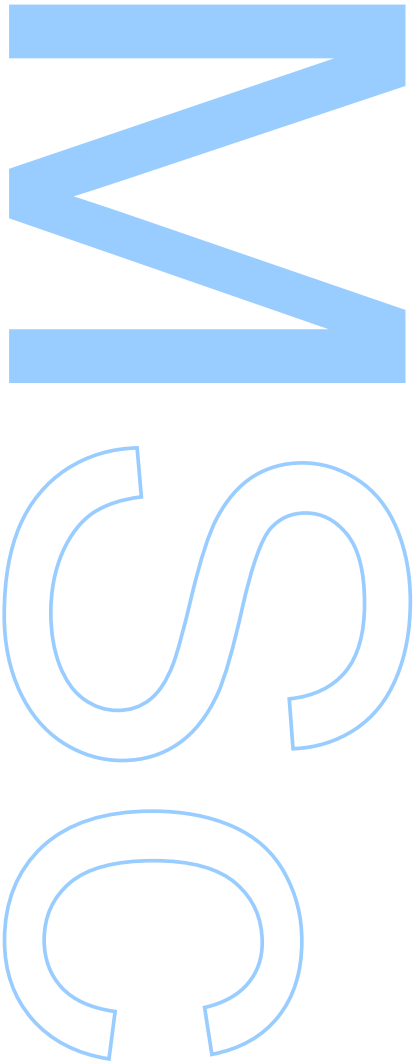
# Privacy Awareness for Mobile Devices

Miguel António de Kermenguy Serpa Pimentel Ramos
Mestrado em Segurança Informática
Departamento de Ciência de Computadores
2021

**Orientador**
João Paulo da Silva Machado Garcia Vilela
Professor Auxiliar
Faculdade de Ciências da Universidade do Porto

**Supervisor**
Mariana da Cruz Cunha
Investigadora
Faculdade de Ciências da Universidade do Porto



U.PORTO

FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO

Todas as correções determinadas pelo júri, e só essas, foram efetuadas.

O Presidente do Júri,

Porto, _____/_____/_____

UNIVERSIDADE DO PORTO

MASTERS THESIS

# Privacy Awareness for Mobile Devices


*Author:*
Miguel RAMOS

*Supervisor:*
João VILELA

*Co-supervisor:*
Mariana CUNHA


*A thesis submitted in fulfilment of the requirements*
*for the degree of MSc. Information Security*

*at the*


Faculdade de Ciências da Universidade do Porto
Departamento de Ciência de Computadores


September 22, 2021

*" Don't wish it was easier, wish you were better. Don't wish for less problems, wish for more skills. Don't wish for less challenge, wish for more wisdom. "*

Jim Rohn

# *Acknowledgements*

I want to thank Professor João Paulo Vilela for accepting me in this interesting project and to whom, together with Researcher Mariana Cunha from C3P, I acknowledge the huge help in this thesis.

To family and friends I appreciate their support, and to them I owe so many ideas that made this project more interesting.

UNIVERSIDADE DO PORTO

# *Abstract*

Faculdade de Ciências da Universidade do Porto
Departamento de Ciência de Computadores

MSc. Information Security

**Privacy Awareness for Mobile Devices**

by Miguel RAMOS

The security aspect is often underrated and not able to keep up with the fast-paced evolution of technology. Users have neither the necessary knowledge nor consciousness to protect themselves in an online world, and even the ones more knowledgeable often ignore simple privacy measures. With the growth of the mobile market share, smartphone users have become an appealing target for both attackers and mass surveillance systems.

The state of the art for this subject is not poor in quantity, but most projects are outdated or lack, if not quality, the necessary adjustments to the real world user with a busy daily life. The existing alternative solutions are usually too basic in what they provide to the user, frequently containing ads and even trackers.

The goal of this thesis is to increase users' knowledge and consciousness about privacy and how to improve it. For this, we created a user-friendly application capable of raising privacy awareness, seeking it to be appealing and informative at the same time. With maximum respect for the user's privacy, we intend not only to help users to improve their device's privacy settings, but also make them more informed in privacy-related aspects with regular nudges and informative news articles.

A field-study with two surveys was performed to evaluate the effectiveness of the developed application. With the collected results and obtained feedback, we could understand that the app had a positive impact on users' privacy awareness. Among the feedback, the application was frequently praised for its capacity to aggregate several privacy related features in just one place.

**Keywords:** Privacy Awareness; Android; Mobile Devices

UNIVERSIDADE DO PORTO

# *Resumo*

Faculdade de Ciências da Universidade do Porto
Departamento de Ciência de Computadores

Mestrado em Segurança Informática

**Consciencialização de Privacidade em Dispositivos Móveis**

por Miguel RAMOS

O aspecto da segurança é frequentemente subestimado e incapaz de acompanhar a evolução acelerada da tecnologia. Os utilizadores não possuem nem o conhecimento nem a consciência necessária para se proteger num mundo online, e mesmo os mais bem informados muitas vezes ignoram medidas simples de privacidade. Com o claro crescimento do mercado móvel, os utilizadores de smartphones tornaram-se um alvo atrativo tanto para atacantes como para sistemas de vigilância em massa.

O estado da arte deste assunto não é pobre em quantidade, mas a maioria dos projetos está desatualizada ou carece, se não de qualidade, da adaptação necessária para o utilizador atarefado do mundo real. As soluções alternativas existentes geralmente são muito básicas no que oferecem ao utilizador, frequentemente contendo anúncios e até *trackers*.

O objetivo desta tese é aumentar o conhecimento e a consciência dos utilizadores sobre o assunto da privacidade e como melhorá-la. Com esta finalidade, criamos uma aplicação de fácil utilização capaz de aumentar a consciencialização para este tema, procurando torná-la apelativa e informativa ao mesmo tempo. Com o máximo respeito pela privacidade do utilizador, pretendemos não apenas ajudá-lo a melhorar as definições de privacidade do seu dispositivo, mas também torná-lo mais informado neste tema com notificações regulares e artigos de notícias informativos.

Para avaliar a eficácia da aplicação desenvolvida, foi realizado um estudo com participantes e no qual foram apresentados dois questionários. Com os resultados recolhidos e o feedback obtido, pudemos compreender que a aplicação teve um impacto positivo na consciencialização dos utilizadores sobre privacidade. Entre os comentários recebidos, a

aplicação foi frequentemente elogiada pela sua capacidade de agregar várias funcionalidades relacionadas com privacidade num só lugar.

**Palavras-chave:** Consciencialização sobre Privacidade; Android; Dispositivos Móveis

# Contents

**Acknowledgements** v

**Abstract** vii

**Resumo** ix

**Contents** xi

**List of Figures** xiii

**List of Tables** xvii

**1 Introduction** 1
- 1.1 Motivation . . . 1
- 1.2 Proposed Solution . . . 2
- 1.3 Contributions . . . 3
- 1.4 Thesis Structure . . . 3

**2 State of the Art** 5
- 2.1 Permission Managers . . . 6
- 2.2 Related Work . . . 7
  - 2.2.1 PrivacyGrade . . . 7
  - 2.2.2 FoxIT . . . 10
  - 2.2.3 TaintDroid . . . 11
  - 2.2.4 SmarPer . . . 12
  - 2.2.5 ProtectMyPrivacy (PmP) . . . 13
  - 2.2.6 A Field Study on Mobile App Privacy Nudging . . . 15
  - 2.2.7 A Personalized Privacy Assistant for Mobile App Permissions . . . 16
  - 2.2.8 Studies comparison . . . 18
- 2.3 Approaches for Raising Awareness . . . 20
  - 2.3.1 Privacy Awareness . . . 22
  - 2.3.2 Application Assessment . . . 27
- 2.4 Conclusions . . . 29

**3 Solution development** 31
- 3.1 Solution Overview . . . 31
- 3.2 Requirements . . . 32

3.2.1 Functional Requirements . . . 32
3.2.2 Non-Functional Requirements . . . 37
3.3 Android application . . . 38
3.3.1 Main screen . . . 41
3.3.2 Application Settings . . . 42
3.3.3 Application Analysis . . . 44
3.3.4 Grouped Analysis . . . 47
3.3.5 Device Settings . . . 56
3.3.6 Privacy Hints . . . 57
3.3.7 News . . . 59
3.3.8 Scheduled tasks . . . 61
3.4 Server side / Backend . . . 63
3.4.1 Database . . . 64
3.4.2 Server Website . . . 65
3.5 Testing . . . 66
3.6 Conclusions . . . 67

**4 Field-Study for privacy awareness 69**
4.1 Pre-Survey . . . 69
4.2 Post-Survey . . . 70
4.3 Scheduled Tasks . . . 70
4.3.1 Hints and News . . . 71
4.3.2 Installed Apps and Security Progress . . . 74
4.4 Collected Data . . . 75
4.5 Results Analysis . . . 76
4.5.1 Pre-Survey . . . 76
4.5.2 Post-Survey . . . 78
4.5.3 Relevance of Privacy Functionalities . . . 85
4.5.4 Usability . . . 89
4.5.5 Collected Data . . . 92
4.5.6 Impact of users' privacy concerns in results . . . 98
4.5.7 Impact of app type of use in results . . . 100
4.6 Conclusions . . . 101

**5 Conclusions 105**
5.1 Future Work . . . 106

**A Pre-Survey 107**

**B Post-Survey 115**

**References 123**

# List of Figures


2.1 Average Users preferences from [32] . . . 9

3.1 Developer use cases diagram. . . . 33
3.2 User use cases diagram. . . . 34
3.3 Application icon. . . . 39
3.4 Final stage of launch screen. . . . 39
3.5 Application overview diagram. . . . 41
3.6 Main screen. . . . 42
3.7 Settings and trackers information screens. . . . 43
3.8 Applications list screen. . . . 44
3.9 Application information screen. . . . 47
3.10 Group by Privacy Level screen. . . . 49
3.11 Progress chart screen. . . . 49
3.12 Group by Permission screen. . . . 50
3.13 Group by Permission charts screen. . . . 51
3.14 Group by Grade and its pie chart screens. . . . 52
3.15 Grades information screen. . . . 52
3.16 Group by Category and specific category screens. . . . 56
3.17 Device Settings screen. . . . 57
3.18 Hints section. . . . 58
3.19 News section. . . . 60
3.20 Application, Database and Website interactions diagram. . . . 64
3.21 Hints and News website. . . . 66

4.1 Nudge example. . . . 74
4.2 Privacy information importance VS Privacy management by smartphone. . . . 77
4.3 Privacy knowledge questions. . . . 80
4.4 Participants choices on privacy actions. . . . 82
4.5 Privacy actions performed by participants. . . . 83
4.6 App section that helps the most to improve the device's privacy according to participants. . . . 85
4.7 Evaluations given by participants to the application. . . . 88
4.8 Usability questions. . . . 90
4.9 Evaluations given by participants to the application design. . . . 91
4.10 Percentages of app sections entries from the main screen. . . . 92
4.11 Granted and denied permissions distribution by permission group. . . . 94
4.12 Changes in the number of total granted permissions compared to the 1st measure for all participants. . . . 96

4.13 Average number of entries per participant and per day in the application during the field-study. . . . 97
4.14 Total number of entries per time of day in the application during the field-study. . . . 97
4.15 Average changes in the number of total granted permissions per participant compared to the 1st measure. . . . 100

A.1 Survey 1: Question 1 . . . 108
A.2 Survey 1: Question 2 . . . 108
A.3 Survey 1: Question 3 . . . 109
A.4 Survey 1: Question 4 . . . 109
A.5 Survey 1: Question 5 . . . 109
A.6 Survey 1: Question 6 . . . 109
A.7 Survey 1: Question 7 . . . 110
A.8 Survey 1: Question 8 . . . 110
A.9 Survey 1: Question 9 . . . 110
A.10 Survey 1: Question 10 . . . 110
A.11 Survey 1: Question 11 . . . 110
A.12 Survey 1: Question 12 . . . 110
A.13 Survey 1: Question 13 . . . 110
A.14 Survey 1: Question 14 . . . 111
A.15 Survey 1: Question 15 . . . 111
A.16 Survey 1: Question 16 . . . 111
A.17 Survey 1: Question 17 . . . 111
A.18 Survey 1: Question 18 . . . 112
A.19 Survey 1: Question 19 . . . 112
A.20 Survey 1: Question 20 . . . 112
A.21 Survey 1: Question 21 . . . 112
A.22 Survey 1: Question 22 . . . 113
A.23 Survey 1: Question 23 . . . 113
A.24 Survey 1: Question 24 . . . 113
A.25 Survey 1: Question 25 . . . 113

B.1 Survey 2: Question 1 . . . 115
B.2 Survey 2: Question 2 . . . 115
B.3 Survey 2: Question 3 . . . 115
B.4 Survey 2: Question 4 . . . 116
B.5 Survey 2: Question 5 . . . 116
B.6 Survey 2: Question 6 . . . 116
B.7 Survey 2: Question 7 . . . 116
B.8 Survey 2: Question 8 . . . 116
B.9 Survey 2: Question 9 . . . 117
B.10 Survey 2: Question 10 . . . 117
B.11 Survey 2: Question 11 . . . 117
B.12 Survey 2: Question 12 . . . 117
B.13 Survey 2: Question 13 . . . 117
B.14 Survey 2: Question 14 . . . 118

B.15 Survey 2: Question 15 . . . 118
B.16 Survey 2: Question 16 . . . 118
B.17 Survey 2: Question 17 . . . 118
B.18 Survey 2: Question 18 . . . 118
B.19 Survey 2: Question 19 . . . 119
B.20 Survey 2: Question 20 . . . 119
B.21 Survey 2: Question 21 . . . 119
B.22 Survey 2: Question 22 . . . 119
B.23 Survey 2: Question 23 . . . 119
B.24 Survey 2: Question 24 . . . 120
B.25 Survey 2: Question 25 . . . 120
B.26 Survey 2: Question 26 . . . 120
B.27 Survey 2: Question 27 . . . 120
B.28 Survey 2: Question 28 . . . 120
B.29 Survey 2: Question 29 . . . 120
B.30 Survey 2: Question 30 . . . 120
B.31 Survey 2: Question 31 . . . 121
B.32 Survey 2: Question 32 . . . 121
B.33 Survey 2: Question 33 . . . 121
B.34 Survey 2: Question 34 . . . 121
B.35 Survey 2: Question 35 . . . 121
B.36 Survey 2: Question 36 . . . 121
B.37 Survey 2: Question 37 . . . 122
B.38 Survey 2: Question 38 . . . 122

# List of Tables


2.1 Features and constraints comparison. . . . 19
2.2 Awareness and Field-Studies. . . . 20

3.1 Use case: Add one hint/news article. . . . 33
3.2 Use case: Analyse one application. . . . 34
3.3 Use case: Analyse applications grouped by similar parameters. . . . 35
3.4 Use case: Consult Device Settings section. . . . 35
3.5 Use case: Consult one hint. . . . 36
3.6 Use case: Consult one news article. . . . 36
3.7 Non-Functional Requirements. . . . 37
3.8 Grades calculation. . . . 53
3.9 Scheduled tasks. . . . 62

4.1 Scheduled tasks exclusive of the field-study. . . . 71
4.2 Scheduled nudges. . . . 71
4.3 Collected data for the field-study. . . . 75
4.4 Changes in the number of apps by privacy level. . . . 93
4.5 Average number of app changes by participant by permission group. . . . 94
4.6 Changes in the number of apps by participant by Grade. . . . 95
4.7 Average number of apps changes by privacy level between participants with higher and lower privacy concerns. . . . 99
4.8 Comparison of answers to usability questions between users that paid a higher (left - green) and lower (right - red) amount of attention to the app. . . . 101

# Chapter 1

# Introduction

## 1.1 Motivation

We are in an increasingly connected and digital world. Many people still do not welcome constant changes in technology, but several times the rapid evolution does not even give them a choice. Even for more privacy aware users, it is not rare to see them ignoring simple privacy measures. Our digital devices have more and more information, but it does not seem that the privacy knowledge is improving at the same rate. All of this draws the attention of not only attackers, but also the ones seeking to profit from using and selling users' information.

This thesis is aimed at the mobile market, having as a case study the Android Operating System. The last decade has seen a huge growing of mobile device usage. In 2020, the worldwide mobile usage on the web increased in five percentage points compared to the previous year, reaching 68%, leaving 29% for desktop usage and the rest 3% for tablets [1]. The market share values point to the same tendency, with mobile share having 54.57% and desktop share almost 12 percentage points below [2]. Focusing only on the mobile operating systems, it is clear the predominance of Android and iOS devices. The available articles and studies are not consensual about these operating systems' market share, but we can conclude near three quarters of devices have the Android OS, leaving about a quarter for iOS devices [3] [4] [5].

Such growth calls the attention of companies and governments, making the mobile industry, mainly Android devices, a target for information gathering [6] [7] [8]. The Edward Snowden case changed the way the world looked at mass surveillance and alerted at the need to make more on the user benefit.

This lack of user data privacy has become clearer with so much news of smartphones spying on their users [9] [10] [11], Android apps leaking private information [12] [13], suspicious collection of information [14], surreptitious ways of gathering data [15] and how easy is to track users [16] [17] [18] [19], among others. Besides that, users usually have low knowledge about the subject [20] and show a dichotomy between their intentions towards disclosure of personal data and their behaviour [21]. In order to minimize so many existing privacy problems, steps like the GDPR, General Data Protection Regulation, have been taken, but more must be done.

Improving privacy is not always easy. Besides the necessary balance between privacy and usability, users many times do not have the needed knowledge. Even if they have concerns about their privacy, discovering how to guarantee it may pose as a significant obstacle.

With the proposed solution discussed below and detailed further ahead, we intend to help users change their behaviour towards their own privacy. By raising their privacy awareness, we believe users will make more responsible decisions when it comes to how, when and with whom to share their private information.

## 1.2 Proposed Solution

Our main objective is to create a user-friendly application capable of raising privacy awareness. Since providing an application that would not respect the user privacy was never a considered option, some decisions were made from the very beginning to not have trackers, a concept to be explained further ahead, to not ask for what are considered dangerous permissions and finally to not collect any type of information from the user device, apart from the anonymous crash reports, out of the performed field-study context.

The developed Android application seeks then to be easy to understand, visually appealing and able to make users more aware of their privacy situation. Providing individual and grouped analysis for the device applications, it will help users to easily obtain an overview of their device privacy situation and quickly allow to consult each app status and interact with its settings.

Although Android settings tend to be well-organized, many users may face certain difficulties understanding which changes should be performed on their privacy benefit.

For this, we created a section in the app dedicated exclusively to explaining and redirecting users to them. We also present several hints to help users better understand what should be done to improve their privacy, which, when possible, redirects the user to the related Android setting. Besides hints, also news were gathered to keep users informed on privacy related events happening in the real world.

A field-study was performed to obtain feedback on the developed application and understand its effectiveness on raising users' awareness. The results demonstrate the positive effect of our application, being capable of capturing participants interest and helping them improve their privacy situation. From the feedback we have also retrieved what is most crucial to be improved, highlighting the nudges' system stability and the application overall design.

## 1.3 Contributions

This thesis was developed within the scope of COP-MODE (COntext-aware Privacy protection for MObile DEvices) [22]. COP-MODE is a research project led by the Universities of Coimbra, Porto and Cambridge aiming at enhancing the privacy of mobile devices through a personalized, automated and context-aware privacy manager. In the mentioned project, several data gathering campaigns were performed to facilitate automated privacy protection. Through these campaigns, a need for better user awareness was identified, which fostered the development of the work in this thesis.

The developed application was tested through a field-study with the final goal of releasing it publicly for societal benefit. The obtained results from the performed field-study will help future developers to understand how to take the most from the application in further improvements.

## 1.4 Thesis Structure

This document is organized in the following chapters: chapter 2 is focused on the current state of the art and related field-studies, chapter 3 describes all the implementation and design decisions, chapter 4 describes the field-study and analyses its results, and chapter 5 is dedicated to final remarks, also analysing some ideas for future work.

# Chapter 2

# State of the Art

This chapter presents the result of a study about the existing Android privacy and awareness related projects. The analysis of related work is a crucial part of information gathering, helping to understand how other teams and researchers were able to solve the problem in matter.

With Android evolution, there were several changes in its permissions' system, including the way permissions are graphically presented to the user. This fact does not preclude analysing older studies since the purpose is more directed at how aware are users about these permissions existence and importance.

Before start analysing the following studies, it is important to have a look at the concept of app permissions. They are used to managing user privacy by controlling access to user data and device functionalities. Each permission can belong to a permission group, which allows an easier presentation of permissions to the user. Each permission is categorized with a protection level assigned by Google itself, and on this work we will focus only on the ones belonging to the "dangerous" level. This way, the application deals with the permissions assigned to the following permission groups: *Calendar*, *Camera*, *Contacts*, *Location*, *Microphone*, *Phone*, *Sensors*, *SMS* and *Storage*. One important thing to notice is that, although from version 9 of Android (API level 28) a new permission group appeared named *Call Logs*, which is now responsible for two of the *Phone* group permissions (*READ_CALL_LOG* and *WRITE_CALL_LOG*), we have decided, for the sake of simplicity for the user and thinking no harm will be brought from this decision, to not add the *Call Logs* group and let the two mentioned permissions remain under the purview of the *Phone* group. Another aspect to be mentioned is that we have always taken into account the number of permissions and not the number of permission groups in the application, for

the main reason that requiring one permission from a group is not the same of requiring all the permissions that belong to that group.

