter, we analyze eight healthcare provider/clinician apps published on CDC's website [30, 11]. Section 5.1 focuses on privacy and compliance, while Section 5.2 on security.

5.1 Privacy and Compliance Analysis

This section discusses the privacy and compliance findings for CDC mHealth apps. In particular, we describe the results obtained after analyzing their privacy policy and data safety section, the way in which they manage consent acquisition, the network traffic, the permissions declared and the number of trackers that they use.

Privacy Policy and Data Safety Section Although all the CDC apps have privacy policies, the latter is not exhaustive in all the aspects that HIPAA requires to include. Only two apps clearly mention the types of data that they process and only one of them explains for which purposes. Six apps are not clear about data sharing, while two of them do not mention the intention to disclose any information to third parties. Moreover, none of the apps mentions the recipients of the data. Surprisingly, none of the policies informs the users about their rights, and neither do they talk about the security measures taken to protect the data, except for one. However, all the CDC apps provide a contact to lodge a complaint and most of them (7/8) address the case of processing data that belongs to children.

Finally, interestingly, only three of the eight CDC apps comply with Google's requirement to fill in the data safety section, while for the others, we cannot find any information there. Additionally, the ones for which the data safety section is available, provide information that differs from the statements of their privacy policies, in all fields except the one about data erasure.

Consent All the CDC apps have a way of accessing the policy through the app; however, none of them prompts it to the user explicitly requiring them to accept, despite this being a HIPAA requirement.

Network Traffic The packets sent through the internet by CDC apps do not contain PHI except for device identifiers, which 6 apps process without mentioning them either in the privacy policy or in the data safety section. Only two of the CDC apps share data with third parties after informing the users through the privacy policy (but not through the data safety section).

Permissions and Trackers Most of the CDC apps have a low number of permissions, except two of them that request more than 20, including some dangerous ones. As concerns trackers, CDC apps in most cases do not use them or they use just a few (the maximum detected was 3).

5.2 Security analysis

In this section we illustrate the outcome of the security assessment for CDC mHealth apps, after analyzing the APK files and the network security.

As concerns the APK analysis, only 3 CDC apps have exported components. The potential code issues identified are related to improper SSL implementation, execution of raw SQL queries, use of insecure hash functions and possible information leaks. Regarding the network analysis, we detected 3 CDC apps making connections using `http`, while the SSL configurations of the web servers to which they connect were good according to `SSL Labs`, with A and B grades.

Takeaway-7. Our analysis of CDC apps suggests that they do not abuse permissions and that they respect user's privacy by not disclosing sensitive data and not making pervasive use of trackers. On the other hand, they often fail in obtaining the user's consent and in informing them about how their data is handled through the privacy policy and the data safety section.

6

Paid mHealth Apps

In this chapter, we analyze a sample of 25 paid mHealth apps to understand the differences (if any) between them and the free ones. Section 6.1 describes our results regarding privacy and compliance, while we discuss the security of paid apps in Section 6.2.

6.1 Privacy and Compliance Analysis

In this section we assess the privacy and compliance of paid mHealth apps, by considering their privacy policy, data safety section, the way in which they handle consent acquisition, the data that we detected in the network traffic, the permissions declared and the number of trackers that they use.

Privacy Policy and Data Safety Section The majority of paid apps (88%) provide the users with a privacy policy page, while for the remaining 3 apps (12%) we were not able to find it in Google Play or within the app itself. The data safety section of every app in our sample is complete except for 3 of them. However, 38.9% of them do not include every aspect required by Google. Among the apps that have a privacy policy, our results show that almost all of them inform the users about which data are being processed and for which purposes. As concerns the sharing of personal data, 35.3% of paid apps do not disclose the recipients of data when they claim to share them with third parties.

Our analysis reveals that most paid mHealth apps fail in informing the users about their rights, in fact only 18.5% of them include user rights in their privacy policy and one app only does it for EU users. On the other hand, the majority of paid apps' privacy policies talk about the security measures taken to ensure the protection of the user data: only 21.4% (6/22) of them do not mention this aspect. They also overall succeed in giving contact information, only 4 policies do not provide it. Lastly, many of the paid apps (38.9%) do not address the case of processing data that belongs to minors. Overall, 88% of the paid apps (22/25) have at least one missing requirement in their privacy policy.

The privacy policy page and the data safety section should contain consistent information about data processing. Nevertheless, the vast majority of paid apps are not consistent between these two sources: only one app does not present discrepancies.

Consent Paid mHealth apps are not particularly careful in obtaining the user's explicit consent before processing their data: only 24% of them (6/25) require the user to click on the "accept" button before using the services. 28% of the apps (7/25) provide the privacy policy to the user but does not require them to explicitly accept, while the remaining ones (48%) do not even give the possibility to check the privacy policy from the app.

Network Traffic The analysis of the network packets reveals that paid mHealth apps send personal data and PHI over the internet, including personal health information, AAID, password, first name, email, device build fingerprints, username, last name. personal notes, latitude, longitude, udid and IMEI. Among these data, we detected that only AAID, device build fingerprints and first name are being sent to third party tracker companies. Among the apps that share data with trackers, 5 of them do not obtain the user's explicit consent, despite this being required by the privacy rules. Moreover, paid apps do not always inform the user about their intention to share data with third parties. We found out that two apps share user's data with trackers even though they do not mention it nor in the privacy policy or in the data safety section.

All the categories of data that we detected in the network traffic should be mentioned among the data that the app processes. However, 68% (17/25) of the paid apps process data that they do not mention in the privacy policy and 84% (21/25) apps do not include in the data safety section some types of data that they actually process. The categories that paid apps do not mention more often are "Health and fitness", "Device or other IDs", "Personal info" and "Location".

Permissions and Trackers The permissions analysis identified 60 unique permissions requested by paid mHealth apps, among which 13 are labelled as dangerous. As concerns the dangerous ones, the most requested by paid apps are `WRITE_EXTERNAL_STORAGE`, `READ_EXTERNAL_STORAGE` and `CAMERA`, similarly to the free apps. Both the numbers of total permissions and dangerous permissions requested by paid apps are lower with respect to free apps. Our analysis detected a lower number of trackers in paid apps as well, with a mean of 2.24 trackers per app, compared to the 5.55 per app for the free ones.

6.2 Security Analysis

This section discusses the security of paid mHealth apps, by analyzing the APK files and the security of the apps' network configuration.

APK analysis The APK analysis detected that many paid mHealth apps have their components exported, leaving them accessible to other apps. In particular 19 apps have at least one exported component.

We found some potential vulnerabilities in the paid apps' code. They concern cryptography (weak or vulnerable configurations of encryption algorithms), WebView or SSL improper configurations, potential SQL injection and information leaks (potentially originating from hard-coded sensitive information, temporary files and capability to read or write to the external storage).

Network Configuration The network traffic analysis results show that although in most of the cases paid mHealth apps make connections using `https` protocol, 15 of them sometimes use `http`, sending therefore data with no encryption.

The SSL configurations of the domains to which paid apps send data are overall good according to `SSL Labs`, with the majority of grades being B.

Takeaway-8. Our analysis suggests that paid apps are worse than free ones in complying with the requirements to have a privacy policy, a data safety section and to obtain explicit consent before processing data. For example, 57.5% of free apps do not ask for explicit consent, while this raises to 76% for paid apps. Conversely, paid mHealth apps request on average a lower number of total and dangerous permissions and they make use of fewer trackers compared to free apps. The amount of data that they share with trackers is lower as well, both in terms of categories of data and the number of apps that shares them. Only 32% of paid apps shares data with trackers, compared to the 45.9% of free ones. Nevertheless, the fraction of apps that share data without informing the user is higher in paid apps than in free ones, as well as the percentage of apps that process categories of data not mentioned in the privacy policy or in the data safety section. Concerning security, we found similar issues and vulnerabilities in both paid and free apps.