The entire structure follows a line of though to help readers first understand what we want to distance from, and then present studies we consider more relevant, focusing not only on general features but also on awareness techniques and field-studies. This way, we intend first to present the concept of current permission managers in section 2.1 and explain the differences to our developed solution, and after clarifying this matter, we will in section 2.2 perform an analysis on several interesting projects that served as inspiration for our own work, together with a compact comparison (in subsection 2.2.8) about some of their features and other information which will help to justify some of our choices. The following and final section, 2.3, is fully dedicated to analysing awareness techniques and how were field-studies performed, both based on studies already present in section 2.2 and on some other briefly described projects.

## 2.1 Permission Managers

In here we intend to make clear the difference between applications denominated as permissions managers and our developed app. By presenting these main differences, we also intend to justify why are these separated from the next section, 2.2, which contains studies more similar to our final product.

There are currently several permission manager applications available in Google Play Store. This study was performed by analysing some of the most downloaded permission managers we found [23] [24] [25] [26] [27], proving how different they are from our final product for several reasons, of which we will present the most important ones.

A clear difference is their common commercial nature, which is easy to spot by the ads spread across the application. We do not intend any monetary return with this application, seeking only to help users manage their privacy on their Android mobile devices and understand how does raising awareness for privacy related subjects changes the users' habits. Still related to this matter, some of these apps contain in-app purchases and even trackers, a concept we will explain later ahead in subsection 2.3.1.2. We were able to collect this information through analysing these apps with our own developed application.

For applications whose purpose is to create privacy awareness, it is expected for them not to ask for promiscuous permissions. Although it was observed to be the reality for

most of these apps, they also usually requested, in runtime, the Accessibility Service which would grant them greater control on the user's device. From what these applications inform the user, this will grant them capability to change the device settings, which considering the type of app and to facilitate users managing permissions makes sense. However, we also made an effort not to request any kind of permission or access that might make the user feel uncomfortable with what our application could do.

Finally, a very clear aspect of these applications is to limit themselves to static analysis of applications permissions and redirecting users to the device's settings, with little or none more advanced analysis performed on each application and no grouped analysis other than classifying them according to number of granted dangerous permissions and grouping by requested permission. By interacting with third-party APIs and performing more analysis, whether individually for applications or grouping them, we intend to present the user with more information to provide them a better understanding of their device's situation and what can be changed.

## 2.2 Related Work

Several studies were analysed to help in the development of the present thesis, and some of them were considered as more closely related to the objective to achieve. The next subsections describe each of the chosen projects. Subsection 2.2.8 will focus on comparing those projects, using them as a basis for several of our decisions in the developed application.

### 2.2.1 PrivacyGrade

PrivacyGrade is the result of the work made by a team of Researchers from Carnegie Mellon University based on a grading methodology of Android smartphone apps [28].

This is the first of the two papers written by this team that will be analysed. The main focus of this study was achieved by using TaintDroid, a technology that we will later analyse with more detail in subsection 2.2.3, in order to identify the actions responsible by triggering the access to sensitive resource and where this sensitive information is sent to, all of this in the top 100 popular Android apps [29]. For each pair of app and resource, it was possible to manually assign to one of these three categories: major functionality,

sharing and tagging or supporting other minor functions, target advertising or market analysis. Several pairs fell into more than one category.

This study also seeks to bring a better understanding of the users' mental models of mobile privacy information to help users make better privacy-related trust decisions. The recruitment was performed through Amazon's Mechanical Turk (AMT) [30]. Questions were made about pairs of apps and resources with the main purpose of understanding the users expectations and how they felt when knowing the real answers. As suggested in AppFence [31], the data collection was focused on four types of sensitive resources: unique device ID, contact list, network location, and GPS location. Several results for different apps and resources were achieved but will not be presented in here.

The results suggest that both users' expectations and the purpose of why sensitive resources are used have a major impact on users' subjective feelings and their trust decisions. Another major finding is that informing users properly of the purpose of resource access can somehow facilitate users' privacy concerns.

The second paper [32] relies on static code analysis to determine the purpose for which an app requests each of its permissions. This usage of permissions was analysed while distinguishing between different types of third-party libraries responsible for requesting access. For example, it is possible to infer that the collection of location data is used for advertising purposes if only used by a bundled ad library. The analysis of third-party libraries and their API calls allowed to determine not only which resources but also why they were being used for.

Androguard [33] is a Python based tool to decompile Android APK files and to facilitate code analysis and was used as the major static analysis instrument. The performed analysis focused on the top 11 most sensitive and frequently used permissions at that time (*INTERNET*, *READ_PHONE_STATES*, *ACCESS_COARSE_LOCATION*, *ACCESS_FINE_LOCATION*, *CAMERA*, *GET_ACCOUNTS*, *SEND_SMS*, *READ_SMS*, *RECORD_AUDIO*, *BLUETOOTH*, *READ_CONTACT*). Several custom analysis scripts were created to interact with Androguard APIs to identify information related to:

- permission(s) used by each app;
- the classes and segments of code involved in the use of permissions;
- all the third-party libraries included in the app;

- permissions required by each third-party library (analysing third-party libraries provided more semantic information of how users' sensitive data were used and to whom they were shared).

Permission information of each app was obtained by parsing manifest files[1] of APK files and the decompiled source code was scanned to find specific Android API calls in order to determine the classes and functions involved in using these permissions. Only the top 400 third-party libraries were analysed.

It is important to note that when sensitive data was used by the application itself, it was not possible to determine why a certain resource was used. The authors considered that there is a high probability that if the resource is accessed within the app's code, then it is required by the mobile app itself rather than to collect data on behalf of a third-party.

Similarly to the previously described study, users (725 participants) responses were collected through AMT to understand the level of comfort the users had when knowing the resources each app accessed and for what reason. As can be seen in figure 2.1, between the four different purposes (Internal functionality, Ads, Analytics and SNS Social Network Sites), the one that brings more discomfort is Ads.

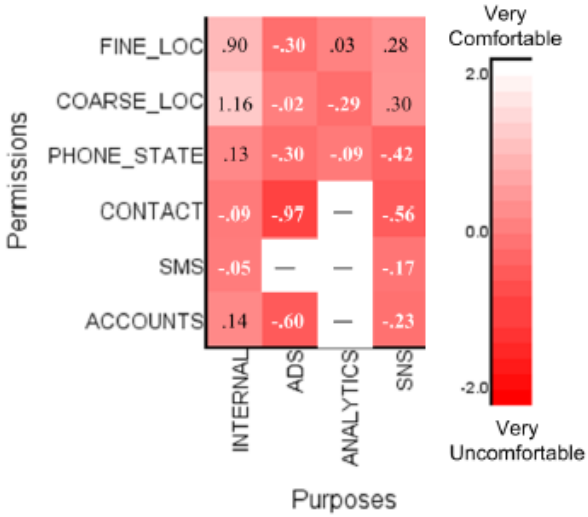



FIGURE 2.1: Average Users preferences from [32]

By using machine learning techniques, it was possible to create four distinct privacy profiles of users with similar preferences, and then were identified the suitable default settings for each of these groups.

[1]The manifest file describes essential information about an app to the Android build tools, the Android operating system, and Google Play.[34]

Between the presented limitations of this work, is the study of a limited number of free apps, not even using paid ones. The authors also stated that several purposes of use of resources could not be identified and the use of more sophisticated machine learning and clustering techniques could possibly further boost the accuracy of the performed predictions.

It is possible to understand that the collected information about the apps and libraries, either in the first study as in the second, due to the fast-paced actualization reality in the information technology area, is already out of date since there is no sign of any update in the most recent years. However, there was a positive contribution to comparing the users expectations and feelings about the apps' usage of resources.

### 2.2.2 FoxIT

For this study, it was developed an Android-based application called FoxIT [35], providing users with several education modules as well as a static smartphone and app permission analysis aiming to increase both privacy awareness and knowledge of mobile users. The app is not in Play Store, but its code is currently available on GitHub [1].

The app's functionalities comprehend a static analysis of smartphone and app permissions and several lessons about privacy relevant issues. Authors claimed that FoxIT focus on more advanced knowledge about privacy than the other app-based interventions existing at that moment.

The app is constituted of two sections that will be now briefly described. The first one is related to apps analysis:

- list of all applications with respective characterization ("harmless" - green face, "moderate" - orange face, "critical" - red face) according to the use of permissions considered "dangerous", "normal" and "other" (according to Google's own rating)
- for each application, the user can select the application to see the list of required permissions, divided into "dangerous", "normal" and "other"
- there is also a button that allows to redirect the user directly to the settings of the application in question

[1] https://github.com/sleep-yearning/PrivacyRiskInfo

- various device settings information is also available, presenting as examples if the installation of unknown sources is enabled, what type of location tracking is enabled, and others.

The second section is aimed at teaching the users through privacy lessons:

- sort of quiz about several privacy related topics
- by completing classes more advanced classes are unlocked and new mascot animations become available (this app's mascot is a fox).

97 participants were invited for a two-week field study, although only 31 were able to complete the requested tasks. The authors conclude that participants reported to have improved the privacy conditions on their smartphone, actively informed themselves about privacy related topics, and prompted others to protect their data.

Although apparently good results were obtained, it was clear the fact that the performed field study was too heavy and too time-consuming, putting too much pressure on participants and very probably biasing the results.

### 2.2.3 TaintDroid

Capable of simultaneously tracking multiple sources of sensitive data, TaintDroid is described by its authors as an efficient and system-wide dynamic taint tracking analysis system [36] [37]. This application is aimed at monitoring sensitive data access to provide informed use of third-party applications by mobile users and valuable information for smartphone security service firms seeking the identification of misbehaving applications.

Assuming all third-party downloaded applications are not trusted, TaintDroid monitors them in real-time to understand how they access and manipulate user's personal information by detecting when and how sensitive data leaves the system. Using dynamic taint analysis (also called "taint tracking"), TaintDroid labels (taints) sensitive information for it to be identified by a taint mark indicating the information type assigned to it. All tainted data is then monitored so when it leaves the system is logged not only the data's label, as well as the application responsible for transmitting the data and the data's destination.

For the application to be able to perform the tracking described above, it is necessary to work at low level, and so it was not possible to implement TaintDroid as a user-space

app. This way, to use TaintDroid users must flash a custom-built firmware which makes the app unavailable for the common mobile user. Using this specially designed firmware, it was also made possible to avoid applications from escaping the virtual machine by modifying the native library loader.

An application study was performed with 30 third-party Android applications to understand how applications use privacy sensitive user data. By relating the monitored accesses with the data exposure by applications, it was found that two thirds of the applications exposed sensitive detailed information. Among it is location data, the phone's unique ID and phone number, all by just taking advantage of the seemingly innocuous access permissions granted when installing. By using the labels assigned in the aforementioned taint tracking technique it was possible to take conclusions like half of the studied applications sharing the location data with advertisement servers and approximately a third of applications exposing device ID and sometimes phone and SIM card serial numbers. The authors stated that TaintDroid caused no perceived latency while running experiments.

As limitations, are presented the capacity of only tracking data (explicit) flows, not tracking control (implicit) flows to minimize performance overhead, and since the target are third-party applications whose source code is unavailable, fully tracking control flow requiring static analysis is not possible. As mentioned before, the installation of TaintDroid requires flashing a custom-built firmware, which makes it an application for a very restricted target public.

### 2.2.4 SmarPer

Permissions context awareness, semi-automatic decision-making at runtime and data obfuscation are the three main goals of SmarPer [38], presented as an advanced permission mechanism for Android with support for finer-grained permissions and multiple decision-levels [39]. As its own name suggests, being SmarPer an abbreviation for Smart Permissions, it aims at helping users manage permissions more efficiently.

This study relies on machine learning to predict users' permission decisions. For each users' decision, data is fitted a linear regression through the Bayesian linear regression model (BLR). SmarPer implementation is based on XPrivacy [40], which allowed to perform a field study with 41 participants for a minimum of 10 days in which SmarPer was

used in the participants own devices to collect permission decisions at runtime. Participants had first access to some training material like written instructions and video tutorials. The results show the possibility of learning users decision patterns with good accuracy even with little training data, being contextual information the key. SmarPer offers obfuscation techniques for four data types: camera, contacts, location and storage. Besides allowing and denying access to their private data, users could also opt to obfuscate it since, by using the Xposed Framework [41], SmarPer was able to modify parameters and returned values before and after the execution of sensitive API calls.

To be able to execute such operations and use the mentioned framework, which allows users to install modules to modify the feel and look of smartphones, it is required all the users in the present study to use rooted devices. Besides that, SmarPer is only guaranteed to be compatible with Android versions from 4.0.3 to 5.1.1.

The goal of this study was to collect at least 75 permissions decisions per participant. If such objective was not reached then the participants were encouraged to continue the study until the necessary data was provided. The participants actions were heavily supervised by daily uploads of decision data to the developers server and if a user was not actively using the smartphone, he or she would be detected and contacted. When finished the data-collection part, each user was confronted with a series of questions to understand certain decisions of allow/deny/obfuscate and to obtain feedback about SmarPer.

As limitations, can first be presented the need for rooted devices between 4.0.3 and 5.1.1 versions of Android. The data collection focused only on popular apps, which can also create a bias problem since most users may be more willing to accept their requests. The authors also stated that the decision modelling can be improved by considering non-contextual factors beyond only contextual factors, the data set size is not big enough to reliably train some advanced machine learning models and it was not possible to verify if decisions provided by participants were not fake or wrong.

### 2.2.5 ProtectMyPrivacy (PmP)

The first ProtectMyPrivacy (PmP) app was developed for iOS in 2012 [42]. In April 2016 a new version of PmP was released for Android [43] which was maintained until December 2017 [44].

Beyond allowing users to control app-level permissions, PmP is also capable of detecting the usage of standard Android API calls to access privacy sensitive data items such

as locations and contacts. When detected the presence of third-party libraries, the user is provided with allow, deny and fake options to control what data is shared with them.

AppOps is a native permission manager introduced in Android 4.3 and hidden from developers in 4.4.2. PmP makes use of AppOps, leveraging and extending its functionality. Users have the flexibility to make decisions on individual or grouped permissions. Just like SmarPer, PmP also makes use of Xposed Framework, which implies the need for rooted devices.

The anonymizer module allows to return fake values instead of privacy sensitive data items. The new fake data matches the original values in structure. The effectiveness of this module was measured by providing fake data to all 300 more popular free apps in Play Store and verifying that none of them crashed.

Android OS delegates the handling of firewall operations permissions to the Linux kernel, and so PmP has a separate module, not part of the Xposed Framework. It allows to implement a network firewall functionality by interacting with the kernel iptables framework. A separate PmP firewall contains the modified iptables rules.

The authors state they do not collect any information capable of identifying users, only a hashed obtained from the device ID with the purpose of distinguishing users and respective decisions in the database. The PmP client app contacts the server for requesting updates and sending heartbeats, used as signals to indicate the total number of active users.

The process of blocking access to user data by third-party libraries started by choosing 30 of the most used libraries and support privacy controls for them. The presented goal was to continue manual research and add more libraries as they become popular, having the top 60 covered in July 2017.

A field-study was performed by providing free access on Google Play and Xposed stores and letting real users make their voluntary contributions, gathering data from more than 10.000 users. The goal was to understand the effectiveness of this App+Library implementation and the results showed, compared to the soil use of AppsOps application, that users were significantly better protected from having their data sent to third-party libraries.

The authors recognize the need for rooted devices as a limitation, writing that “PmP is skewed towards more technically savvy users”, and by making use of AppOps they limit its use to Android versions between 4.3 and 4.4.2. The detection of sensitive information

usage is not effective when data is asked by the app itself and then passed as a parameter to the third-party library, although this is not the typical model. Another problem is the possibility of obfuscation by third-party libraries, which hinders the protection against those apps or libraries. The current decision model assumes all the data used by the app is used for internal purposes and not for sharing with third-party entities, making the user vulnerable to less reliable applications. For future work is presented the option to use static analysis techniques on decompiled apps and other tools to infer data accesses purposes so more useful and complete information is presented to the user.

### 2.2.6 A Field Study on Mobile App Privacy Nudging

This study [45] aims to evaluate the benefits of providing users with an app permission manager and informing them through nudges to raise data collection awareness. The importance of understanding these benefits come from the perception that smartphone users are often unaware of how their installed apps collect and use their private data. Two research questions are here focused:

- Is providing users access to a fine-grained app permission manager an effective way to encourage them reviewing and modifying app permissions?
- Is it worth to improve the effectiveness of a fine-grained app permission manager, to regularly alert users through privacy nudges about their apps sensitive data collection?

By using AppOps, it was performed an analysis on installed apps behaviour to detect unexpected invasive behaviour data access. With the collected information, this work measures the effect of privacy nudges in raising user awareness to adjust or at least review their app permissions, performs all the evaluation in the participants own devices and informs participants through nudges for all installed apps on the devices.

The adopted methodology is as follows:

- 23 participants were invited, answered some questions and a 'study client' app was installed that allowed them to access AppOps (an app was needed to be able to access AppOps) through a special installation with USB connection to the computer. As a mandatory requirement, participants had to have Android versions 4.3 - 4.4 (4.4.2 no longer worked because AppOps was removed in this version for non-rooted Android devices).

- Phase 1: (7 days) In the first 7 days, the user did not have access to AppOps, only information was collected about the installed applications and respective requests for permission access.
- Phase 2: (7 days) The AppOps application was made available, nothing more;
- Phase 3: (8 days) In the first 4 days, specific nudges were shown to each of the four chosen permission types (location, phone contacts, calendar and call logs) in a random order, and in the last 4 days all the nudges were repeated in the same order. The first 4 days showed statistics since the beginning of the study and the second 4 days showed statistics since the last equal nudge (which happened 4 days before).
- In the end, participants responded to an online survey on AppOps experience, privacy nudges, experience gained, etc. Some participants also agreed to do an interview at the end for more in-depth feedback.

This field-study allowed to understand that Android users really benefit from app permission managers such as AppOps, and periodic nudges are an important way of improving their effectiveness by regularly reminding the user for privacy aspects. It was also noted that the more simplistic and personalized to the users' interests, the more efficient are the nudges.

As main limitations, the authors presented the little number of users with the necessary Android versions (4.3 - 4.4) and the need for internet connection all the time, which caused several disruptions in the study results since some users turned it off. We can also note the need for a special in person installation quite impractical.

### 2.2.7 A Personalized Privacy Assistant for Mobile App Permissions

This next study [46] is based on a methodology to learn and create privacy profiles for permissions settings. Using the public PrivacyGrade dataset, see subsection 2.2.1, it was given importance not only to show the frequency of access to private data but also the inferred purpose of the access.

The main focus of this study is building privacy profiles from users' real-world permission settings. For that, a field study was performed to create a dataset using information of permission settings, purpose information and app categories. With the collected information, it was then possible to use privacy nudges, making users aware of unexpected data practices and suggesting them better aligned privacy preferences.

A profile-based personalized privacy assistant (PPA) was designed and implemented by the authors. Six groups of privacy-related permissions were created to organize permission settings: Location, Contacts, Messaging, Call Log, Camera, and Calendar. In order to achieve enhanced user awareness, the permission manager was extended to not only show an app's most recent access request, but also the access frequency of the last seven days as well as, when available, purpose information from PrivacyGrade dataset. By presenting this information through nudges, users can click them to open the permission manager and change their settings.

To assign users to the generated privacy profiles, a maximum of five questions is asked about their privacy preferences. The choice of questions takes into account the type of apps each user has on its own phone to create a dynamically personalized set of questions. The PPA would then pass the user's features to the server side, where a scalable SVM (Support Vector Machine) classifier would be trained to generate recommendations for privacy settings. Before the generation of the questions, users' preferences are first aggregated in the training dataset by:

- each permission;
- each (permission, app category) pair;
- each (permission, purpose) pair.

To perform this study, it was needed the participants to have rooted Android devices and install the app to collect real settings stemming from user behaviour. In the first week, the permission manager app was available to the users at the same time it was collecting the frequencies of permission requests for installed apps. In the second week, privacy nudges were shown once a day, providing information about one of the six available permissions already mentioned above. In the end, participants were asked to fill an exit survey.

A second field study was conducted to evaluate the effectiveness of the created privacy profiles. Two conditions were used to perform this study, one named 'treatment condition' in which were considered profile assignment and recommendations and other named 'control condition' without profile-based support. In the first two days PPA silently collected permission access frequency statistics for installed apps and on the third day the app interacted with the users. In the treatment conditions, users were asked up to five questions and assigned to a profile, according to which some recommendations were

made and then feedback on them was requested. On the other side, the control condition only showed an introduction screen explaining they could now use the PPA app. A final survey was performed to obtain feedback.

The results show that privacy choices based on the recommendations tended to be accurate. It was concluded the recommendations were effective with high precision. Users indeed benefited from personalized privacy setting recommendations according to the assigned profile. Regular privacy nudges made participants restrict additional permissions and so proved to be an important aspect in raising user awareness.

The first presented limitation is the need for root access, which not only limits the number of users available to participate in the requests, but also increases the possibility of having more biased results. Another limitation is the short length of the performed studies, avoiding the users fully converging on stable privacy settings.

### 2.2.8 Studies comparison

This work is intended at alerting and informing users to privacy related subjects, which according to PrivacyGrade (subsection 2.2.1) is effective and has positive results. After analysing several apps and studies, we noticed the existence of several drawbacks that we intend to avoid. On the other side, we propose the implementation of some novel features that were not contemplated in the read articles. Some other requirements, as the need for rooted devices, if the app is still upgraded and which are the target Android versions will also be contemplated in here. The table 2.1 provides us the possibility of a quick overview, helping to make a more reasoned comparison by analysing the main available features, the need for root access or special firmware, if is still upgraded and to which range of Android versions is suited.