7

Limitations

This chapter illustrates the limitations of our work, which concern the following phases of the analysis:

- **Login and App Usage**. To collect the network traffic of mHealth apps, we downloaded them on the phone and interacted with them for a few minutes, trying to perform a login (if available) and access as many functionalities as possible. However, we were not always able to access all the features; for example, we could not perform payment actions or actually reserve an appointment with a doctor. For some apps, we could not even sign up, since they required specific information like Social Security Number (SSN), or we needed a special link or code to create an account. Moreover, some apps detected that the phone was rooted and did not start, while other apps identified the interceptor proxy and did not connect to the internet, making it impossible to capture the network traffic. For this reason, our analysis may have missed some of the data that mHealth apps send, since they may be sent when using functionalities that we could not access, or when the app is used for a long time, which we could not do.
- **Network Traffic Analysis**. To inspect all the packets sent over the internet in a reasonable time, we used an automatic approach to look for known strings inside the packet body or in the HTTP query string. The strings that we found correspond therefore only to a subset of the PHI and personal data that mHealth apps send, since we may have missed other sensitive information that is not related to something that we input ourselves in the

app or that we know in advance (such as device IDs). This method may also generate some false positives, in the cases in which the data that we input in the app is sent over the internet but not in relation to our personal information (for example the word "allergy" can be given as input to some mHealth apps but can also be related to internal functionalities).

Another limitation of the network traffic analysis is the identification of tracking domains. We considered the well-known tracker list that `exodus` provides and classified the domains based on their presence on the list, while we were not able to collocate the ones that are not there. Moreover, we assumed that apps share information with third parties only when they share it with tracker domains because we do not know the nature of the other domains (first party or third party). Therefore, we may have missed some cases of data sharing with third parties without the user being informed.

8 Related work

Security and privacy of mobile applications. Many studies in the literature inspect mobile applications focusing on both privacy issues and security risks.

Harper et al. [26] analyzed animals-related Android apps to understand whether they can put users at risk. Kumar et al. [35] investigated geo-differences in mobile apps and how they affect the security and privacy of users in different regions. Many researchers looked into privacy issues of mobile apps. Some of them mostly focused on permissions analysis [20, 27], while others aimed at analyzing privacy policies to understand how many apps actually provide them, evaluate compliance and detect inconsistencies [60, 4, 55, 44]. An important matter in mobile apps' privacy is to understand whether the app behavior is actually consistent with the statements of the privacy policy: many studies addressed this problem by proposing automatic approaches to detect such violations [5, 61, 52, 12, 36, 8]. Kollnig et al. [33] conducted a privacy analysis mainly focused on the lack of consent to third-party tracking. Violations of consent are also discussed in other studies [43, 44] and third-party tracking in mobile apps is also investigated by Razaghpanah et al. [47], that proposed a method to detect advertising and tracking domains and evaluate the impact that privacy regulations have on them. Kollnig et. al [34] compared Android and iOS mobile applications focusing on privacy and compliance aspects.

Security and privacy of mHealth applications. As concerns mHealth apps, many papers perform an analysis of privacy policy, permissions, apk and network traffic, also focusing on compliance with the privacy rules [45, 62, 3]. Hatamian et al. conducted a similar study considering COVID-19 contact tracing apps [28], while Gruber et al. [25] focused on mobile childcare applications. Other studies focused on security vulnerabilities and possible attack surfaces of mHealth apps that could in turn lead to privacy leaks [29, 10]. Another study addresses the security threats of a subset of mHealth apps, i.e. menstruation cycle tracking apps [14].

Our differences. Our work addresses as many aspects as possible to evaluate the privacy, compliance and security of mHealth apps. We consider not only USA and EU privacy regulations, but also Google's requirements. In addition to privacy policies, we analyze Google Play's data safety sections, comparing these two sources of information that should be ideally consistent with each other. Our study focuses on different types of mHealth apps: on top of the most popular free ones, we also include paid and CDC-endorsed mHealth apps, comparing the results and highlighting the differences that we find.

9

Conclusion

In this work, we investigated the privacy and security of mHealth applications in the Android ecosystem. mHealth area has been growing in the last few years and has brought many advantages and benefits to the users. However these apps deal with a lot of sensitive data, so it is important that they respect users' privacy by following security best practices and privacy regulations. After the analysis, we found out that mHealth apps are not very efficient and clear in informing users about the processing of their data. Many of them have missing details in their privacy policy or in Google Play's data safety section and the policies are not always explicit about certain aspects. Additionally, they often provide information that diverges between the privacy policy and what the developers declare in the data safety section. Our investigation detected some potential violations of the privacy rules, since it often happens that mHealth apps process categories of personal data that are not mentioned in the policy, share sensitive data with third parties without informing the user, or process user data without first obtaining explicit consent (in 71% of cases). mHealth apps can also pose security threats, as we detected connections to the internet without using encryption, usage of vulnerable shared libraries and not proper protection of components, which can lead to potential information leaks.

The results and findings of our study impact a huge number end-users, as the most popular mHealth apps that we consider count more than 8 millions download each, on average. Therefore, our work contributes to emphasize the importance of creating awareness among both users and developers about the significance of privacy while dealing with sensitive health-related data.

References

[1] *<permission>*. URL: `https://developer.android.com/guide/topics/manifest/permission-element`.

[2] Mohammed M Alani and Ali Ismail Awad. "Paired: An explainable lightweight android malware detection system". In: *IEEE Access* 10 (2022), pp. 73214–73228.

[3] Mehrdad Aliasgari, Michael Black, and Nikhil Yadav. "Security vulnerabilities in mobile health applications". In: *2018 IEEE Conference on Application, Information and Network Security (AINS)*. IEEE. 2018, pp. 21–26.

[4] Benjamin Andow et al. "{PolicyLint}: Investigating Internal Privacy Policy Contradictions on Google Play". In: *28th USENIX security symposium (USENIX security 19)*. 2019, pp. 585–602.

[5] Benjamin Andow et al. "Actions Speak Louder than Words: Entity-Sensitive Privacy Policy and Data Flow Analysis with PoliCheck". In: *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, Aug. 2020, pp. 985–1002. ISBN: 978-1-939133-17-5. URL: `https://www.usenix.org/conference/usenixsecurity20/presentation/andow`.

[6] *Art. 4 GDPR*. Accessed: 2023-02-27. 2022. URL: `https://gdpr-info.eu/art-4-gdpr/`.

[7] *Body Editor Photo Editor*. URL: `https://play.google.com/store/apps/details?id=breastenlarger.bodyeditor.photoeditor`.

[8] Duc Bui et al. "Consistency Analysis of Data-Usage Purposes in Mobile Apps". In: *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. 2021, pp. 2824–2843.

[9] *Choose a category and tags for your app or game*. URL: `https://support.google.com/googleplay/android-developer/answer/9859673?hl=en%5C#zippy=%5C%2Capps`.

[10] Y Cifuentes, L Beltrán, and L Ramrez. "Analysis of security vulnerabilities for mobile health applications". In: *International Journal of Health and Medical Engineering* 9.9 (2015), pp. 1067–1072.

[11] *Consumer/General Public Apps*. URL: `https://www.cdc.gov/digital-social-media-tools/mobile/generalconsumerapps.html`.

[12] Andrea Continella et al. "Obfuscation-Resilient Privacy Leak Detection for Mobile Apps Through Differential Analysis." In: *NDSS*. Vol. 17. 2017, pp. 10–14722.

[13] *COVID-19 growth in medical app downloads by country 2020 | Statista*. Accessed: 2023-14-02. 2020. URL: `https://www.statista.com/statistics/1181413/medical-app-downloads-growth-during-covid-pandemic-by-country/`.

[14] Mounika Deverashetti, K Ranjitha, and KV Pradeepthi. "Security analysis of menstruation cycle tracking applications using static, dynamic and machine learning techniques". In: *Journal of Information Security and Applications* 67 (2022), p. 103171.

[15] *drozer*. 2022. URL: `https://github.com/WithSecureLabs/drozer`.

[16] *Exodus Privacy*. URL: `https://exodus-privacy.eu.org/en/`.

[17] Parvez Faruki et al. "Android security: a survey of issues, malware penetration, and defenses". In: *IEEE communications surveys & tutorials* 17.2 (2014), pp. 998–1022.

[18] Michèle Finck and Frank Pallas. "They who must not be identifieddistinguishing personal from non-personal data under the GDPR". In: *International Data Privacy Law* 10.1 (2020), pp. 11–36.

[19] *Flo Ovulation & Period Tracker*. URL: `https://play.google.com/store/apps/details?id=org.iggymedia.periodtracker`.

[20] José Javier Flors-Sidro et al. "Analysis of diabetes apps to assess privacy-related permissions: systematic search of apps". In: *JMIR diabetes* 6.1 (2021), e16146.