There are some aspects present in other studies we find interesting and relevant to add to our developed application, and that obviously do not require root. A first analysis of the FoxIt (subsection 2.2.2) application shows some similarities that our app has with it, such as the grouping of applications with the same categorization, which follows the same principle of FoxIT by considering the number of dangerous and non-dangerous permissions. We also made an effort on informing the user about some of its device settings, explaining their purpose and redirecting the user to them.

TABLE 2.1: Features and constraints comparison.

| Study (Subsection) | Features | Root/ Special Firmware | Still upgraded | Android versions |
|---|---|---|---|---|
| Privacy Grade (subsection 2.2.1) | • Use of TaintDroid for deep analysis on app behaviour<br>• Use of AndroGuard to decompile code and possibilitate static code analysis, determining how each permission was used by the app itself and the included third-party libraries | - | No | - |
| FoxIT (subsection 2.2.2) | • Grouping of apps by categories<br>• Information on the user's device settings | No | No | 6.0-? |
| TaintDroid (subsection 2.2.3) | • Taint Tracking technique used to detect from where, to where and when sensitive information leaves the system | Yes | No | 2.1-4.3 |
| SmarPer (subsection 2.2.4) | • Use of XPrivacy and the Xposed Framework to collect and study users' permissions decisions | Yes | No | 4.0.3-5.1.1 |
| ProtectMyPrivacy (subsection 2.2.5) | • With AppOps allows to control app-level permissions<br>• With the Xposed Framework, is capable of detecting Android API calls to sensitive data, offering the allow/deny/fake options | Yes | No | 4.3-4.4.2 |
| Mobile App Privacy Nudging (subsection 2.2.6) | • By using AppOps, detection of unexpected invasive behaviour data access | No | No | 4.3-4.4.2 |
| Personalized Privacy Assistant (subsection 2.2.7) | • Creation of privacy profiles, assigned to users according to their answers about privacy preferences | Yes | No | 4.4.0-5.X |

One of the main requirements in this study is the development of an application that is easily upgradeable and that, therefore, contrasts with several of the ones presented above, such as PrivacyGrade, which no longer has updates in its database, SmarPer (subsection 2.2.4), which was intended only for versions 4.3.3 to 5.1.1, and either PmP (subsection 2.2.5) as 'A Field Study on Mobile App Privacy Nudging' (subsection 2.2.6) make use of AppOps, thus limiting its use to versions 4.3 to 4.4.2. Unlike the later one, we also want to avoid the need for special, face-to-face installation. Another fundamental requirement is to make the app available to the common user through the Google Play Store, so the need for users with rooted devices or custom-built firmwares such as in TaintDroid (subsection 2.2.3), SmarPer, PmP and 'A Personalized Privacy Assistant for Mobile App Permissions' has been removed. It is also intended to be an easy-to-understand app, avoiding the need for prior training as done in the study with SmarPer.

## 2.3 Approaches for Raising Awareness

Based on the table 2.2, we will on this subsection perform an analysis similar to that of the subsection 2.2.8, but this time focusing on awareness techniques and how the field-studies were executed. Beyond the already analysed studies, some other will be mentioned and explained with less detail for each of the subjects that will be covered below.

TABLE 2.2: Awareness and Field-Studies.

| Study (Subsection) | Awareness | Surveys/Field-studies | No. participants | Field-study duration |
|---|---|---|---|---|
| Privacy Grade (subsection 2.2.1) | • Grading apps | • Through AMT, questions made about pairs of apps and resources to understand users' expectations and how they felt when knowing the real answers | (2 studies) 1st: 179 2nd: 725 | (2 studies) 1st:6 days 2nd:3 weeks |

**Table 2.2**: Continued from previous page

| | | | | |
|---|---|---|---|---|
| FoxIT (subsection 2.2.2) | • Apps characterization (harmless/moderate/critical)<br>• In-apps quizzes about several privacy related topics | • Field-study to obtain feedback on app's effectiveness | 37 | 2 weeks |
| SmarPer (subsection 2.2.4) | - | • Field-study to understand how and why users have a certain interaction with permissions when asked to allow/deny/obfuscate | 41 | 10 days |
| ProtectMy Privacy (subsection 2.2.5) | - | • Provided free access to the app and users could contribute to this project by using the app to evaluate its effectiveness in increasing user protection | 10000+ | 1+ year |

**Table 2.2**: Continued from previous page

| | | | | |
|---|---|---|---|---|
| Mobile App Privacy Nudging (subsection 2.2.6) | • Privacy nudges specific to each of the chosen permission types (location, phone contacts, calendar and call logs) | • Field-study collecting information to measure the effect of privacy nudges in raising user awareness<br>• Online survey on the field-study<br>• Some participants also agreed to do an interview at the end | 23 | 22 days |
| Personalized Privacy Assistant (subsection 2.2.7) | • Privacy nudges to alert about unexpected data practices and suggest better aligned privacy preferences | • One field-study to collect information on participants devices and show privacy nudges later. Exit survey performed<br>• Another field-study to evaluate the effectiveness of the created privacy profiles from the first study | (2 studies)<br>1st: 85<br>2nd: 138 | (2 studies)<br>1st:2 weeks<br>2nd:9 days |

### 2.3.1 Privacy Awareness

Since raising awareness is one of the main aspects of this thesis, it had to be carefully studied. Based on the analysis of awareness techniques from table 2.2, together with

some other studies presented below, we will describe and justify in here some of our choices related to creating awareness, namely grades, nudges, trackers and news/hints.

- In the study 'Inspect what your location history reveals about you' [47], the authors focused on creating awareness on how much is possible to tell about someone by knowing their location history. The participants' location history, provided by Google in their smartphones, was requested and, after some study, conclusions like genre, age and salary were presented to the users, seeking to alert them to the lack of privacy they were exposed by sharing their location all the time.

- 'Surveillance Self-defence' [48] is a project by the Electronic Frontier Foundation to help people to be protected from electronic surveillance. In the context of privacy, this project offers a huge amount of information: numerous articles, guides, security scenarios and news.

The first study type is probably one of the most impactful by creating a certain discomfort in users when showing them what is possible to perform with their data. It is more viable to perform with a web application, as is the case of this study, where someone submits data by their own will, or in person than with a mobile application because, although possible to perform, would probably make the user uncomfortable and suspicious on the app behaviour by the way it processed its device information. This is then one of the reasons we opted for more informative and "neutral" analysis, although we do not discard some analysis of this kind in future work.

On the other side, the second mentioned study is not about any type of analysis, only intending to help people by providing several privacy related information in one website. The closest we have to this approach is the presentation of hints and news.

Other idea we also consider interesting, and possible for future implementations, and which would complement the presentation of news and hints, is to include in-app quizzes. This technique is used in FoxIT (subsection 2.2.2) and helps to engage the user in the process of learning privacy related subjects.

The next subsections will address our choices for raising privacy awareness.

#### 2.3.1.1 Nudges

The technique of alerting or reminding users through nudges, although not new, is very important, especially when dealing with awareness apps and field-studies. We understood from the beginning the need for its use and made an effort to learn which type of nudges should appear, with which content and in which period of time. Here are some related studies:

- 'Understanding User Preferences of Digital Privacy Nudges' [49] is a more theoretical study seeking to understand users' preferences regarding design variations of digital nudges. Authors intend to give a contribution by giving implications on how to design digital nudges. The conclusions were that colours are easier to understand, avoiding on pressure such as time delay and textual based nudges.

- This next study, 'Nudging People Away from Privacy-Invasive Mobile Apps through Visual Framing'[50], is based on the 'Framing Effects' principle, defending that people's decisions depend in part on the way problems are stated and presenting options as a loss or as a gain significantly affects people's choice [51]. Among the conclusions, negatively-framed information tends to influence more than positively-framed information of the same magnitude, although the authors demonstrated it is possible to create semantically equivalent privacy ratings framed in both positive and negative light. Recommendations on using more visual framing, leveraging visual attributes prevalent through the culture, were given to help developers catching the users' attention.

- Providing a multi-disciplinary assessment related to privacy and security decision-making, the study 'Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online' [51] focuses on the emerging field of soft paternalism. Soft paternalism interventions attempt to influence decision-making to improve individual well-being, at the same time freedom of choice is preserved. This is achieved by reframing the available choices to increase the likelihood of users making self-beneficial decisions. The idea is then to design tools and policies that enhance choice without restricting it.

By analysing these studies, it becomes clear the need to personalize the nudges to make them inviting and easy to understand. We want the user to be engaged and for

that we made an effort to always present nudges with short and clear texts, adapted to the situation, and when possible clickable, allowing the user immediate interaction with what the nudge is alerting/informing of.

Looking at the table 2.2, we notice the two last studies making use of privacy nudges to alert the user about invasive behaviour detected in real-time. This type of analysis requires, in the most recent Android versions, root access and so is nonviable in our case.

The amount, frequency and type of nudges will be different depending on whether it will be in or out of context of the field-study. All the details will be discussed further ahead in the document in chapters 3 and 4.

#### 2.3.1.2 Trackers

A tracker is a piece of software meant to collect data about you based on your device usage, and is usually distributed by companies as a SDK (Software Development Kit), enticing developers by making their lives easier [52]. The entire process of analysing application trackers will be detailed further ahead in this document, but in here we will take a look at how some other projects use the information from trackers:

- Warden [53] is a FOSS (Free and Open Source Software) app management utility which contains a static curated list of known trackers retrieved from Exodus Privacy [54] database. This list is used to be cross-checked with the class names obtained for each app in its DEX file[1] in order to identify the trackers. Other more advanced features are implemented but require root.

- Yale Privacy Lab contains a repository [56] related to research profiles on Android app trackers hidden in popular Google Play apps. Several information about trackers, permissions and other subjects is available, being this a repository aimed at creating awareness on this theme.

- Exodify [57] is a browser extension able of showing how many trackers there are in Android applications when searching in the Play Store. The idea is to help people decide whether they accept to install applications based on the tracker information about them.

- TrackerControl [58] is an open source and free Android app to allow users control and monitor trackers' actions on their mobile devices. The Disconnect blocklist [59]

[1] A DEX file is an executable file saved in a format that contains compiled code written for Android.[55]

is used together with an in-house blocklist to reveal the companies behind tracking, the trackers' category and purposes. An Android VPN functionality is used to analyse app's network communications locally.

In our case, the list of trackers for each application is retrieved from Exodus Privacy, just like the first mentioned study, Warden. Besides that, we also follow the example of the fourth study, TrackerControl, by collecting some more information about trackers' categories from the Disconnect blocklist.

#### 2.3.1.3 Application's Privacy Grading

Despite already mentioned a characterization of applications based on the number of dangerous permissions, it was found important to distinguish apps through a more extended analysis. In here we have an example of a study that uses a very similar approach:

- The 'CAP-A Project' [60] [61] [62] is part of a wider collective awareness platform for privacy concerns and expectations [63]. In here we focus on the mobile app they developed. Its main purpose is to provide users, for each app, beyond information present in the App Store like description and number of downloads, also two scores. One score is based on how honest the app is with regard to its privacy-related requests, and the other one, named the community score, is calculated based on how close the community's expectations are to what the app is in fact requesting. It is also possible to contribute with our own expectations for each app.

Although mainly based on scores, this mentioned application presents an association between score ranges and grades. Before presenting the biggest differences to our grade assignment, we would first like to mention PrivacyGrade (subsection 2.2.1) as another source of inspiration. These two studies have in common the usage of crowdsourcing to assign grades by measuring the gap between people's expectations of an app's behaviour and the app's actual behaviour, with PrivacyGrade also making use of static code analysis. In our case, we used different information to assign grades, which will be listed and explained in section 3.3.4.3, considering both static code analysis and crowdsourcing as nonviable options for the nature and duration of this thesis. Instead, we have focused on information related to the number of dangerous permissions requested, number of trackers and if the applications requested permissions not expected for their assigned category.

#### 2.3.1.4 News/Hints

None of the mentioned studies implemented, as an awareness technique, the presentation of security/privacy hints and news. We opted for this since we considered it to be a valuable technique to raise user awareness, either by giving them advises through hints or informing with news. We also want to highlight the personalization of both hints and news to each user, according to the user device brand (e.g. Samsung) and installed applications. Some hints allow to redirect the user to the corresponding Android settings, facilitating his/her interaction with them.

### 2.3.2 Application Assessment

As part of this thesis, a field-study was performed with the main purposes of understanding the application effectiveness and how to improve it. For this, we sought inspiration in the aforementioned studies, present in table 2.2, together with the ones listed below:

- The study 'A survey on smartphone user's security choices, awareness and education' [64] had the objective of understanding how much importance people give to privacy issues and which security measures they used. Smartphones physical security was clearly the topic mobile users were more concerned about. The need for more privacy awareness to the general public was highlighted and also the fact that even more advanced users usually follow weak practices.

- Seeking conclusions on how aware are users about their privacy, according to their installed applications, the authors of the study 'A study on users' privacy perception with smart devices' [65] developed an application which would also provide a form of awareness to users. The two main goals were to periodically question users about their knowledge related to the behaviour of one of their apps and how does information about it change their perception on this matter and related risk. The described experiment was performed with 17 users and demonstrated a clear need to increase user awareness before providing technological and legal solutions.

In our work, a clear decision made from the beginning was not to collect sensitive data from users, whether inside or outside the context of the field-study. We also wanted an application not exclusive of a field-study, but readily available for the general user.

With this field-study, we intend to obtain answers for some of our questions:

- Is a permission manager, without any ads or trackers, that has total respect for the user's privacy and intended to raise privacy awareness, an appealing application for users to have installed on their devices to manage their privacy?
- Which aspect of the application proved to be the most valuable to raise privacy awareness and then should be further improved?
- Is there any advantage on regular nudges, essentially the ones related to privacy hints?
- How is the application effective in improving user awareness as time evolves? Will users focus on the application only the first days, or their interest will remain throughout the field-study duration?
- What can be improved?

Just like the second mentioned study above, 'A study on users' privacy perception with smart devices', we also seek conclusions on how aware are users about their privacy. With our field-study, we want to understand the evolution of knowledge and privacy concerns of users, both according to their answers and the collected data. The chapter 4 will further detail what type of conclusions we seek to achieve with the surveys for specific type of questions and collected data.

Analysing the table 2.2, we gathered some ideas of how to conduct our own field-study. One of the main goals we have is to obtain feedback on our application, which is similar to FoxIT and even PMP. 'Mobile AppPrivacy Nudging' also sought to measure the effect of privacy nudges and made use of online surveys, which in our case are in-app surveys, with the difference that we opted not to have interviews with participants and rely only on the surveys and collected data. In 'Personalized Privacy Assistant' it was decided to present only one final survey and show privacy nudges based on collected data. We instead presented two surveys, one at the beginning and another at the end.

We have chosen to have a 10 day field-study just like SmarPer, believing this to be the correct duration for users to consult the application, also allowing a reasonable number of nudges to appear. The initial idea was to follow the same example of studies like FoxIT and 'Personalized Privacy Assistant' with a 2-week duration field-study, however, we have opted to reduce the time and increase the nudges' frequency to at least two per day. A longer field-study period could prejudice the answers to the final survey by causing users to forget what they have done during it.

It was not strictly defined by us the range of participants number. After the invitation had been sent, 42 participants accepted to participate and, at the end, 32 participants contributions were considered valid.

## 2.4 Conclusions

Being Android the current most used operating system for smartphones, it is natural to observe a special interest from researchers, and the privacy concerns subject is one of the most discussed. We have seen in here several studies, some of them including apps as their final product, that provide us a better understanding on what is already done, what is yet to be improved and which gaps should be fulfilled.

Based on all of this state of the art research and intending to help solve the already presented problem, an Android application was developed as an output of this thesis. As described throughout this chapter, our final product contains both similarities and innovations when compared to other studies, not only when it comes to features but also awareness techniques. We mainly seek to obtain a user-friendly and easy to maintain application that gathers several of the discussed ideas in other studies and adding some others, in order to make it publicly available to be able to raise privacy awareness and, on a first stage, to help us understand how impactful our app is on user behaviour.

We then sought to achieve an appealing user-friendly app, which would gather some of the most interesting ideas from other studies, together with some of our ideas, that would let the user informed on the privacy/security theme and always having maximum respect for the user privacy. The next chapter is fully dedicated to describing the developed solution.

# Chapter 3

# Solution development

Everything related to the implementation and design of the solution will be described in this chapter. The problem seeking to be solved was already described in chapter 1 and now is time to address how it was addressed.

We start with sections 3.1 and 3.2 by providing an overview of how the solution was thought and designed, as well as listing the requirements guiding our implementation. Section 3.3 will focus on the several features provided by the developed Android application and the following one, 3.4, will do the same but focusing on the server side. Finally, the testing procedures will be described in section 3.5.

## 3.1 Solution Overview

From this work was intended to result an Android application with the purpose of helping users have a much better perception on how their private information is handled, together with giving them suggestions on how to improve their privacy. This app would then allow to assess the effect of awareness on users' privacy behaviours. It was then clear the need for features able to inform, alert and suggest the user according to their device status. Customizing the application to the user is something we strive for and also a matter to be further improved.

As a general overview of the features, we highlight the capacity to analyse the privacy side of each app individually, the grouping of applications according to common aspects, the gathering of several privacy related device settings in one place and the offering of hints and news.

As it will be described in the requirements, the hints and news should not be embedded into the application, but stored in a database where new data could be added, modified or deleted at any time. And so, alongside with the app creation, it was deployed a database and a website, this last one with the only purpose of adding new hints and news.

Being an overview, everything said in this section will be analysed in the light of the defined requirements and further detailed in the following sections.

## 3.2 Requirements

This section seeks to demonstrate to the reader the result of the requirements gathering phase. Here are described the functional and non-functional requirements, using the FURPS+ model, and explained the identified use cases.

### 3.2.1 Functional Requirements

In the context of an Android application which provides several features, the chosen approach was to define only some functionalities to be presented in use cases, being these the ones considered to be the main core of the application. Below are presented the use case diagrams for the developer, figure 3.1, and user, figure 3.2, together with the respective tables for each one (for the developer, a single table was able to describe the process of both use cases).

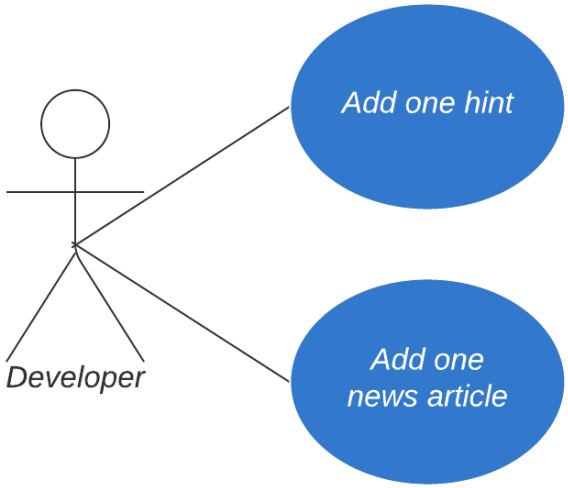



FIGURE 3.1: Developer use cases diagram.

TABLE 3.1: Use case: Add one hint/news article.

| **Use case** | Add one hint/news article |
|---|---|
| **Objectives** | Allow the developer to insert a valid hint/news article into the database |
| **Basic Flow** | • The developer accesses the server website<br>• The website is loaded<br>• The developer fulfils all the mandatory fields and optionally the non-mandatory ones<br>• The server validates all the inserted information and informs the hint/news article was inserted successfully |
| **Pre-conditions** | • The website is online and reachable<br>• The database is active and reachable |
| **Post-conditions** | • A new hint/news article exists in the database |

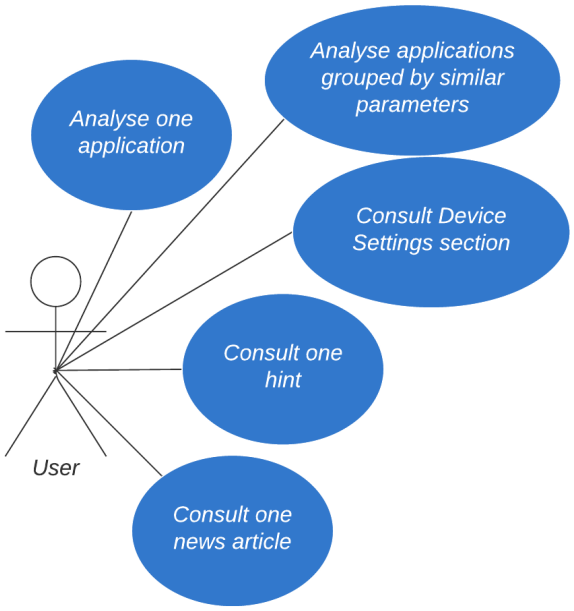



FIGURE 3.2: User use cases diagram.