[21] *GDPR - User-Friendly Guide to General Data Protection Regulation*. URL: `https://www.gdpreu.org/`.

[22] Michelle Goddard. "The EU General Data Protection Regulation (GDPR): European regulation that has a global impact". In: *International Journal of Market Research* 59.6 (2017), pp. 703–705.

[23] *Google Play's Data safety section*. URL: %5Curl%7Bhttps://support.google.com/googleplay/android-developer/answer/10787469?hl=en%5C#zippy=%5C%2Cdata-types%7D.

[24] *googleplay*. URL: https://github.com/89z/googleplay.

[25] Moritz Gruber et al. "We may share the number of diaper changes: A Privacy and Security Analysis of Mobile Child Care Applications". In: *Proceedings on Privacy Enhancing Technologies* 3 (2022), pp. 394–414.

[26] Scott Harper, Naryam Mehrnezhad, and Matthew Leach. "Are Our Animals Leaking Information About Us? Security and Privacy Evaluation of Animal-related Apps". In: *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE. 2022, pp. 38–51.

[27] Majid Hatamian et al. "A Multilateral Privacy Impact Analysis Method for Android Apps". In: *Privacy Technologies and Policy*. Ed. by Maurizio Naldi et al. Cham: Springer International Publishing, 2019, pp. 87–106. ISBN: 978-3-030-21752-5.

[28] Majid Hatamian et al. "A privacy and security analysis of early-deployed COVID-19 contact tracing Android apps". In: *Empirical software engineering* 26.3 (2021), pp. 1–51.

[29] Dongjing He et al. "Security concerns in Android mHealth apps". In: *AMIA annual symposium proceedings*. Vol. 2014. American Medical Informatics Association. 2014, p. 645.

[30] *Health Care Provider/Clinician Apps*. URL: https://www.cdc.gov/digital-social-media-tools/mobile/healthcareproviderapps.html.

[31] *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*. URL: https://www.cdc.gov/phlp/publications/topic/hipaa.html.

[32] A Jayanthilladevi, K Sangeetha, and E Balamurugan. "Healthcare Biometrics Security and Regulations: Biometrics Data Security and Regulations Governing PHI and HIPAA Act for Patient Privacy". In: *2020 International Conference on Emerging Smart Computing and Informatics (ESCI)*. IEEE. 2020, pp. 244–247.

[33] Konrad Kollnig et al. “A Fait Accompli? An Empirical Study into the Absence of Consent to Third-Party Tracking in Android Apps”. In: *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. USENIX Association, Aug. 2021, pp. 181–196. ISBN: 978-1-939133-25-0. URL: `https://www.usenix.org/conference/soups2021/presentation/kollnig`.

[34] Konrad Kollnig et al. “Are iPhones Really Better for Privacy? Comparative Study of iOS and Android Apps”. In: *arXiv preprint arXiv:2109.13722* (2021).

[35] Renuka Kumar et al. “A Large-scale Investigation into Geodifferences in Mobile Apps”. In: *31st USENIX Security Symposium (USENIX Security 22)*. Boston, MA: USENIX Association, Aug. 2022, pp. 1203–1220. ISBN: 978-1-939133-31-1. URL: `https://www.usenix.org/conference/usenixsecurity22/presentation/kumar`.

[36] Qian Luo et al. “Automatic Detection for Privacy Violations in Android Applications”. In: *IEEE Internet of Things Journal* 9.8 (2022), pp. 6159–6172. DOI: `10.1109/JIOT.2021.3109785`.

[37] René Mayrhofer et al. “The android platform security model”. In: *ACM Transactions on Privacy and Security (TOPS)* 24.3 (2021), pp. 1–35.

[38] *mHealth Apps Market Size, Trends and Global Forecast To 2032*. Accessed: 2023-14-02. 2023. URL: `https://www.thebusinessresearchcompany.com/report/mhealth-apps-global-market-report`.

[39] *mitmproxy*. URL: `https://mitmproxy.org/`.

[40] *Mobile Security Framework (MobSF)*. URL: `https://github.com/MobSF/Mobile-Security-Framework-MobSF`.

[41] *My Calendar Period Tracker*. URL: `https://play.google.com/store/apps/details?id=com.lbrc.PeriodCalendar`.