TABLE 3.2: Use case: Analyse one application.

| **Use case** | Analyse one application |
|---|---|
| **Objectives** | Allow the user to analyse individually any application of his/her device |
| **Basic Flow** | • The user enters the 'Application Analysis' section<br>• The app lists the available applications<br>• The user selects the desired application<br>• The app opens a new screen with several information about the selected application |
| **Pre-conditions** | • The app is opened in the main screen<br>• The application to be analysed belongs to the type of applications selected in the app settings |
| **Post-conditions** | • The screen with information about the desired application is displayed |

TABLE 3.3: Use case: Analyse applications grouped by similar parameters.

| **Use case** | Analyse applications grouped by similar parameters |
|---|---|
| **Objectives** | Allow the user to perform a wider analysis of several applications based on similar parameters |
| **Basic Flow** | • The user enters the 'Grouped Analysis' section<br>• The app allows the user to choose what type of grouped analysis he/she wants to make<br>• The user selects the grouped analysis type he/she wants<br>• The applications displays the apps grouped by the chosen similar parameter |
| **Pre-conditions** | • The app is opened in the main screen<br>• The application to be analysed belongs to the type of applications selected in the app settings |
| **Post-conditions** | • The screen with applications grouped by similar parameters is displayed |

TABLE 3.4: Use case: Consult Device Settings section.

| **Use case** | Consult Device Settings section |
|---|---|
| **Objectives** | Inform the user about some Android settings, redirect him/her to them and, when possible, inform which is their status |
| **Basic Flow** | • The user enters the 'Device Settings' section<br>• The app shows information about some of Android settings, allowing the user to be redirected to them and, when possible, informing about their status |
| **Pre-conditions** | • The app is opened in the main screen |
| **Post-conditions** | • The screen with information about Android settings is displayed |

TABLE 3.5: Use case: Consult one hint.

| **Use case** | Consult one hint |
|---|---|
| **Objectives** | Let the user consult one of the several available hints, divided into categories |
| **Basic Flow** | • The user enters the 'Privacy Hints' section<br>• The app shows all the hints, divided into different categories<br>• The user selects the desired hint<br>• The app opens a new screen with the hint title and text and, when existing, a button to redirect the user somewhere else where he/she can interact with the respective settings |
| **Pre-conditions** | • The app is opened in the main screen |
| **Post-conditions** | • The screen with information about the desired hint is displayed |

TABLE 3.6: Use case: Consult one news article.

| **Use case** | Consult one news article |
|---|---|
| **Objectives** | Let the user consult one of the several available news |
| **Basic Flow** | • The user enters the 'News' section<br>• The app shows the available news<br>• The user selects the desired news article<br>• The app opens a new screen with the news article title, summary, date and a clickable source |
| **Pre-conditions** | • The app is opened in the main screen |
| **Post-conditions** | • The screen with information about the desired news article is displayed |

### 3.2.2 Non-Functional Requirements

Having already presented the functional requirements, the remaining of the FURPS+ model, the non-functional requirements, will be listed in table 3.7.

TABLE 3.7: Non-Functional Requirements.

| Usability |
|---|
| • Comprehensible application to non-IT people, easy to understand and navigate through |
| • Appealing design |
| • Available both in English and Portuguese |
| • Capacity of saving data locally without requesting for *Storage* permission |
| **Reliability** |
| • Send of anonymous crash reports |
| • Ability to function correctly independently of possible third-parties errors |
| • Database authentication |
| **Performance** |
| • Optimized performance, adapted to each type of task |
| **Supportability** |
| • Modularity and scalability, for future addition of features |
| • Maintainability, to facilitate correction of problems and improvement of functionalities |
| • Configurability, for high-level settings |
| • Capacity to add, modify or delete any hint or news at any time |
| **Other(+)** |
| • Implementation requirements: |
| – Android OS (version $\geq$6.0) |
| – Simple server-side |

## 3.3 Android application

The main application features, and so the core of this work, will be described in this section. All the implementation intended to solve the problem domain while following the aforementioned requirements. But before, it is important to mention some aspects in common and how requirements were taken into consideration.

This application was developed and tested to be supported in smartphones with Android versions 6.0 (API level 23) or higher. This version introduced a new permissions model in the Android OS, with users now being able to directly manage app permissions at runtime. This was a major change for the way users interacted with applications' permissions, and so we considered it important to make our application available to all versions from Android 6.0.

The chosen programming language for the development of this application is *Java*. This choice was considered taking into account several of the advantages provided by its language: strong support of an expansive community, powerful development tools available, platform independent, object-oriented approach and easy to learn/understand. At first, another technology was being considered, *Flutter*, however *Java* proved to be much more adequate especially due to functionalities like accessing application permissions. Java is the primary option for developing native applications on the Android platform [66] [67] [68] [69].

Having the non-functional requirements from table 3.7 always in mind, we list below several decisions made to respect them:

- An appealing design was always pursued throughout the application development, carefully choosing colours and the visual distribution. The application logo was then a crucial aspect, seeking to have an attractive design. It joins the concepts of 'eye' and 'settings', with the purpose of the user to get an idea of an application that looks after his/her privacy by managing the device settings. The chip wires are intended to create a feel of deeper analysis, since we go beyond showing basic information and redirecting the user to the Android available settings.

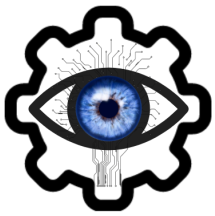


FIGURE 3.3: Application icon.

- To achieve better performance, there is some necessary pre-processing in the application opening. Since we focus on the device applications, it is necessary to access their information like package name, version and application name. This last one, application name, presented however a significant challenge due to the time it took to be retrieved from the system. The way of solving this issue was to obtain all the apps names in the application opening and relating them to the corresponding package name, which clearly improved the performance of the application. At the same time, it was decided to add an opening animation which would improve the application's visual aspect, containing the logo and simulating someone typing the application name in a Linux Bash shell. The UI and background concurrent processing was possible thanks to the use of threads. Figure 3.4 presents the final stage of launch screen.

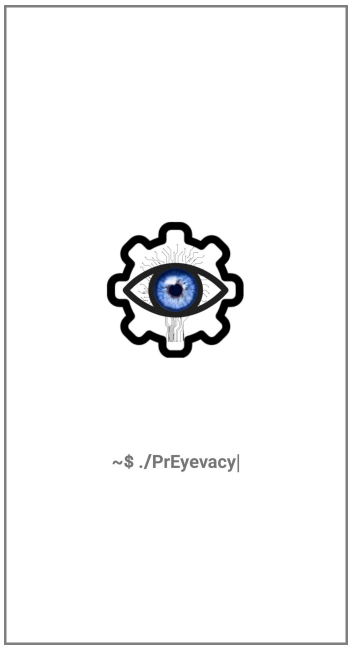



FIGURE 3.4: Final stage of launch screen.

- Since the beginning, the purpose of asking no dangerous permissions was a must,

and then it was needed to be able to save data locally without asking for *Storage* permission. The chosen solution was using the Serializable interface for several reasons, being among them the simplicity of use, the huge object supportability, the ability to easily adapt to changes and the capacity of not relying on third-party tools or libraries. This solution was, however, not fit to save passwords and API keys that should at least have some layer of protection, and for that was used a NDK (Native Development Kit) file. Although this is not a flawless technique, the use of a NDK file allowed to provide the necessary security to the database username and password, as well as the Exodus Privacy database API key. Based on C++, this file cannot be decompiled and disassembling it poses quite a difficulty, essentially when the data to be protected is encoded in some way, which in our case is Base64 [70] [71].

- Another aspect to address is the sending of a report when an uncaught crash happens, and, in some cases, caught exceptions are also sent, helping the app developers to understand the cause of the problem. Each report contains the following information: date, error message, version release, API level, board type, brand, model and device type. This allows to have a wide view on "what happened where" without invading the user privacy by sending totally anonymous reports.

- To achieve good supportability, it was made an effort for the several application components and screens to fit well on different screen sizes. Three ranges of screen height sizes in pixels were considered to adapt the user interface when necessary: $< 1300$, $\geq 2000$ and the remaining values between. Beyond the screen size, supportability was achieved by a development planning having in mind aspects like modularity and scalability to ease adding new features or extend the existing ones, maintainability to code maintenance and configurability with the aggregation of app high-level settings.

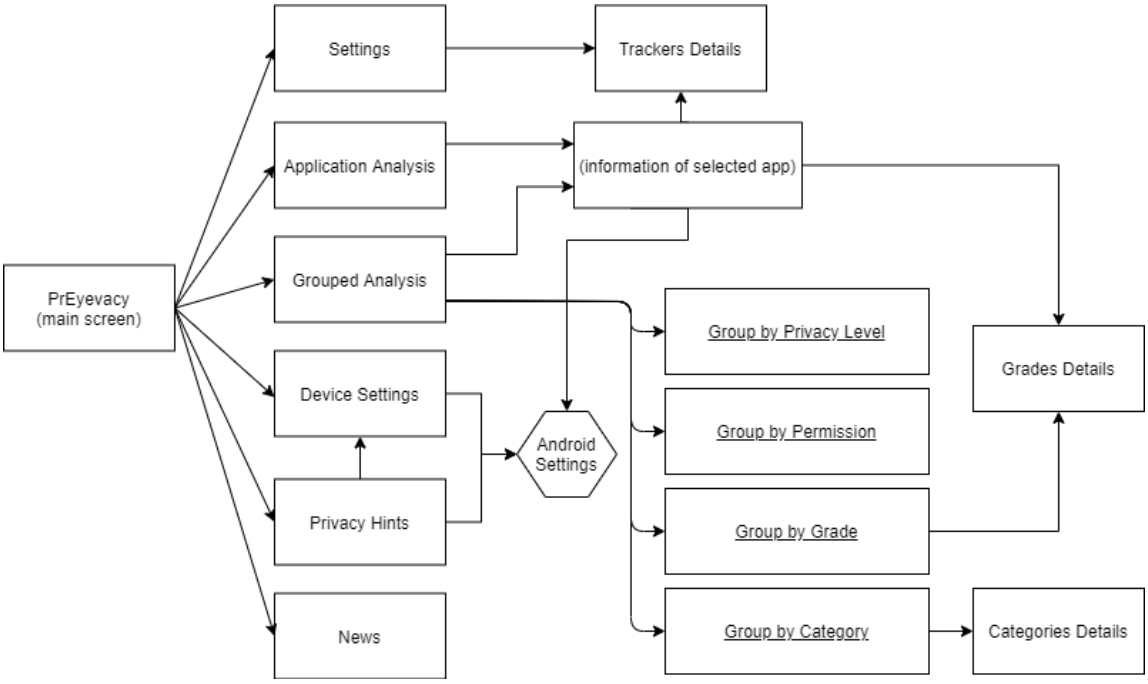



FIGURE 3.5: Application overview diagram.

The figure 3.5 presents an overview of the several components of the application and how they link to each other. The main components are accessed from the main screen and will be described in the next subsections. From them, the user can access all the application functionalities. The scheduled work that happens in background, aiming to bring a greater experience and further engage the user, is also going to be discussed in subsection 3.3.8.

### 3.3.1 Main screen

This screen is presented right after the launch screen and allows the user to enter the main sections of the application. The layout aims to be simple, as visible in figure 3.6, with the following components:

- The application title, which text font is randomly chosen each time this screen is loaded and changed to a different one each time the user clicks on it.
- The application logo. A winking effect was added to the eye in the logo with intervals of 4 to 7 seconds between winks.
- The main application sections buttons: *Application Analysis*, *Grouped Analysis*, *Device Settings*, *Privacy Hints* and *News*. All these sections will be described further ahead.

- The application settings, accessible through a gear shape button on the top bar of the screen.

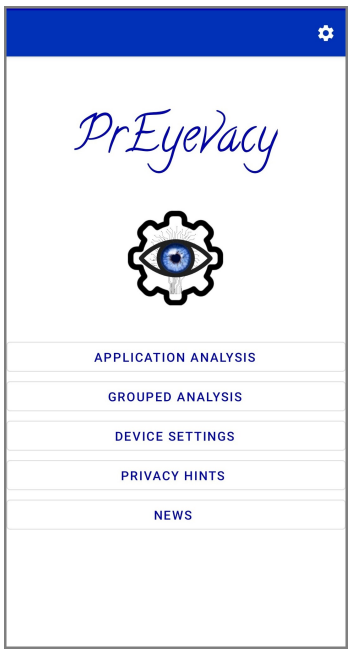



FIGURE 3.6: Main screen.

### 3.3.2 Application Settings

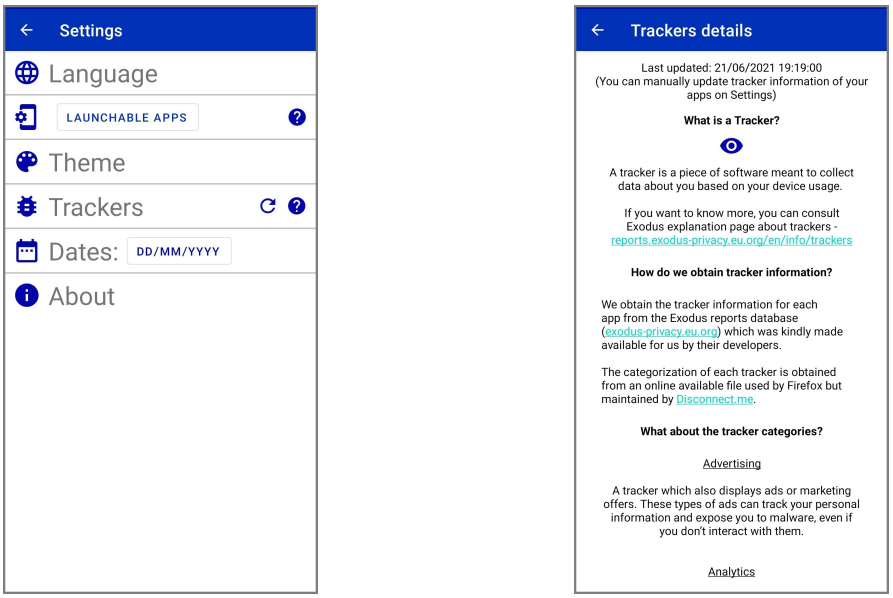
Presented in figure 3.7a, this section in the application deals with the settings transversal to the entire application. There are five of them possible to be changed:

- **Language** - As indicated to be done in the requirements, the whole application is available both in English and Portuguese. The initially chosen language is Portuguese if the device is using it, and English in any other case.

- **Type of Apps** - There are here three options. For each one the user can read a small description explaining in what it consists of. This setting will define which applications will be presented and analysed throughout the application. The default one is *Launchable Apps*, which, as the name suggests, deals with all the apps possible to be launched. The other two are *User Apps*, the ones installed by the user, and *All Apps* which will show all system and non-system apps. Choosing this last option will, as is informed to the user, degrade the app performance at certain operations due to the much larger number of apps to be processed. Every time the application is launched, the selected option is *Launchable Apps*.

- **Theme** - It is possible to choose among 5 themes - *Default*, *Green*, *Red*, *Orange* and *Black* - each of them written with the main theme colour. Each theme will focus on one specific colour, used to the top bar, to paint most icons and some of the text.

- **Trackers** - Here is possible to manually update tracker information for all applications. It is also accessible an information screen, presented in figure 3.7b, related only to trackers containing the last manual or automatic update, answering what is a tracker and how tracker information is obtained, and finally the explanation of all tracker categories that can be shown when listing the trackers for each application. As already mentioned in subsection 2.3.1.2, to obtain trackers we rely on two external services, *Exodus* to retrieve the initial list of trackers and searching for the device applications and *Disconnect blocklist* to get the trackers categories. This is one of the cases the requirement 'Ability to function correctly independently of possible third-parties errors' had to be implemented. The implementation is then prepared to deal with problems as inactive external services or malformed responses.




(A) Settings screen. (B) Trackers information screen.

FIGURE 3.7: Settings and trackers information screens.

- **Dates format** - Three date formats are available: Day/Month/Year which is the default, Month/Day/Year and Year/Month/Day. All the dates in the application will respect the chosen format.

- **About** - Here is presented a small description of the application and the context in which it was developed.

### 3.3.3 Application Analysis

It is important that users can analyse individually each application they have on their devices. By selecting this option, all the applications belonging to the chosen type of apps (as already described in subsection 3.3.2) are displayed, as visible in figure 3.8. For each one is presented in red the number of granted dangerous permissions, calculated using a thread for the sake of performance. The usage of threads and mainly the pre-processing performed in the application launch, as described in the beginning of this chapter, were crucial to decrease the response time, most notable when the number of applications increases.

This screen also allows searching for applications by their name by clicking on the search icon, and two sorting methods are implemented: by name (from A to Z, used by default) and by number of dangerous granted permissions (in descending order).

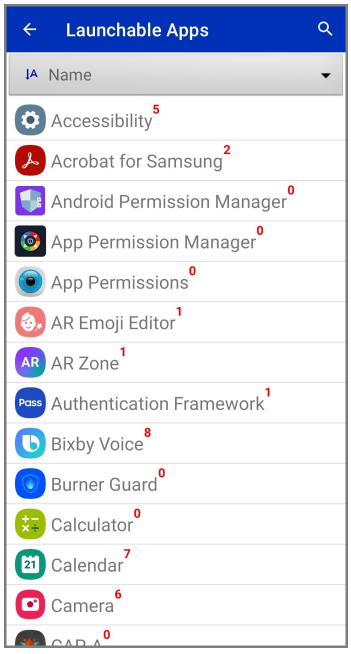



FIGURE 3.8: Applications list screen.

By clicking in any application, a new screen is shown with several information. On the top is displayed the application logo and its assigned grade. Clicking on the grade will open another screen, providing information about the grades and how they are calculated by our application. In here, our explanation about it will be left for subsection 3.3.4.3.

At the top bar, the user can click an icon that will show or hide part of the screen information, which is by default hidden. This hidden part is merely informative and not dedicated to helping users improve their privacy. It contains:

- Application name;
- Package name;
- Application version;
- Application path;
- Target SDK version;
- Date of installation;
- Date of last modification.

Independently of the above information being displayed or not, the following information, more dedicated to the privacy aspect, is always visible as seen in figure 3.9. They consist of:

- **Privacy Level** - Here is displayed the assigned privacy level. The user can click on the information button to obtain some textual explanation about the concept of privacy level. We will further discuss this in subsection 3.3.4.1.
- **App Category** - This part will only be visible if the device has Android 8.0 (API level 26) or latter, and displays the application category. An information button shoes textual explanation on the category concept. We will further discuss this in subsection 3.3.4.4.
- **Required Features** - Presents the list of required features. Features are used to inform external entities about the set of hardware and software features on which the application depends.
- **Required/Granted/Denied Permissions** - The user can consult here three lists, one for the required permissions, another for the ones he granted and one more for the ones he denied. For every list the dangerous permission group names are painted in red and for each one is presented below the list of corresponding permissions. For all the three lists there can be also *Other* permissions, which are not considered as dangerous, that belong to the type of information that is hidden by default but can be made visible by clicking on the top bar icon mentioned before. There are some special cases that need to be mentioned:

  - For the *Location* permission, it is made a difference between apps being able to access it only when using the app and when are able to access it in background even when the app is not being used.
  - For the *Storage* permission, from Android 11, there is a difference between accessing all files and accessing media files only. Our application invites the user to consult the analysed application settings when detects a request to access all the files.
  - For permissions *Microphone* and *Camera* our application warns the user when detects possible requests to activate any of these permissions in background and without user knowledge. Since only from Android 11 it is possible to verify this difference on Android settings, then only from this version we invite the user to consult the analysed application settings.

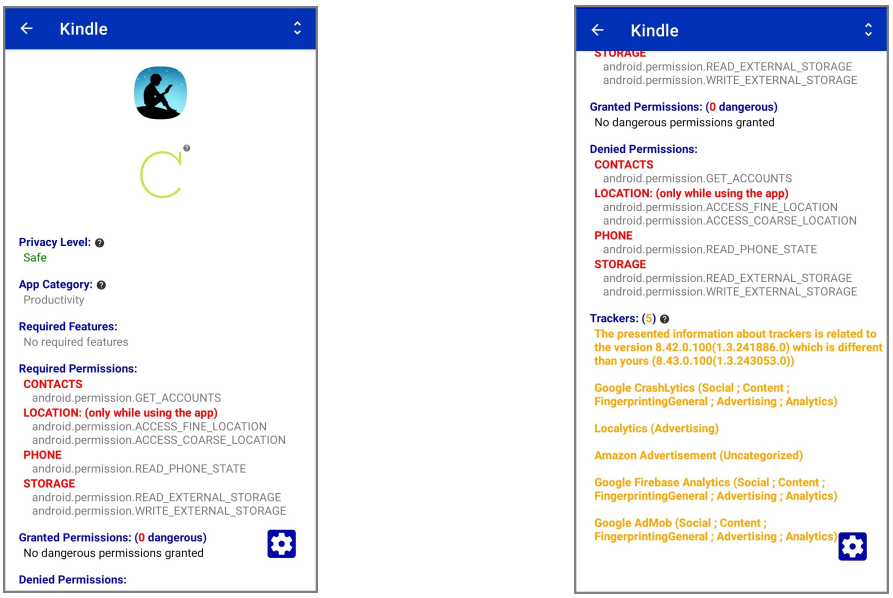
  In order to raise user awareness and foster the user to reduce dangerous granted permissions, we also present some information for when at least one dangerous permission is granted in the following situations:

  - When analysing a launchable application assigned with a *Dangerous* privacy level, the user is warned through flashing dangerous icons on top of the granted permissions list and the button that will allow the user to consult and change the analysed app's permissions. It is also displayed a short text, strongly encouraging the user to review if it is possible to revoke some permissions.
  - When the consulted application is launchable and assigned with privacy level *Medium*, which means at least one dangerous permission is granted, the user is invited to consult the application settings, indicating the button for that purpose with a red arrow.
  - When the user is consulting a non-launchable system app, then he/she is informed that these type of applications usually do not allow its permissions to be denied, but still we encourage him/her to consult the application settings in the case some dangerous permission is granted, indicating the button for that purpose with a red arrow.

- **Trackers** - All the information related to trackers is here displayed for the application in analysis, containing the list of trackers and corresponding tracker categorization. An information button redirects the user to another screen fully dedicated

to the tracker concept, which was already mentioned and explained in subsection 2.3.1.2.

Every time this screen is loaded its content is updated, guaranteeing any change made to the application is visible to the user. After consulting all this information, it is possible that the user may want to consult the device settings related to the application, and so, in the bottom right corner of the screen, there is a gear shape button for that purpose. When clicked, a floating message appears informing the user of the possibility to change the application permissions on the new opened screen.




(A) Top part of screen. (B) Bottom part of screen.

FIGURE 3.9: Application information screen.

### 3.3.4 Grouped Analysis

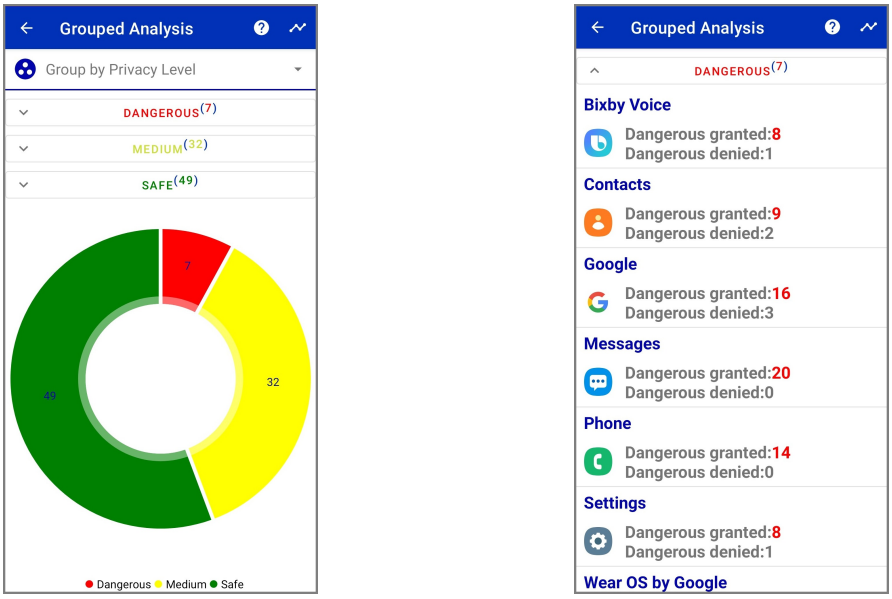
The four subsections that follow will explain the different ways of grouping applications according to similar factors. This will significantly help the user understand how private his/her information is by studying the applications under the point of view of some important common aspects. Just like the analysis in subsection 3.3.3, this one will focus on the apps belonging to the chosen type of apps in the application settings, already described in subsection 3.3.2. Three similar aspects for all the following subsections are the information button on top of the screen, which will perform a different task for each one, the ability of all of them to update its content when reopened, which will guarantee always updated information being displayed to users independently of their changes in

their own device settings for the applications permissions (or even the installation and removal of applications), and finally the possibility of opening the application analysis screen, described in subsection 3.3.3, by clicking on any app on the presented lists.

#### 3.3.4.1 Group by Privacy Level

This is the first of the performed grouped analysis and also one of the most important. This analysis intends to alert the user to the amount of dangerous permissions that are granted to each application. By clicking on the already mentioned top bar information button, the following explanation text is shown, which will also help to describe here this analysis: "*Based only on the number of granted dangerous permissions for each app. It represents the 'power' you provide the application to access your data and control your phone. Privacy Levels can be improved by reducing the permissions you grant, but remember some apps will necessarily require many permissions to work properly, with the Phone (can be other similar name) usually being one of them. Although you should take into account all applications, essentially the launchable ones, we advise you to focus on the ones installed by you.*". This text will help the user understand the analysis and how to improve their privacy situation by reducing the number of apps in the *Dangerous* level. There are three privacy levels:

- **Safe** - No dangerous permissions granted. Button colour: green.
- **Medium** - Belong to here all the apps not fitting in the *Safe* and *Dangerous* levels. Button colour: yellow.
- **Dangerous** - The minimum number of dangerous granted permissions for an app to belong to this level is a quarter of all possible dangerous permissions to be requested. This value was tested on several devices with different characteristics and type of apps, and it was considered to present always a valuable and correct division of applications. Button colour: red.




(A) All levels shown. (B) *Dangerous* level opened.

FIGURE 3.10: Group by Privacy Level screen.

As visible in figure 3.10a, for each of the described privacy levels, the number of applications belonging to it is presented and the list of apps becomes visible by clicking on the respective level button. Each button is painted as indicated in the above bullet points to help the user easily interpret what each level represents. Another valuable asset is the pie chart created with the number of applications belonging to each level and respecting the same colours mentioned above.

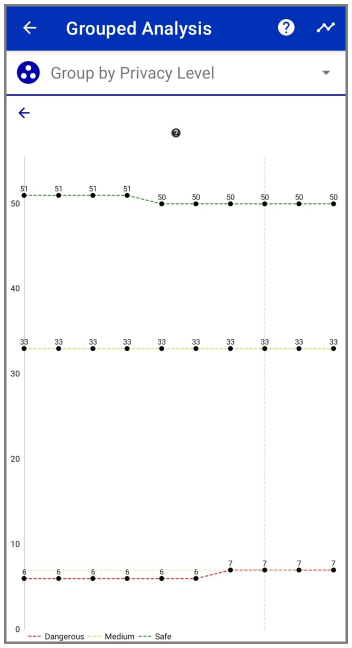
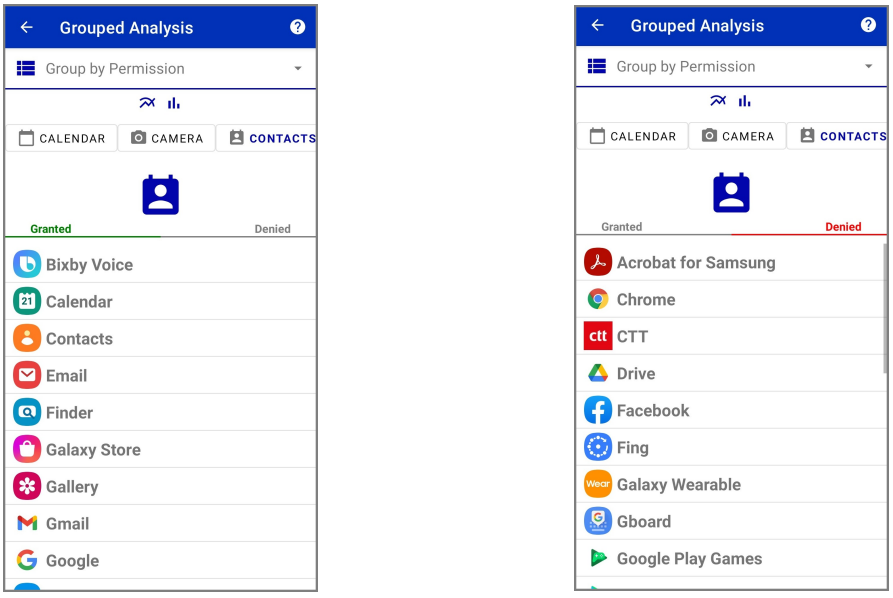



FIGURE 3.11: Progress chart screen.

This analysis contains yet another graph, this one dedicated to the user progress towards the discussed privacy levels and visible in figure 3.11. This graph will show information collected every day to present the user his/her progress on the number of apps for each privacy level. The graph will only be visible when a minimum of three data collections were performed and will present a maximum of 15 measures. The user has access to the period over which the graph focuses and is also shown another important information: the graph values are only based on the launchable apps. This choice was to avoid a graph with huge values if taking into account all applications, in which a change in one application would be hardly noticeable, and also thinking this is more useful than just contemplating the apps installed by the user. This data collection will be discussed in subsection 3.3.8.

#### 3.3.4.2 Group by Permission

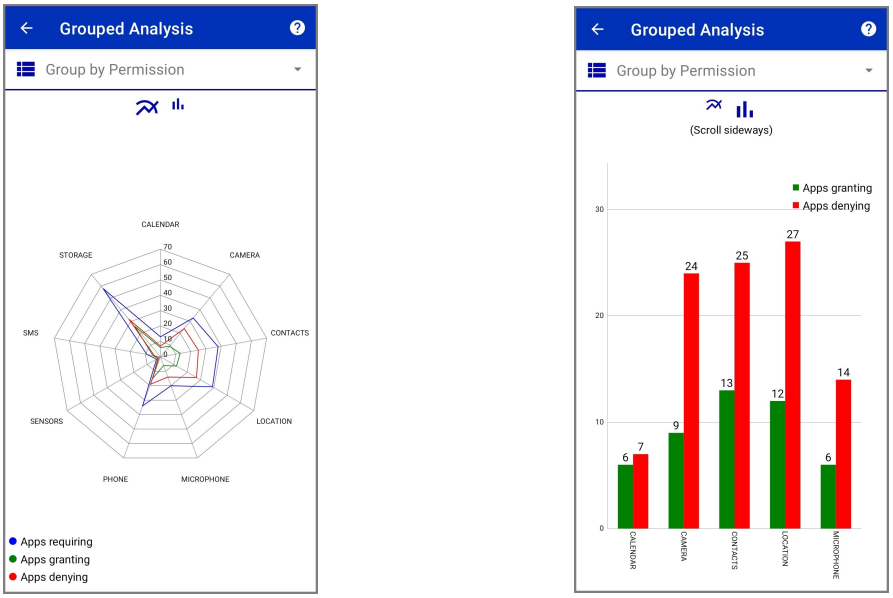
This screen contains a horizontal scroll view for all the available permission groups. For each one a list with the applications is displayed, having that certain permission group granted, or the ones which have seen its access denied, according to the user selection. The information button on the top bar, when clicked, shows a small description for each permission group under the corresponding icon, which has the same effect as clicking on the permission group icon itself.




(A) Granted apps for *Contacts* group permission. (B) Denied apps for *Contacts* group permission.

FIGURE 3.12: Group by Permission screen.

For this subsection of Grouped Analysis in the application there are two available graphs. The first one, figure 3.13a is a radar chart which is able to give the user a general idea of the number of apps requiring, granting and denying each of the permission groups. The second graph was actually divided into two bar charts due to its size, being the first presented in figure 3.13b and having another one similar but with the remaining permission groups. They both contain, for each permission group, the number of applications granting and denying it. The number of apps requiring that group permission was not contemplated here for three reasons: it is not the focus of this graph, can be calculated by adding the apps denying with the apps granting and can be consulted in the radar chart. With the radar chart it is easier to get a quick idea of the general situation related to permission groups and the bar charts provide the exact values of applications granting and denying them.



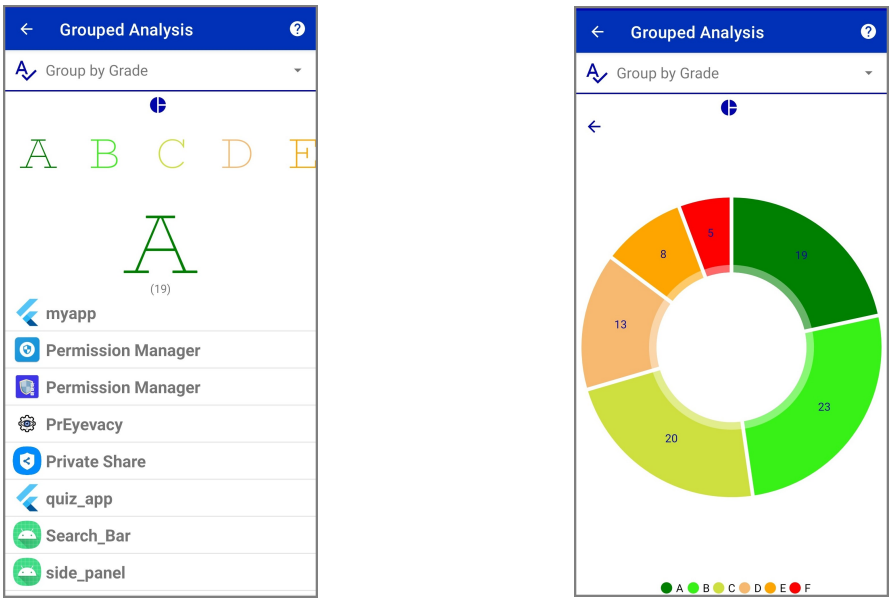

(A) Radar chart. (B) Bar chart.

FIGURE 3.13: Group by Permission charts screen.

#### 3.3.4.3 Group by Grade

As seen in figure 3.14a, similarly to the last subsection, this one contains a horizontal scroll view containing the grades from A to F. Each one is painted with a determined colour according to what it represents. A is painted green and F is painted red. By selecting a grade, that same grade letter is shown in a larger size in a view below, under which the number of applications is shown to which were assigned the selected grade and also

the corresponding list of apps. It is also possible to consult a pie chart containing the distribution of applications by grade, visible in figure 3.14b.




(A) Group by Grade. (B) Pie chart.

FIGURE 3.14: Group by Grade and its pie chart screens.

Clicking on the bigger size grade letter already mentioned, or on the top bar information icon, a new information screen is opened where the user can read everything there is to know about grades in our application, partly visible on figure 3.15.

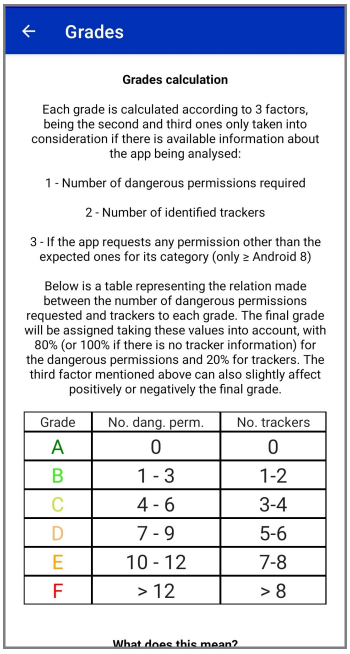



FIGURE 3.15: Grades information screen.

We now explain the process of grade assignment. Each grade is calculated according to 3 factors, namely:

- 1 - Number of dangerous permissions required;
- 2 - Number of identified trackers;
- 3 - If the app requests any permission other than the expected ones for its category (only $\geq$ Android 8).

The second and third factors are only taken into account for assigning a grade if there is available information for the app under consideration. The expected permissions for each category, mentioned in the third factor, will be explained in subsection 3.3.4.4.

A grade is assigned by obtaining a position from 0, grade A, to 5, grade F. The relationship between each position with the first two factors are represented in table 3.8. Based on this table, we will pick the grade position, on the left column, for the first and second factors according to the numbers of dangerous permissions and trackers for the specific application being analysed.

TABLE 3.8: Grades calculation.

| Position (Grade) | No. dangerous permissions | No. trackers |
|---|---|---|
| 0 (**A**) | 0 | 0 |
| 1 (**B**) | 1 - 3 | 1 - 2 |
| 2 (**C**) | 4 - 6 | 3 - 4 |
| 3 (**D**) | 7 - 9 | 5 - 6 |
| 4 (**E**) | 10 - 12 | 7 - 8 |
| 5 (**F**) | >12 | >8 |

To assign a grade there are some different scenarios, with the first factor mentioned above always taken into account:

- Has tracker information: $1st factor * 0.8 + 2nd factor * 0.2$
  - Has category information:
    - Requests non-expected permissions: + 0.35
    - Requests only expected permissions: - 0.35
- Does not have tracker information:

- Has category information:
  - Requests non-expected permissions: add two dangerous permissions and calculate 1º st factor
  - Requests only expected permissions: subtract two dangerous permissions and calculate 1º st factor
- Does not have category information: take only into account 1º st factor

To exemplify the above scheme, an application with 8 dangerous permissions and 2 trackers, and requesting non-expected permissions for its category will have its grade assigned as follows: $3 * 0.8 + 1 * 0.2 + 0.35 = 2.95$. This value is rounded to 3 and the assigned grade is D.

This will guarantee that both the number of trackers and the permissions requested according to the app category will take effect, if there is enough information, in the final application grade assignment.

There is one important aspect to be noticed. The assignment of grades to applications cannot be altered by the user by changing any kind of settings. Contrary to the Group by Privacy Level analysis described in subsection 3.3.4.1, this analysis is based on non-changeable aspects of each application, and each app can only assigned to a different grade than before if one of the following things happen:

- we change our grade calculation formula;
- the analysed app is upgraded (or even downgraded);
- the information on the application trackers change.

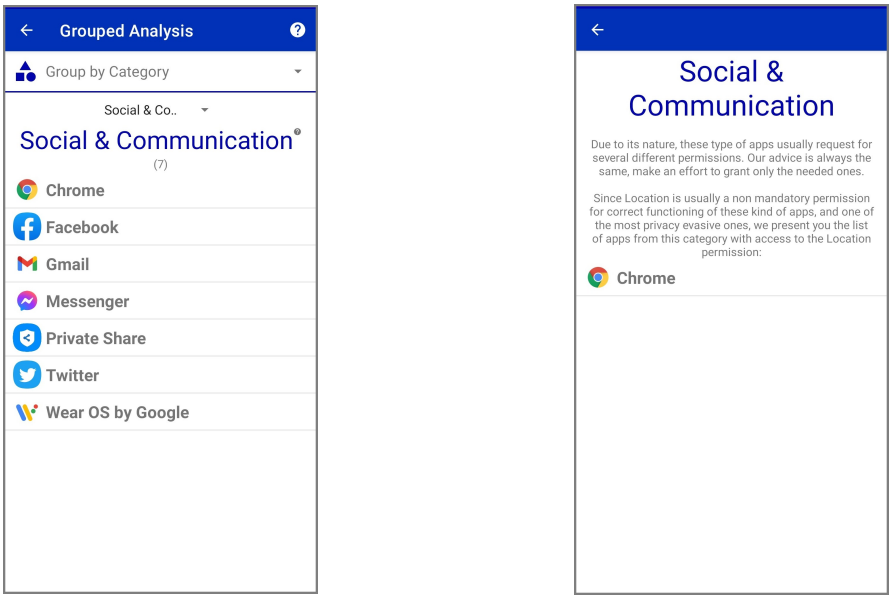
#### 3.3.4.4 Group by Category

This subsection will only be available on devices with Android 8 or greater, since before it was not possible to obtain category information. As seen in figure 3.16a, a small drop-down box allows to select the category. Right below it is presented a clickable title of the selected category and the list of applications belonging to it. The top bar button shows some explanation text on the categories division and its purpose. The main objective of this study is to observe whether applications are being granted permissions other than the ones expected for its own category. The expected permissions for each category were

gathered through the analysis of at least 10 of Google Play Store apps from the 'Recommended for you' section and other top suggestions, without being logged in, for each category.

By clicking on the category title, or the little information button near it, a new screen, visible in figure 3.16b is opened containing a small description of what is expected to be granted for that category and below it the list of applications with granted access to other permissions is presented. We will now explain which permissions we are expecting for each category:

- **Games** - *Storage*.
- **Music & Audio** - *Storage*, *Microphone*, *Phone*.
- **Movies & Video** - *Storage*, *Camera*, *Microphone*.
- **Photos & Images** - *Storage*, *Camera* (it may make sometimes sense to ask for the *Microphone* permission, but we though better not to consider it).
- **Social & Communication** - This type of apps tend to ask several different permissions, so in this case we opted to show users which apps have granted access to the *Location* permission since most of the cases it can be deactivated without interfering with the app main functionalities.
- **News & Magazines** - *Storage* (some apps from this category also ask for *Location* permission to personalize the news to be shown, but still we did not consider it as one of the expected permissions).
- **Maps & Navigation** - *Location*, *Storage*.
- **Productivity** - Due to its nature, these type of apps can request several different dangerous permissions. The user is invited to analyse these apps according to the number of granted dangerous permissions in the Group by Privacy Level section of our application.
- **Undefined** - Here applies exactly the same case as of Productivity category by the fact that we do not have information on the application category, and so the user is advised to analyse these apps in the Group by Privacy Level section of the application.




(A) Group by category. (B) Category information.

FIGURE 3.16: Group by Category and specific category screens.

### 3.3.5 Device Settings

Android settings are usually well organized and easy to understand. However, especially for non-IT people, it may pose some difficulty to find some specific settings. In an attempt to help users find the most important settings related to privacy and security, this section in the application was created and is divided in three categories visible in figure 3.17 and explained below:

- **Status Settings** - Here is presented the status for each setting, painted in red or green according to whether it is harmful or not to the user privacy/security. The user is shown an explanation text when clicking the setting and, for when it is possible to be performed, another click redirects the user to the corresponding Android settings screen.
  - Device lock protection;
  - Install from unknown sources (only $<$ Android 8);
  - Ads personalization.
- **Specific Settings** - For each of these settings, an explanation text is presented when clicking on the information button, and the corresponding section in Android settings is opened when clicking in the setting name itself.

  - Device admin apps;
  - Install from unknown sources (only $\geq$ Android 8);
  - Default apps (only $\geq$ Android 7);
  - Google Play Protect;
  - Accounts and Sync;
  - Location Service.

- **General Settings** - Clicking on this type of settings will directly open the Android settings corresponding section, which due to its general nature will allow direct navigation to several of the others mentioned above.
  - Security Settings;
  - Privacy Settings.

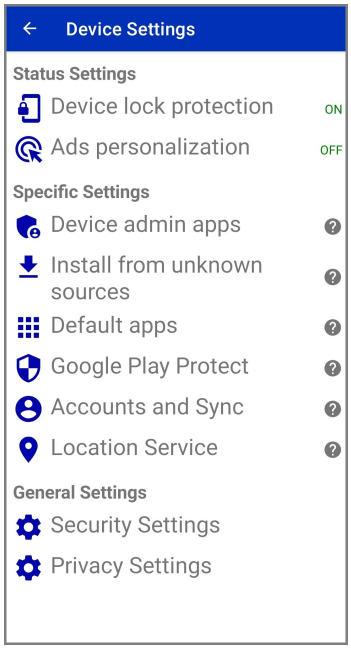



FIGURE 3.17: Device Settings screen.