[42] AKM Iqtidar Newaz et al. “A survey on security and privacy issues in modern healthcare systems: Attacks and defenses”. In: *ACM Transactions on Computing for Healthcare* 2.3 (2021), pp. 1–44.

[43] Trung Tin Nguyen et al. “Share First, Ask Later (or Never?) Studying Violations of {GDPR’s} Explicit Consent in Android Apps”. In: *30th USENIX Security Symposium (USENIX Security 21)*. 2021, pp. 3667–3684.

[44] Ehimare Okoyomon et al. "On the ridiculousness of notice and consent: Contradictions in app privacy policies". In: *Workshop on Technology and Consumer Protection (ConPro 2019), in conjunction with the 39th IEEE Symposium on Security and Privacy*. 2019.

[45] Achilleas Papageorgiou et al. "Security and privacy analysis of mobile health applications: the alarming state of practice". In: *Ieee Access* 6 (2018), pp. 9390–9403.

[46] *Privacy, Deception and Device Abuse*. URL: https://support.google.com/googleplay/android-developer/topic/9877467.

[47] Abbas Razaghpanah et al. "Apps, trackers, privacy, and regulators: A global study of the mobile tracking ecosystem". In: *The 25th Annual Network and Distributed System Security Symposium (NDSS 2018)*. 2018.

[48] *Recital 38-Special Protection of Children's Personal Data*. URL: https://gdpr-info.eu/.

[49] Tejpal Sharma and Dhavleesh Rattan. "Malicious application detection in androida systematic literature review". In: *Computer Science Review* 40 (2021), p. 100373.

[50] Yun Shen, Pierre-Antoine Vervier, and Gianluca Stringhini. "Understanding worldwide private information collection on android". In: *arXiv preprint arXiv:2102.12869* (2021).

[51] Vikas Sihag, Manu Vardhan, and Pradeep Singh. "A survey of android application and malware hardening". In: *Computer Science Review* 39 (2021), p. 100365.

[52] Rocky Slavin et al. "Toward a framework for detecting privacy policy violations in android application code". In: *Proceedings of the 38th International Conference on Software Engineering*. 2016, pp. 25–36.

[53] *SSL Server Rating Guide*. URL: https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide.

[54] *SSL Server Test*. URL: https://www.ssllabs.com/ssltest/.

[55] Peter Story, Sebastian Zimmeck, and Norman Sadeh. "Which apps have privacy policies?" In: *Annual Privacy Forum*. Springer. 2018, pp. 3–23.

[56] *Summary of the HIPAA Privacy Rule*. URL: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

[57] Rosanna Tarricone et al. “Distinguishing features in the assessment of mHealth apps”. In: *Expert Review of Pharmacoeconomics & Outcomes Research* 21.4 (2021), pp. 521–526.

[58] Stacey A Tovino. “The HIPAA privacy rule and the EU GDPR: illustrative comparisons”. In: *Seton Hall L. Rev.* 47 (2016), p. 973.

[59] *User Data*. URL: `%5Curl%7Bhttps://support.google.com/googleplay/android-developer/answer/10144311?hl=en%5C&ref%5C_topic=9877467%7D`.

[60] Luca Verderame et al. “On the (Un)Reliability of Privacy Policies in Android Apps”. In: *2020 International Joint Conference on Neural Networks (IJCNN)*. IEEE, July 2020. DOI: `10.1109/ijcnn48605.2020.9206660`. URL: `https://doi.org/10.1109%5C%2Fijcnn48605.2020.9206660`.

[61] Xiaoyin Wang et al. “Guileak: Tracing privacy policy claims on user input data for android applications”. In: *Proceedings of the 40th International Conference on Software Engineering*. 2018, pp. 37–47.

[62] Wanrong Zhao et al. “Security and Privacy Analysis of Mhealth Application: A Case Study”. In: *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE. 2020, pp. 1882–1887.

Acknowledgments

I would like to express my special thanks to my advisor prof. Mauro Conti and to prof. Selcuk Uluagac for the support and guidance throughout this thesis project. Many thanks to all the members of the amazing CSL and ADWISE labs, with whom I had the pleasure to work during one of the best experiences of my life. Last but not least I would like to thank my family and friends for always being there for me during this journey.