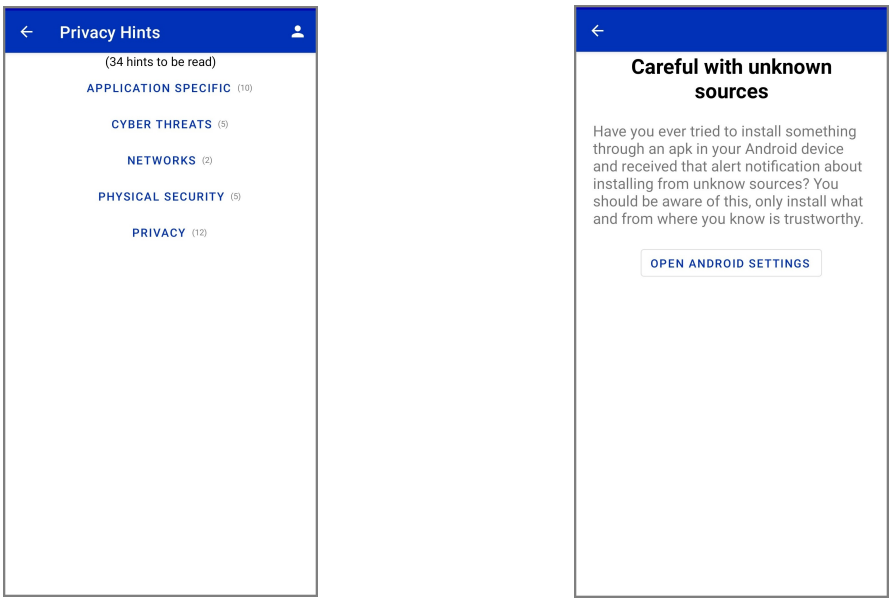
### 3.3.6 Privacy Hints

With several of our discussed features, we intend to help people making their own analysis of their applications. By presenting news, we want to keep people informed about privacy related issues. In here, we want to advise the user through privacy and security hints, presenting them grouped by categories. All the hints and categories can be

changed at any time in the database by developers, and so there is no need to update the application to receive new hints updates.

To help the user keep track of which hints were already read, the total number of hints to be read is displayed as well as the respective amount for each category. Hints to be read are highlighted in bold and so more noticeable. New hints are included in a different and highlighted category, only to be considered as no longer new when this category is opened. The presence of new hints is visible in this section's button at the application main screen through a colourful icon.

As of the current implementation, all the hints are loaded from the database, assuring not only new hints, but also modified ones are always updated in the application. However, as will be described in future work, a way of getting only the new and modified hints is considered an improvement. All hints that are retrieved are saved locally and so, when opened without internet connection, this screen will display all the saved hints and inform the user that the device is offline, allowing him/her to refresh the screen.




(A) Hints list screen, divided into categories. (B) Hint screen.

FIGURE 3.18: Hints section.

In the top bar, the user can select whether he/she wants to see all the hints, which is the default behaviour when opening this screen, or a selection of them considered to be adapted to him/her. This selection is made based on the device brand and the applications installed on it. In a short text, the user is informed in what this selection consists of. This selection of hints to the user, according to its device, is important to create a

more direct connection between our application and each user and help him/her make the necessary changes in the device.

When the user selects one hint, a new screen is displayed, figure 3.18b, containing the hint title together with a short to medium size description text. In order to make hints more practical and help users make the necessary changes to increase their privacy, we show the user a button that will redirect him/her to the respective Android settings. This behaviour is possible to be added from the database, as explained in subsection 3.4.2, and so users do not need to update the application to see these buttons for new hints. In some cases, it is not possible to have the correct behaviour just by using information from the database, and so when possible to open certain Android settings but not through the database, the hint will present a button redirecting the user to the Device Settings screen in the application, described in subsection 3.3.5, that will allow the user to consult the correct Android settings. These buttons in hints will only be shown to users if their device Android version is compatible with the respective setting.

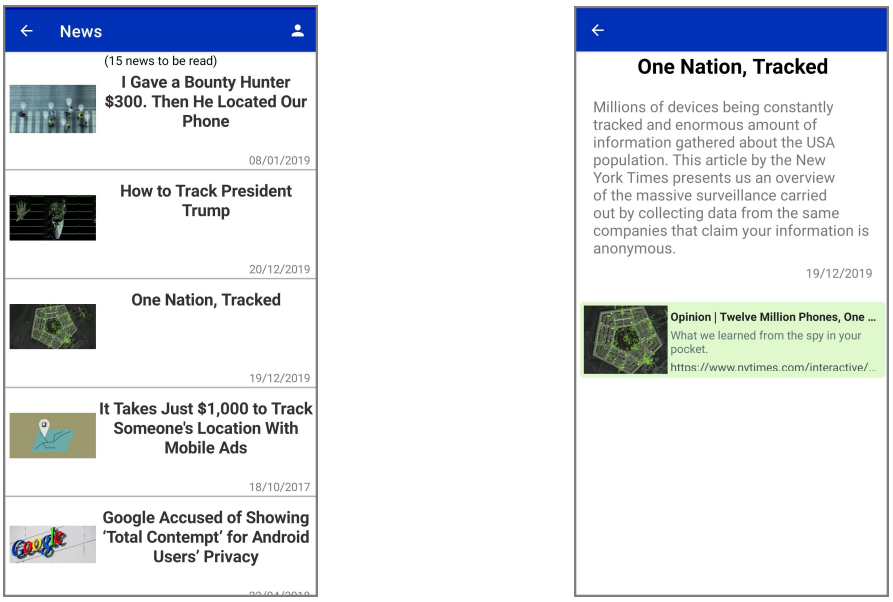
Beyond the implementation, a relevant amount of time was dedicated to gathering information on the 34 privacy/security hints, opting to group them into 5 categories: "Application Specific" (each hint is specific to a certain application, dedicated to some of the most popular), "Cyber Threats" (how to avoid being a victim of a cyberattack), "Networks" (how to access networks safely), "Physical Security" (protect the device and its information from strangers and unexpected events) and "Privacy" (privacy aspects and settings).

### 3.3.7 News

The news section in the application contains several similarities with the hints list screen as it is the case of the news to be read being highlighted in bold and the number displayed at the top of the screen. When new news are available is also noticeable in the application main screen through a colourful icon. A button will allow the user to change between all or just new news (in hints is a new category), and just like hints the news are no longer considered as new only when this button is clicked. Similarly to hints, the user is warned if not having internet connection and is able to refresh the screen. Finally, it is also possible to consult the list of news more suited for the user, based on his/her device's brand and installed applications, being here also possible to target applications based on their category.

Despite the similarities, there are also some different aspects, and we start by pointing out how they are ordered. News are first sorted by if they were already read or not, being the ones not yet read displayed first, and then by date of arrival, which is the same as saying ordered by its insertion into the database. The date of the news itself is displayed below the title. Another different aspect is the possibility of existing news adapted only to Portuguese users, and so will only be displayed when the chosen language is Portuguese.

Beyond the title and date, for each news, the application is able to retrieve an image obtained from the news website metadata (URL shown in the *og:image* tag of the target website). If the application has not yet these images saved locally, it will retrieve and save them, and so they can be presented even if the user re-opens the screen while offline. This image is not necessarily obtained from the website metadata since another one can exist in the database (through a URL), which helps to avoid problems loading certain images. The images size was adapted to different sizes of screens.




(A) News list screen. (B) News screen.

FIGURE 3.19: News section.

There is one more important aspect to highlight. Just like hints, news are retrieved independently of whether they are new to the user or modified, and so this is a task set for future work, however, news are obtained by ranges. The chosen range is 25, considered to be a reasonable value avoiding too much information being retrieved and too less news being shown at each time. The presented number of news to be read is then specific for the visible news range, as well as the shown news when consulting the more suitable ones to the user. News can only be considered as new if they belong to the first range, since

only these news are saved locally, and then possible to be consulted offline, which will reduce the amount of information being serialized each time.

The figure 3.19a shows how the news are listed, and when selecting one of the news article, a new screen (figure 3.19b) is shown containing the news title, an abstract, the date and a clickable source URL. With network connection, this URL is transformed into a rich link preview, which adds an image and some other information, making it more attractive and appealing to the user.

17 news were gathered, from each 2 are in Portuguese, addressing several privacy and security information articles or related events. They aim to inform, alert and increase user interest in the area.

### 3.3.8 Scheduled tasks

A relevant amount of effort was placed on scheduled tasks, working on background, to gather information in order to present useful nudges to users. This aims at improving users privacy awareness by engaging the user soon after the application is installed and keep reminding him/her about privacy matters, even when the interest for the application decreases with time. It is important to mention that some scheduled tasks in the developed application were implemented only for the purpose of the field-study, and that those will only be described in section 4.3.

There are several options to perform scheduled tasks in background, being among them JobScheduler, WorkManager, BroadcastReceiver and AlarmManager. The chosen one was AlarmManager since it was the best to perform operations at defined times with regular intervals in a timely manner, allowing to decide how often to present the user with certain nudges. This way, we were able to consider which period(s) of the day the users would be more receptive for the nudges. A schedule based on constraints has its advantages, like executing certain tasks when there is network connection, but is more directed at operations to be performed on certain events and without regular intervals between them.

In table 3.9 is presented information, for each task, about when it is executed for the first time, the interval to be executed again and how it is rescheduled in case the user reboots the device. As stated by the authors of the study 'Functional Digital Nudges: Identifying Optimal Timing for Effective Behavior Change' [72], the optimal timing to present nudges will depend on what we want to achieve. Some examples are presented

in the study, for example, nudging the user before a meal when he/she is trying to keep a healthy diet, that enforce a connection between nudging and a certain event or action. In our case, we do not have that type of connection, however, we intended to choose to correct timing to nudge users based on when we think they may be more receptive. In the task 'Hints and News', we opted to present them during/after lunch, believing most users will be less busy and more relaxed at this moment, and then more receptive to open and read our nudges. The following subsections will be dedicated to each of the tasks.

TABLE 3.9: Scheduled tasks.

| Task | Start * | Repetition interval | Restart from boot ** |
|---|---|---|---|
| Hints and News | Following day (2:00 pm) | 1 week | Same day (2:00 pm) |
| Installed Apps and Security Progress | Following day (5:00 pm) | 1 day | Same day (5:00 pm) |
| Trackers Update | 1 minute after | 1 week | After 24h |

* from installation moment

** when restarting on same day at some hour, if is passed the defined hour the notification appears as soon as possible

#### 3.3.8.1 Hints and News

This task starts by checking the existence of new hints or news, and if it does, informs the user through a nudge which will redirect him/her to the hints or news list section, respectively. If there are both new hints and news, then the user is redirected to the application main screen where colourful icons indicate the existence of new hints and news, as described in subsections 3.3.6 and 3.3.7.

If there are no new hints and news, then a hint will be suggested. The choice of the hint to suggest favours hints yet to be read and, among these, the ones which are able to redirect the user to Android settings.

#### 3.3.8.2 Installed Apps and Security Progress

The first performed operation here is to check if there are new installed apps which are evaluated by our application with a low grade. As mentioned in subsection 3.3.4.3, grades vary from A to F, and we consider E and F to be low grades. If one or more apps evaluated

like this are found, then the user is informed which one(s). The nudge will redirect the user to the *Application Analysis* section with information about the found application with low grade (chooses the first to be found if there are more than one).

Independently of being or not found new low grade apps, this task will always check and save the number of launchable applications for each privacy level. To know more about privacy levels consult subsection 3.3.4.1, where the graph dedicated to this information is mentioned, and visible in figure 3.11, showing the progress of the number of apps in each privacy level in the measured period, which goes up to fifteen measures.

After performing what is described in the last paragraph, the user can be presented with a nudge to invite him/her to consult the mentioned progress graph if these four conditions are met: no new low grade apps were found, the day of the month is 1 or 16, there is enough information for the graph to be visible and there are changes in the measured period on the number of apps by privacy level.

#### 3.3.8.3 Trackers Update

This task is the less frequent but at the same time the first to be executed. The only performed action is to update the trackers information and no nudge is shown to the user about it. If a user tries to update trackers while they are already being updated on the background, he/she is informed about the background processing already performing such operation.

## 3.4 Server side / Backend

For the developed application, a server belonging to the COP-MODE project was chosen to hold the database and a website to interact with it, two components we will further detail in the next subsections. In figure 3.20, the possible interactions between the app, database and website are presented, together with which actor is allowed to perform each operation.

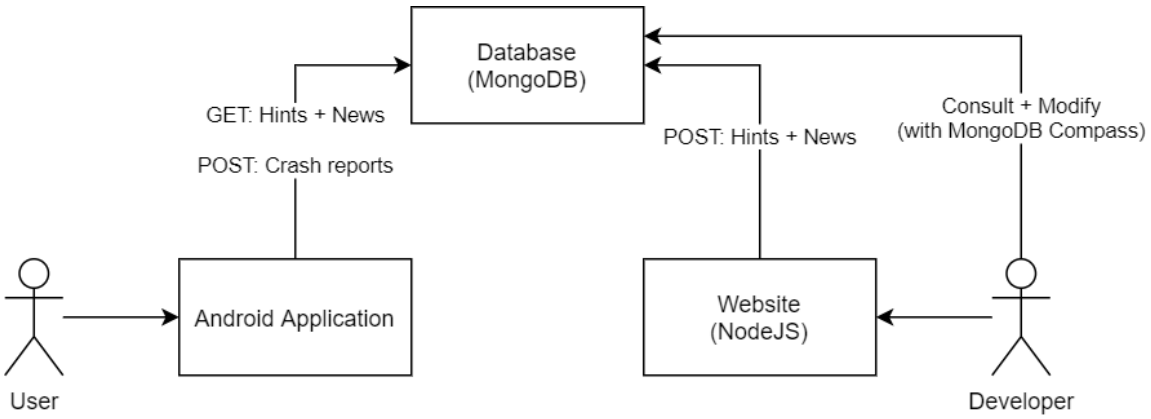



FIGURE 3.20: Application, Database and Website interactions diagram.

### 3.4.1 Database

To store information on server-side, it was chosen the MongoDB database [73]. Characterized as a NoSQL database, MongoDB offered what was required for the purpose, having these as some of its main advantages: powerful querying with excellent performance, well documented, light weight, provides an easy to understand graphical interface to interact with. The huge scalability of NoSQL databases made this a preferable choice to any other SQL database. It also provides good security, with some features like the ones we will discuss below, and, being NoSQL, is not vulnerable to SQL injection [74] [75] [76].

Two databases were created: COPMODEAndroid, containing the collections *hints* and *news*, and COPMODECrashReport with collection *crash*. Also, two users were created: *admin* will full access to all collections, and *user*, with read-only permissions to COPMODEAndroid database and read and write permissions to COPMODECrashReport. Knowing this, the *admin* user is only used by the developers and the server website, to insert hints and news (discussed in subsection 3.4.2) and the other user, named *user*, is used by the developed application. As already mentioned in section 3.3, the application store safely the credentials to connect with the database. The server website can only insert and not modify or delete hints and news since MongoDB provides an excellent graphical interface program, MongoDB Compass [77], which makes the interaction with the database information very easy.

Due to the nature of information, it was not found important to store it encrypted. All the transferred information does not contain any private/sensitive data, and so the communication is not encrypted, which improves the network communication performance and respects the requirement of maintaining a simple server-side.

### 3.4.2 Server Website

The purpose of this website is to insert hints and news into the database. The chosen technology to develop it was, apart from *HTML* and *CSS* for client-side, *Node.js* for server-side. *Node.js* offers many advantages that we value, as it is the case of scalability, ease of learning and extended support [78] [79].

A *README.md* file was created to help future developers with how and what information can be inserted, listing all the mandatory and optional fields and explaining each one. Although this file can be consulted, all the main information can also be consulted in the website screen itself in tooltips for each text field. It is important to remind that this website is only for inserting hints and news and not to modify or delete them. As mentioned before, an external graphical interface can be used for it.

About security aspects, this website will connect to the database with the highest privilege user to be able to write hints and news information. For now, the website requires no authentication to be used, which respects the non-functional requirements of this work, simplifying the server-side implementation. To assure someone non-authorized cannot add information at any time, this website is only active when needed to be used.

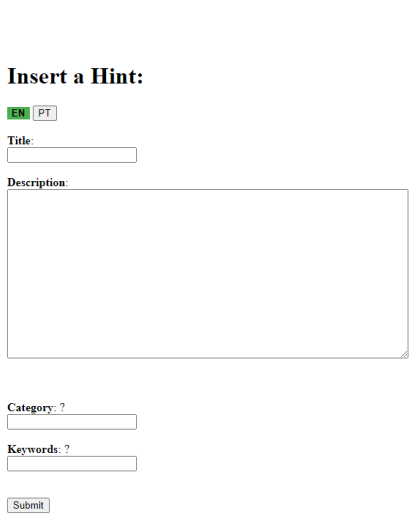
The information that can be inserted is as follows:

- Hints (figure 3.21a)
  - Mandatory fields *title* and *description* for both Portuguese and English.
  - Mandatory *category*, written in English and case-insensitive, must be one of the available ones in the server. Translation to Portuguese is automatic, and a tooltip lists the available categories.
  - Optional *keywords*, explained by a tooltip what and how can be inserted. Data that can be inserted: app package names, device brands and special codes for the application to associate the hint with Android settings.
- News (figure 3.21b)
  - Mandatory *title* and *description* in English and Portuguese (possible to insert news only in Portuguese).
  - Mandatory news *date* (tooltip indicating the necessary news format).
  - Mandatory news *source*.

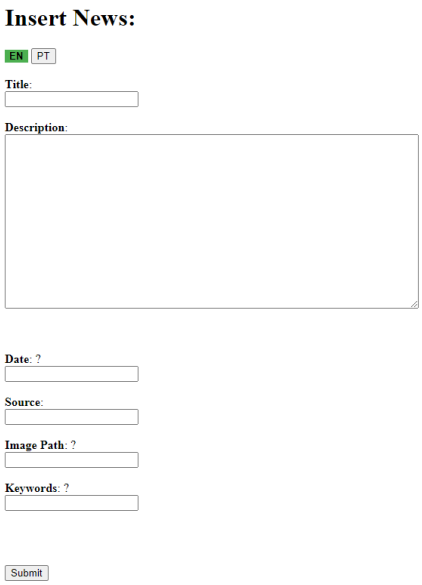
- Optional *image*, which can be, as explained in the tooltip, a website image URL or a path for a local image, placed inside a folder destined for it.
- Optional *keywords*, explained in a tooltip, in which can be inserted: app package names, device brands and numeric values corresponding to apps categories, described in subsection 3.3.4.4.

All the inserted data is validated and error messages are shown for every wrong inserted information and when mandatory fields are left empty. Beyond the mentioned information, an *id*, which will be used to uniquely identify each hint and news article, is also inserted and consists of a timestamp concatenated to a random number up to a thousand.

The figure 3.21 shows the website sections to insert hints (3.21a) and news (3.21b).




(A) Website: Hints section.




(B) Website: News section.

FIGURE 3.21: Hints and News website.

## 3.5 Testing

Throughout the development process, the application was continuously tested to avoid unexpected behaviours. These tests were focused on two main aspects:

- The interaction with the user interface - to guarantee the correct functioning of both graphical interface and associated running code. This type of testing was the most

common and is based on simulating a normal use of the application, contemplating cases most likely to cause errors.

- Background/scheduled tasks - these tests are more complicated due to the "invisibility" of most actions and difficulty of catching errors. Due to the amount of scheduled tasks used, this type of tests was very common. They focus on guaranteeing the right actions are performed at the right time.

Beyond manual tests, some automatic testing was implemented directed at the UI responsiveness. This helps to avoid that changes in the code create unexpected behaviour interacting with the user interface and that adequate response times are maintained.

On the server-side, the testing was performed during the current insertion of news and hints by analysing the website response to the inserted data. The inserted data was then verified in the database and checked if correctly retrieved by the application.

Finally, the field-study itself results as a crucial test since the application is used by several participants in their daily lives. The feedback provided in the final survey, that will be discussed in section 4.5, constitutes a major help to identify aspects to be corrected and improved. The post-survey contains some questions that were used as usability tests and which are discussed in subsection 4.5.4.

## 3.6 Conclusions

This chapter focused on the development process and its final result, starting by listing the defined requirements, both functional and non-functional. Following, the application is described, explaining several implementation decisions divided in the main sections of the application. All the scheduled background processing is also detailed, justifying their utility and scheduling intervals. Another section is aimed at the server side implementation, contemplating the server website and the chosen MongodDB database. Finally, the several testing procedures and their intent are described.

# Chapter 4

# Field-Study for privacy awareness

This chapter will be fully dedicated to our field-study, whose main objective is assessing the effectiveness of the app on user's privacy awareness. Beyond this, we aim at obtaining feedback from the app and seeking answers to the questions listed in subsection 2.3.2, to which contributed both the surveys' answers and the collected data. The field-study was performed for a period of 10 days and contained two in-app surveys, one at the beginning and another at the end. With 42 participants deciding to participate when the field-study started, 32 participants contributions were considered valid. Each participant confirmed to be above 18 years old and agreed to the data collection which, as informed, does not contain any sensitive information. The final reward was a 20€ FNAC Gift Card, conditioned on the effective use of the application.

Although the application was developed to be supported by Android 6.0 or higher, as mentioned in section 3.3, for this field-study we have only accepted users with Android versions 8.0 or higher. This was due to lack of testing of the nudges' system on versions 6 and 7 and because the Group by Category app section is not available in versions below 8.0, as explained in subsection 3.3.4.4.

The first sections, 4.1 and 4.2, will focus on each of the surveys and what we intend to obtain with them. Section 4.3 details the scheduled tasks and their purpose, and section 4.4 focuses on the data collected from participants' devices. Finally, section 4.5 will perform the analysis of both the surveys answers and collected data.

## 4.1 Pre-Survey

The pre-survey was divided in sections with the following purposes:

- declaration of over 18 years old and email is requested (to ensure that all participants answer the surveys, but without any intention to match the answers with the corresponding participant);
- participant demographic information;
- previous knowledge in the IT area, with smartphones and privacy on smartphones;
- what kind of privacy actions did users already know and put into practice.

## 4.2 Post-Survey

The second, and final, survey was divided in sections with the following purposes:

- understand how knowledge in the IT area evolves about smartphones and smartphone privacy;
- understand whether the use of the application has led users to acquire new practices to protect their privacy;
- get feedback and suggestions for improvement, both on functionalities and usability.

The user email is not asked here since it was saved locally and automatically sent. The user is notified to fill in the survey at 2pm of the last day of the field-study, with a daily notification until the survey is submitted.

## 4.3 Scheduled Tasks

In subsection 3.3.8 several background running tasks for improving users privacy awareness by presenting them nudges were already described. However, they were created to be part of the app in its final stage when available to the public, and so here some tasks dedicated at engaging users only in the context of the field-study are described.

The table 4.1 lists the tasks and presents some brief information about them. Below it, we further detail each task, having as basis what was already written in subsection 3.3.8 for each one.

TABLE 4.1: Scheduled tasks exclusive of the field-study.

| Task | Start * | Repetition interval | Restart from boot ** |
|---|---|---|---|
| Hints and News | Following day (1:30 pm and 6:30 pm) | 1 day | Same day (1:30 pm and 6:30 pm) |
| Installed Apps and Security Progress | Following day (5:00 pm) | 1 day | Same day (5:00 pm) |

* from installation moment

** when restarting on same day at some hour, if is passed the defined hour the notification appears as soon as possible

### 4.3.1 Hints and News

In the context of the field-study, this task has seen its frequency increase to twice a day with a daily appearance. However, the biggest difference is related to the type of hint to be chosen and even, in some cases, relevant information other than hints. We have chosen then to present the user with 13 specific nudges, each one with a specific purpose, presented in table 4.2.

TABLE 4.2: Scheduled nudges.

| No. | Nudge | Related survey question | Collected data |
|---|---|---|---|
| 1 | **Hint**: Inform users about ads personalization and advise to disable it | **Checkbox option**: 'Turn off ads personalization' | - |
| 2 | **Hint**: Suggestions of alternative applications that have better respect for the user privacy | - | If users have installed, or replaced their applications for the suggested alternative apps |

**Table 4.2**: Continued from previous page

| | | | |
|---|---|---|---|
| 3 | Alerting the user for the applications with the worse privacy level, listing them and inviting the user to check if any permissions can be revoked | - | Number of applications by privacy level |
| 4 | **Hint**: Advise to only have the location service active when strictly necessary | **Checkbox option**: 'Avoid having the location service active except when strictly necessary' | Location service status at the beginning and end of the field-study |
| 5 | **Hint**: Suggestions of alternative communication applications that have better respect for the user privacy | - | If users have installed, or replaced their applications for the suggested alternative apps |
| 6 | Information about what the 'Phone' permission group gives apps access to, redirecting the users to the list of apps with this permission group granted | **Checkbox question**: 'An application asking for the "Phone" permission will ask "Allow X to make and manage phone calls?". If this permission is allowed, what do you think this permission will allow the application to do?' | Number of granted permissions from this permission group |
| 7 | **Hint**: Advise to use a safe web browser | - | If users have installed, or replaced their applications for the suggested alternative apps |
| 8 | **Hint**: Explanation of the importance of locking the device and listing of locking options | - | Device locking status at the beginning and end of the field-study |

**Table 4.2**: Continued from previous page

| | | | |
|---|---|---|---|
| 9 | **Hint**: Suggestions of alternative online sharing applications that have better respect for the user privacy | - | If users have installed, or replaced their applications for the suggested alternative apps |
| 10 | **Hint**: Advise users to manage, in their device settings, how Google can use their data | **Checkbox option**: 'Check Google service settings on your device by changing how your Google account(s) controls your data' | - |
| 11 | Information about what the 'SMS' permission group gives apps access to, redirecting the users to the list of apps with this permission group granted | **Checkbox question**: 'An application asking for the "SMS" permission will ask "Allow X to send and view SMS messages?". If this permission is allowed, what do you think this permission will allow the application to do?' | Number of granted permissions from this permission group |
| 12 | **Hint**: Advise users to use incognito mode in their devices to better assure their privacy | **Checkbox option**: 'Use incognito mode (e.g. in browsers, Youtube, Google Maps, etc.)' | - |
| 13 | Alerting the user for the applications in the worse privacy level, listing them and inviting the user to check if any permissions can be revoked (same as number 2) | - | Number of applications by privacy level |

In figure 4.1 is visible an example of a nudge. The reasoning behind the selection of the hints/nudges is as follows:

- **Nudges number** 1, 4, 10 and 12: 3 checkbox questions, one in the pre-survey (question A.24), and two on the post-survey (questions B.14 and B.20). These checkboxes will help to understand if the user was already aware of those subjects, if interacted with them during the field-study and if intend to pay attention to them in the future. The nudge number 8 will, just like number 4, help understand if users changed certain service status to improve their privacy.

- **Nudges number** 2, 5, 7 and 9: these nudges will only appear if the hint is considered adapted for the user, in other words, if the user has installed the applications we suggest to be replaced. We will analyse these nudges' effectiveness by observing if users have performed the suggested apps alterations.

- **Nudges number** 3 and 13: the objective is to alert and remember the user to check if any permissions can be revoked on the apps requesting the most. It is listed the applications in the *Dangerous* privacy level, or in the *Medium* privacy level in there are no apps considered as *Dangerous*.

- **Nudges number** 6 and 11: here the user is shown some information on what these permissions groups may allow the applications to perform. The users' knowledge evolution on these permission groups will be evaluated with checkboxes in the pre-survey, questions A.19 and A.18, and two more on the post-survey, questions B.8 and B.7.




FIGURE 4.1: Nudge example.

### 4.3.2 Installed Apps and Security Progress

In the context of this field-study, the invitation for the user to consult the graph showing the progress for the number of apps in each privacy level in the measured period, visible in figure 3.11, has the same conditions as in subsection 3.3.8 (no new low grade apps were found, there is enough information for the graph to be visible and there are changes in the measured period on the number of apps by privacy level), but instead of checking if the day of month is 1 or 16, checks if the day of the month is multiple of 3 (which had two

occurrences in the field-study period). A warning of low app usage was also added and is shown in a nudge if the app is not used for three consecutive days.

Besides these changes, this task is also used for the collection of some data, namely the 'Total number of granted and denied permissions' and 'Number of granted permissions per app', which can be consulted on table 4.3, and which happens daily.

## 4.4 Collected Data

TABLE 4.3: Collected data for the field-study.

| Collected Data | Frequency | Purpose |
|---|---|---|
| Number of applications 'Grouped By Privacy Level' | Begin and end of the field-study | Understand if the applications in the worse privacy levels decrease |
| Number of applications 'Grouped By Permissions' | Begin and end of the field-study | Understand which permission groups are most affected by users changes |
| Number of applications 'Grouped By Grades' | Begin and end of the field-study | Understand if users opt for applications with better grades |
| General use of the app metrics: usage of the app, visited sections, number of read hints and news | Continuously collected | Understand the type of use given by the participants to our application and which are the most visited sections |
| Total number of granted and denied permissions | Daily collected* | Understand if there is a decrease on the number of total granted permissions throughout the field-study duration and if users tend to make changes only in the first days of using our application |
| Number of granted permissions per app | Daily collected* | Complement the information of total granted and denied permissions, helping to understand how permissions access is changed for each app (we do not collect information on which apps the user has installed) |
| Alternative applications | At the end of the field-study | Understand if suggestions on alternatives apps to improve privacy have a real impact on users by observing if they actually install the suggested apps |
| Status of 'location service' and 'smartphone lock' | Begin and end of the field-study | Check if there are changes in the status of these services in the beginning and end of the field-study |
| Check if the suggested hints (listed in table 4.2) were read | End of the field-study | Help to understand the effectiveness of nudges on the user |

* in task 'Installed Apps and Security Progress' described in subsection 4.3.2

Table 4.3 contains all the collected data from the participants devices, the collection frequency and its purpose. The ones mentioning the beginning of the field-study in their frequency, collect data to be sent when submitting the pre-survey. All of them collect data to be sent when submitting the post-survey. We remind none of the collect data corresponds to sensitive information and are based on numerical values.

## 4.5 Results Analysis

This section will perform the result analysis based on the answers of the surveys and collected data. We will first focus on the pre-survey, then on the post-survey and finally on the collected data. Although we opted for this division, some questions and data will be analysed outside of the context of the survey in which they were collected to better achieve comparative results. We also want to note that, all the citations of participants answers were translated in a way that its idea remains the same.

### 4.5.1 Pre-Survey

Starting with demographics data (questions A.2 to A.5), 75% of participants were between 18 and 24 years old, 19% between 25 and 39 and the remaining 6% between 40 and 60. Almost half, more specifically 47%, already had a degree, 31% had finished basic school and 22% had a master's degree. Predominance for a male public with 72% of answers. About occupation, 56% were from computer science/engineering and 16% other types of engineering, with the remaining participants choosing other options.

For an overview of participants knowledge about the area (question A.6), one participant have been using smartphones for 1 to 3 years, two from 3 to 5 years and the remaining 91% use them for more than 5 years. About a half, 44%, spends from 3 to 6 hours per day on it, with only two participants answering less than one hour (question A.7). As it would be expected, the knowledge in computer technology would be greater than the knowledge of privacy/information security on smartphones. In scales from 1 to 5, the most chosen option on the first question (A.8) was 5, corresponding to the highest knowledge level, with 47% of answers, in contrast with 38% of choices on option 2, the second lowest level and the most chosen, for the privacy/security knowledge (question A.9). Still on question A.9, 28% of participants answered 4, a quarter answered 3 and the remaining 9% answered 5.

It is also interesting to compare how important the privacy of information is for participants with how they consider their devices manages it. On a scale from 1 to 5, the most chosen options were 5 for the first question (A.10) with 44% of participants and 3 for the second question (A.11) with 47%. Figure 4.2 allows to compare the answers to these two questions and realise that participants consider their information privacy is not being given enough value by their devices.

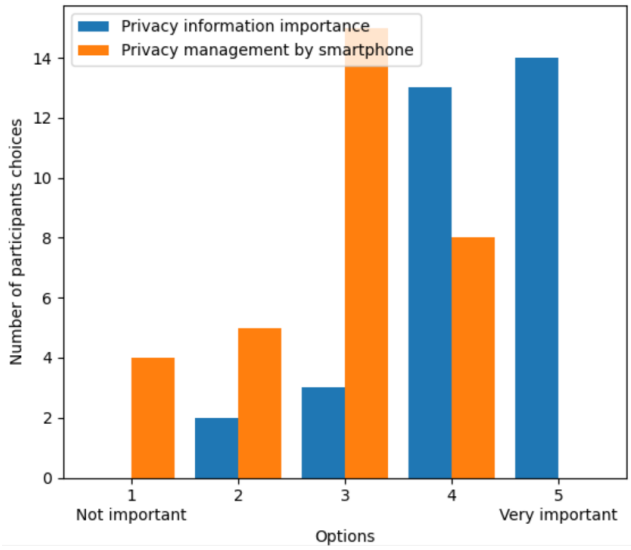



FIGURE 4.2: Privacy information importance VS Privacy management by smartphone.

By asking the participants what they consider it could be done to have a better management of information privacy on smartphones (question A.12), their answers focused in more transparency for the requested permissions and collected data by apps, warnings of when sensitive data is being accessed, preliminary analysis to assure apps really need everything they are asking to access, hinder the propagation of applications known to break the privacy of users and, citing one of the answers, " Creation of apps, such as preyevacy, whose objective is to protect data against other apps that do not care and even benefit from data collection". Participants also demonstrated concerns with the cross-checking of data between various applications that allows to create detailed profiles about users and how the collected data is used and to whom it is sold.

Looking now at a more practical side, 100% of participants claimed to know what app permissions were (question A.14), what was in the majority of the cases confirmed with the text answers to explain that concept (question A.15). In question A.16, although two participants claimed they had never performed changes in the apps permissions and only

other two saying they do it regularly to improve privacy, the rest states that they have already performed changes, with 53% of participants claiming they know reasonably/quite well how to do this and 34% saying they do not do it often and admitted feeling confused about that.

Questioning participants if they care about granting only the necessary permissions to applications (question A.21), 59% claim to grant only the ones they think that are necessary for the type of application, 31% claim to have this concern but only for some applications and the remaining say they do not care about it, granting everything that the application asks for since they consider that if the application asks for it, it is important.

Regarding applications to improve privacy that they have already used (question A.22), only four participants indicated one application, two of them using the already pre-installed security management app on the device. Asked specifically about the use of antivirus, firewall or privacy managers (question A.23), the most chosen option with 44% of choices was "No, although I think I should use", having 22% of participants saying they used this type of application because they considered it important. It is important to notice 16% of the answers choices of not using it because of felling there is nothing to protect on the device, and also the same value of 16% of participants saying they do not use it because of not considering that it will help improve privacy and security.

### 4.5.2 Post-Survey

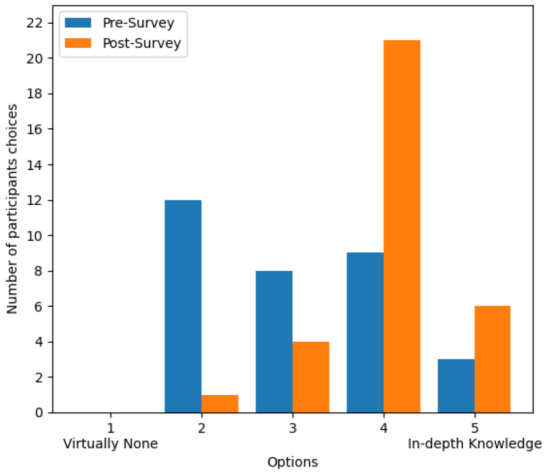
The answers we will analyse on this post-survey will allow to understand the impact that the field study had in the participants using the PrEyevacy application. Several questions from the pre-survey will be mentioned in a comparative analysis of the answer's evolution.

With the 1st question (B.1) we intend to understand the contribution of the application's use. Precisely 50% said they became more knowledgeable in the area and that in the future they will know better how to improve their privacy, with 44% saying it had a good impact but believe they could have been better instructed and the remaining 2 participants (6%) saying that, despite the positive impact, they could not enjoy enough of the application.

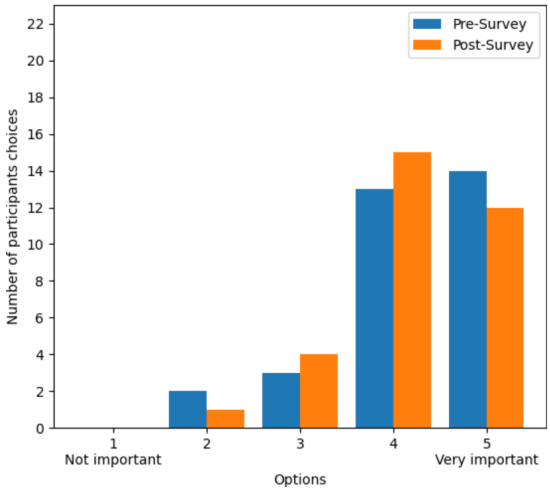
Then the participants were asked (question B.2) to justify their choice to the previous question. The responses are generally very positive, highlighting the help given to participants to better understand permissions, be more attentive to their applications and

privacy settings, be more alert to multiple actions by companies that do not respect the privacy of users, understand more about what certain permissions actually do and gain knowledge of the existence of trackers. Two of the answers were more detailed in which participants said they had learned a lot from the application and stayed significantly more aware by using it, highlighting the news section for giving real world facts that they had no idea, being one of the suggestions to describe what each permission grants to applications.

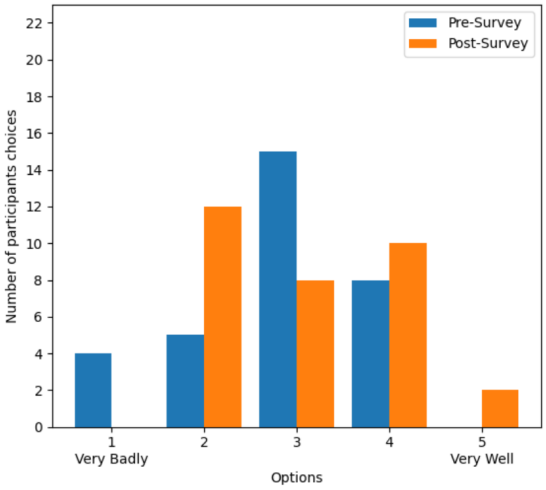
The following three questions (questions B.3, B.4 and B.5) were already asked in the pre-survey and repeated in here. The figure 4.3 allows to compare the answers from the two surveys. Figure 4.3a demonstrates how users think they benefited from using the application, showing they felt our application helped them learn more about the privacy and information security on smartphones. The slight changes visible in figure 4.3b from the beginning to the end of the field-study in the importance given by participants to their information privacy are not relevant enough to obtain conclusions from this graph.




(A) Question: What is your knowledge in privacy/information security on smartphones?




(B) Question: How important do you consider to be your information privacy?




(C) Question: How do you think your smartphone manages your privacy?

FIGURE 4.3: Privacy knowledge questions.

Finally, figure 4.3c demonstrates how participants' consideration for the way their smartphones manage their privacy had slightly improved from the pre- to post-survey. However, just like in figure 4.3b, the results are not representative enough to draw solid conclusions. In fact, an improvement in the post-survey could be because users discovered new settings provided by the device to manage privacy that they did not know, and a worsening could be explained with participants gaining more knowledge of privacy issues and existing dangers. We believe this is the reason why there was neither a strong improvement nor worsening from one survey to the other.

When questioning participants about how they thought their privacy was managed by their smartphones (question B.6), 84% said they think it could be better managed but the most important thing is the user's own action, with 9% of participants saying they show little regard for the privacy of their users and only two participants considering it good enough. This demonstrates the existence of users' perception for the need of being careful with their actions and not only rely on the system protection.

On table 4.2 in subsection 4.3.1 two of the nudges, 6 and 11, focused on teaching the user more about permission groups *Phone* and *SMS*. When asking about these two groups (questions B.7 and B.8), together with *Contacts* group permission (question B.9), which was not explained during the field-study, we sought to find out if these nudges allowed participants to understand more about these groups of permissions. However, the evolution of correct answers between pre-survey and post-survey for each of the permissions groups did not allow to conclude that the mentioned nudges had a positive effect on

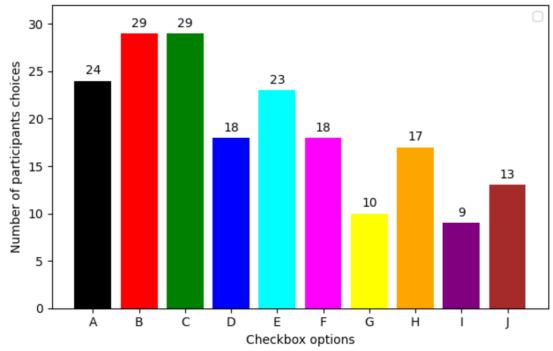
users, as the evolution of correct answers were from 88% to 87% for *SMS* permission, 72% to 70% for *Phone* permission and 86% to 84% to *Contacts* permission. We strongly believe that providing this information in-app about all permission groups, and not only though nudges to certain permission groups, brings a greater benefit to the users' knowledge about this subject.

In the participants' interaction with the application permissions settings (question B.11), 47% said they have made changes during the field-study, 31% answered they feel confident to perform changes in the future and 13% that, despite not having made changes, it was clear how to make them. There are still 3 participants (9%) admitting to still feel some confusion with these settings. Comparing this question with the question A.16/A.17 of the pre-survey, the highlight is for the 2 participants that answered, in the pre-survey, to never have made changes to permissions, and that during the field-study have performed them, understanding how to do it.

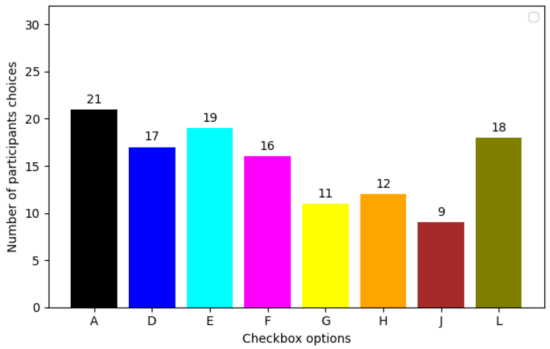
The next question (B.12) asks the participants if they think they will acquire the habit of making changes to the settings to increase their privacy/security on the smartphone. 34% answered that they already had this habit but will intensify their attention regarding these definitions, 16% that they already had this habit and nothing will change, with still 2 participants saying they had not this habit in the past and do not intend to acquire it since they think there is no need for it. The highlight is for the 44% of participants answering that they did not have the habit but were sensitized and that, therefore, will change their behaviour, demonstrating how the developed application had a strong impact on the users' awareness. Comparing with the question A.16/A.17 of the pre-survey, stands out 25% of participants that, even saying they already knew how to make changes, said afterwards they would intensify their attention and 28% that, saying they were not used to making changes to permissions nor did they understand them very well, replied then that they were sensitized and would reinforce their behaviour.

Still in line with the previous questions, the aim is now (question B.13) to find out if users will be more attentive when granting permissions requested by applications. The results demonstrate something similar to those obtained in the previous question, with the same value of 44% to two of the following options, that they did not have this concern but now will only grant the necessary permissions and that they already had this concern but will now be more attentive. Comparing with the question A.21 of the pre-survey, we highlight that all the participants who claimed to grant all the permissions that the

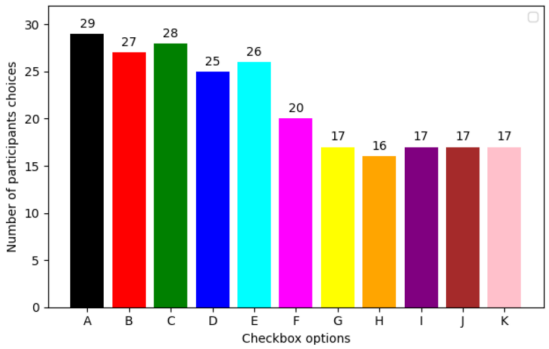
applications asked because they thought they should be important, now say they will be more attentive.




(A) Participants choices on privacy actions they remember doing, before the field-study.




(B) Participants choices on privacy actions they remember doing, during the field-study.




(C) Participants choices on privacy actions they intend to worry about, in the future.

FIGURE 4.4: Participants choices on privacy actions.

**A** - Change privacy permissions in your own app settings

**B** - Always keep your smartphone version up to date

**C** - Update your apps regularly

**D** - Check whether the applications used by default are reliable or should be changed

**E** - Avoid having the *Location* service active except when strictly necessary

**F** - Turn off ads personalization

**G** - Check Google service settings on your device by changing how your Google account(s) controls your data

**H** - Use incognito mode for privacy reasons (e.g. in browsers, Youtube, Google Maps, etc.)

**I** - Uninstall some application to install another similar one with fewer permissions

**J** - Uninstall an application because of permissions

**K** - Use an antivirus, firewall or privacy manager

**L** - Update your apps and/or your smartphone software

By analysing the figure 4.4 above corresponding to participants answers to three similar questions with checkboxes, one from the pre-survey (question A.24) and two from the post-survey (questions B.14 and B.20), the actions participants are most concerned about are those corresponding to the letters A, B, C and E. In a rough analysis, there are generally no significant changes, however, we see a positive evolution from figure 4.4a to 4.4c with emphasis on privacy actions of letters D, G and I, having this last one seen a considerable evolution in its number of participants who were worried and intend to worry in the future, corresponding to the replacement of applications by similar ones with less permissions. This evolution may be due to some hints we presented dedicated to encouraging users to replace their apps for some other known to better respect their privacy, which can be seen in table 4.2 on nudges 2, 5, 7, and 9. In figure 4.4c it is also verified that, even with only 25% of the participants, corresponding to 8 out of 32, who stated in question A.23 of the pre-survey that they used antivirus, firewall or privacy manager, here we obtain a value of 17 participants stating that they will be concerned about this issue in the future, which is evidence of raised privacy awareness.

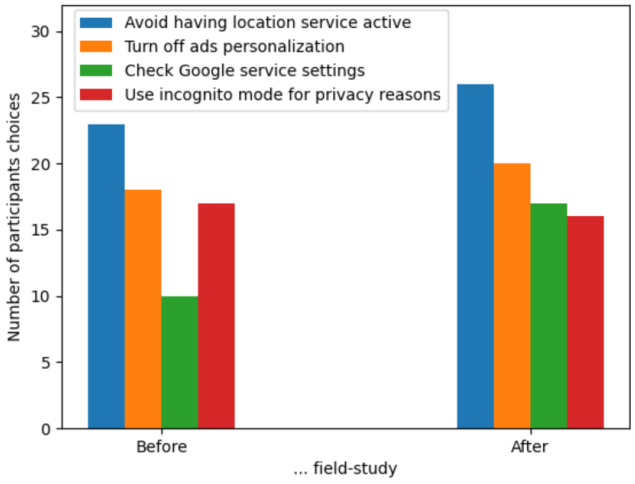



FIGURE 4.5: Privacy actions performed by participants.

In figure 4.5, we focus on the evolution of 4 of the options (corresponding to letters E, F, G and H) from the above mentioned privacy actions, getting the number of participants that already worried with them and intend to be concerned about in the future. These 4 options were chosen to evaluate the effect of nudges 1, 4, 10 and 12 from table 4.2. The actions that were able to gain more attention than before with this field-study were the

*Location* service turned off, being also the most chosen one on both periods of time, the deactivation of ads personalization with an increase of just two participants choices, and checking the Google service settings which was the one that caught the most attention of participants with an increase of 7 participants choices between surveys. Participants do not seem to concern so much about the use of incognito mode to protect their privacy, which is a non-surprising point since even in our hint about this subject we have alerted this technique cannot avoid most of the tracking.

From the aforementioned checkboxes questions, one of them refers to actions that the participant remembers having performed during the field-study. When selecting the first option, "Change privacy permissions in your app's own settings", 2 other questions are presented. The first is to ask the reason for the changes they remember making (question B.15). Most participants justify that they removed the permissions because they thought the application did not need them. One of the participants focused on the information our app provides about which applications request permanent access (in the background even without the user's knowledge) to the *Location*, *Camera* and *Microphone* permission groups. In the second question (B.16), the participant is asked to indicate permissions that he/she has seen and was not expecting to be requested. Many of the participants stated that they did not remember, but some presented specific cases, presenting the access of the email application to the call log, games accessing *CAMERA* and several apps asking for the *LOCATION* permission when it did not seem to be necessary as some examples.

In question B.17, participants were asked if they had uninstalled any application to install another one with less permissions. 25%, 8 participants, answered positively, to whom was asked (question B.18) if they intend to keep and continue using these replacement applications. The answers demonstrate both satisfaction with the new application for doing the same with less permissions and some confusion for having to adapt to a new application. Three replacement applications were mentioned in the text answers: Tor [80] (probably instead of Google Chrome [81]), Silence [82] instead of WhatsApp [83] and Firefox [84] instead of Google Chrome.

Participants were also asked (question B.19) to indicate some privacy actions that they remember having taken in addition to those already mentioned in the checkbox's options. In the responses, several actions were mentioned, including disabling ads personalization, analysing applications based on assigned grades by our app, reading hints and

seeing which trackers are present in the applications, changing WhatsApp to Signal, using *Location* only when necessary, reviewing social account settings, using incognito mode and deactivating unnecessary permissions. This demonstrates how the application was able to sensitize users to several aspects related to their privacy, and also the effectiveness of nudges since actions related to the nudges 1, 3/13, 4, 5 and 12 from table 4.2 were mentioned. We also highlight one of the comments: "I especially liked the recommendations for apps that have better privacy (I already use Brave and plan to change others in the future)", in which the participant praised hints suggesting apps that have greater respect for the user's privacy, which were presented with the nudges 2, 5, 7 and 9 of the aforementioned table.

### 4.5.3 Relevance of Privacy Functionalities

Focusing now on feedback from participants, we started by asking which of the 5 main sections of the application they considered most helpful in managing privacy (question B.21). As can be seen in graph 4.6, the 'Application Analysis' section was preferred by exactly half of the participants, followed by 'Grouped Analysis' with 31%, 'Device Settings' with 13% and 'Privacy Hints' with 6% (2 participants). It shows participants focused on a more granular analysis, but also considering important to have a more general analysis. We believe that the choices for the 'Device Settings' section were for its redirections to the Android settings and corresponding explanation, allowing users to easily change their privacy settings and have a better understanding of them.

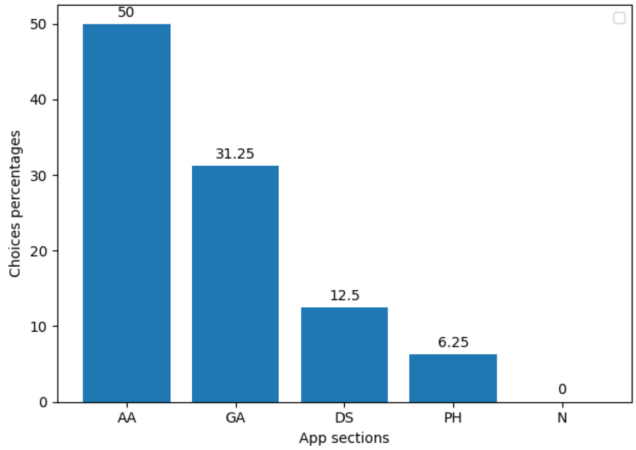



FIGURE 4.6: App section that helps the most to improve the device's privacy according to participants.

**AA** – Application Analysis

**GA** – Grouped Analysis

**DS** – Device Settings

**PH** – Privacy Hints

**N** – News

In the following question (B.22), all the participants were unanimous in agreeing that the available features were sufficient to help them improve their privacy.

The next two questions relate to hints and news. The first (question B.23) asks if the participant considers that they help to improve their privacy, to which 50% totally agreed and 34% agreed, with the rest of the participants neither agreeing nor disagreeing. This result demonstrates this to be an important component in the application. The second question (B.24) focuses on whether customizing device-based hints and news helps them know how to improve privacy. In here, the 'I fully agree' and 'Agree' options had respectively 41% and 34% of choices, with the remaining 19% neither agreeing nor disagreeing and 6% (2 participants) disagreeing. With 75% of the participants responding positively, this is also a component to pay attention to.

Participants were then asked to indicate what should be added in the application (question B.25). Five of the participants said they considered the application complete enough. The rest gave quite diverse answers, of which we present some, considered to be more important and viable of the suggestions: more detailed explanation of each permission, gamification, immediate analysis of when the application is installed and better organization in the way of showing permissions for each application.

We tried to analyse whether the application was able to meet the expectations of users with question B.26. The answers to the question A.13 of the pre-survey demonstrate how the participants were interested in gaining more knowledge about their privacy in various aspects. Despite the challenging initial expectations, when asking participants if they consider they have been achieved, all responses were positive. Several of the participants even mentioned that their expectations were exceeded and several justified the positive answer with various aspects that they learned anew. Most of the comments state to now have a better understanding of permissions and how to manage them to improve privacy, highlighting how the app was able to group permission information about the apps. Below are some participants comments:

- "Without doubt, the grouped analysis allowed me to easily understand which applications had more permissions, and the hints taught other small precautions I can take to improve the security of my smartphone."
- "Exceeded because it is an interface that tells us how many applications have too many permissions (grouped analysis) and aggregates everything in one place and with colour indication, without having to go to various places in the smartphone settings to review them."
- "Yes, it clearly presented my device's privacy points and how to improve."
- "It met my expectations, as I managed to gain greater knowledge of the applications I use on a daily basis and the level of security I have on my smartphone. I also got to know hints to improve this security."
- "It was much better than my expectations. Very appealing, user-friendly, easy to use, intuitive even for those with no knowledge of the subject. Very good! Congratulations!"

Except for one participant who did not consider it useful for him/her, all the other participants intended to keep the application installed (question B.27). The justifications focus on how the app helped them to improve their privacy and covered several aspects, mentioning: "great hints", "very informative news" and the ability to help maintaining privacy on devices, as it can be seen in the below comments:

- "Yes, it is a quick way to check permissions on my apps and a good place where I have compiled hints that I can review."
- "Yes, I think it might be quite useful and easier to use than device settings."
- "Yes, I think it is a good way to be aware of permissions, the hints are great and the news section is very informative and curious."
- "Yes, because I consider the app useful. It has shortcuts to get to specific parts of the settings and has information to help you understand more about the subject."

- "Probably, since there are not many applications that allow to view application permissions this way."

Users were then asked to rate the application on a scale of 1 to 10 in question B.30. In the graph 4.7 is the distribution of responses. The average of the answers is 8.56 which indicates a significantly positive evaluation.

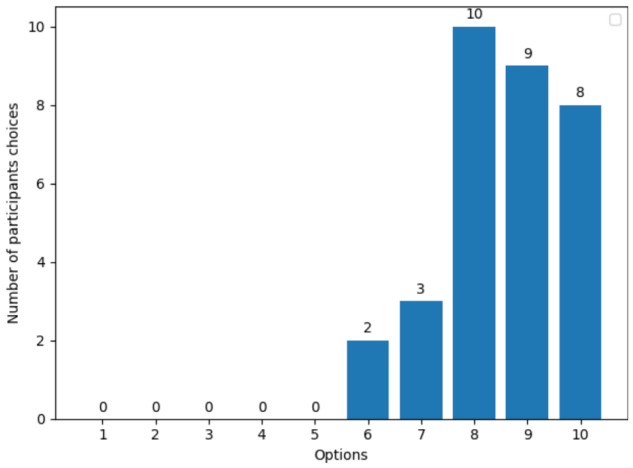



FIGURE 4.7: Evaluations given by participants to the application.

The justifications and opinions about the campaign and app asked in this next question (B.31) allowed us to understand that what most hindered the above evaluation was problems in notifications and wishes for improvements in the user interface. The responses are mainly very positive, with several participants highlighting the importance of this type of campaigns and stressing that they cannot find better alternatives to our application. Below are some responses received:

- "I think this campaign was very useful. I already have some experience in the world of technologies and even so I learned how to be more secure through this application, so I believe that people with less experience will learn even more."
- "I think it is the first application that can aggregate everything in one place and show the user its level of privacy, almost always having a shortcut to go to the settings to be changed."
- "The App achieved everything it promised and its simplicity helped to make everything less complicated. It is an app that anyone who wants to manage their privacy

can install and use with ease, without having to have prior knowledge of the subject. The news section makes it more interesting and interactive, creating a desire to visit the app instead of just having it for security reasons. Congratulations on the project!"

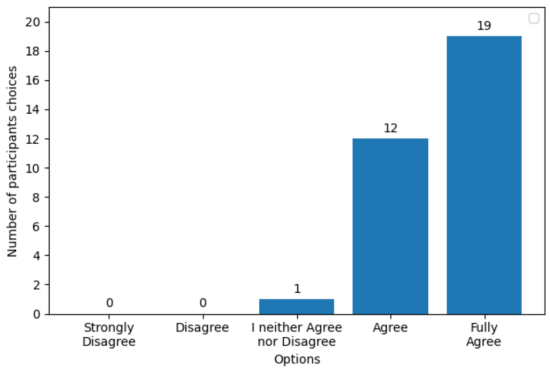
- "Excellent application, the fact to show all permissions by apps in a list helps a lot in the speed of making changes to permissions. Another positive point is the vulnerability rank that makes us solve problems from the most serious."
- "I liked the application, I will keep it installed and explore the rest of the features I have not tested yet."

### 4.5.4 Usability

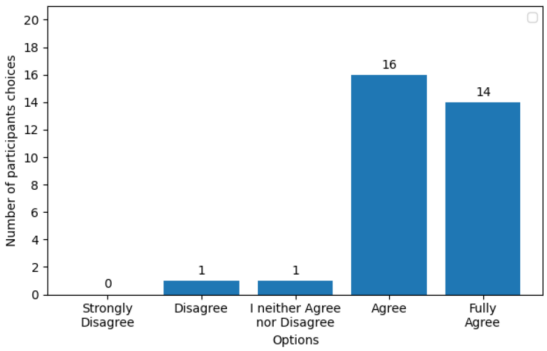
This subsection is the main core of the usability tests, as already mentioned in section 3.5. With them, we intend to understand what can be improved in the overall app appearance and interaction with the user.

Asking about errors that participants have noticed (question B.28), 53% say they have had none, while the remaining participants mention problems, mainly related to notifications. This is an issue that will clearly have to be revised. The following question (B.29) is related to nudges, asking whether participants received daily notifications, and if not then how often. Five participants said they did not receive notifications at all. Of the rest, 21 claimed to have received it daily, with the remaining six participants indicating some other frequency.

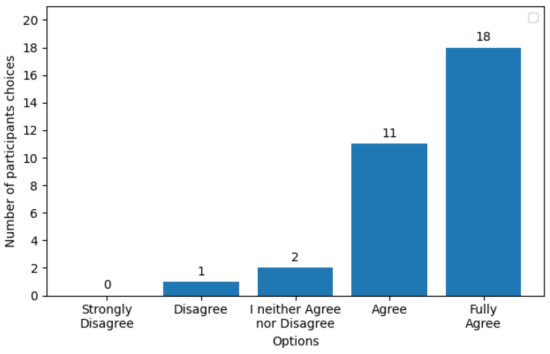
The last 5 questions of the post-survey are presented in figure 4.8. To these questions, the same five answers options were provided: 'I fully agree', 'Agree', 'I neither agree nor disagree', 'Disagree' and 'I strongly disagree', allowing the user to not having a clear opinion on the subject or express a higher or lower feeling of both agreement and disagreement with what is being stated.



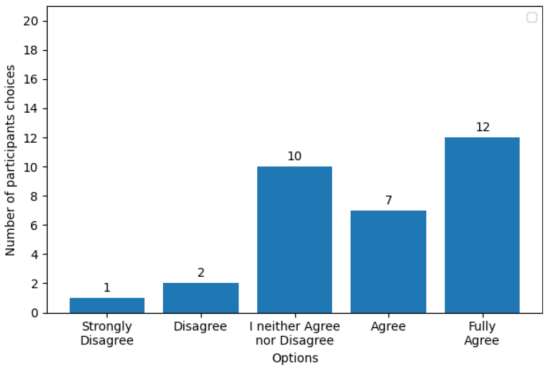

(A) Question: I find it easy to navigate between the different pages of the application.



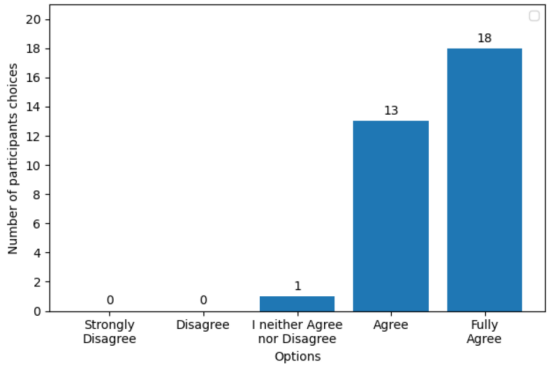

(B) Question: I consider that there was a correct visual distribution of the buttons and that they were easy to understand.




(C) Question: I consider the graphics of the application in the section 'Grouped Analysis' explanatory and easy to understand.




(D) Question: I consider the notifications I received simple and appealing, and with relevant content when clicked.




(E) Question: Overall, I consider the use of the application easy to understand.

FIGURE 4.8: Usability questions.

A general analysis of these 5 graphs allows us to understand that the visual presentation of the application is significantly well received. However, based on suggestions given to previous questions, we can make some improvements. Figures 4.8a, 4.8b and 4.8e show the application is easy to understand and navigate, with an appealing visual distribution of buttons. Figure 4.8c proves participants were pleased with the presented graphs in the app section 'Grouped Analysis'. At last, figure 4.8d demonstrates how notifications are the aspect that most needs improvement.

In figure 4.9 we obtain the ratings given to the application's design with question B.37, with an average of 7.34 on a scale of 1 to 10.

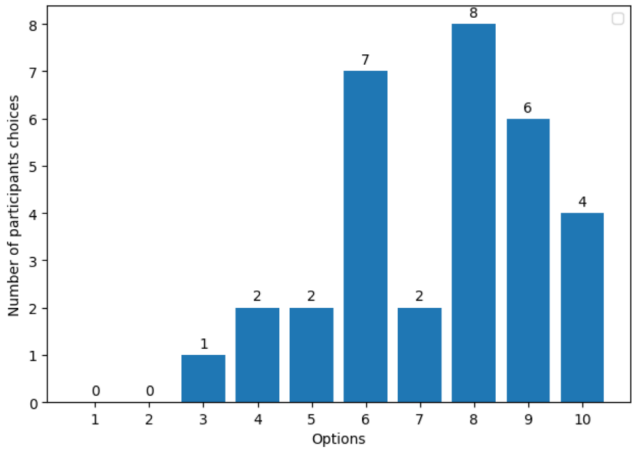



FIGURE 4.9: Evaluations given by participants to the application design.

The last question in the survey (B.38) is precisely intended to understand the answers given about usability, inviting any suggestions for improvement. Responses generally stated that the design is appealing but that it can be improved and modernized. Below are some of the comments that summarize most of the answers given:

- "The design is good, but there is always room for improvement, with a more modern interface."
- "I like the fact that it's simple and minimalist, which makes the experience easier and intuitive. I liked the fact that there was the option to change colours. However, I think that in the future it would be advantageous to invest in a more appealing design. The usability is very intuitive, it's easy to explore the various functions of the App!"

- "I think the design is simple and beautiful although it could be more modernized, but the button layout is very good!"
- "The application design is easy to understand and use. The only criticism would be the aesthetic part that could be improved."
- "The design is quite simple which does not immediately catch your eye, although the usability is well crafted."

### 4.5.5 Collected Data

In this subsection, we intend to draw some conclusions based on the collected data from the participants' devices during the field-study.

When analysing the sections that participants consulted the most, by counting the number of times they were opened from the application's main screen, it was observed what is represented in figure 4.10. In question B.21 participants answered that the most useful section was 'Application Analysis' and the same is verified when analysing the most used. We must also notice how section 'Grouped Analysis' also had a significant usage percentage, demonstrating that a clustered analysis with similar parameters is appealing and helpful to users. 'Privacy Hints' and 'Device Settings' have also captivated the participant's interest, with 'News' section in the last place.

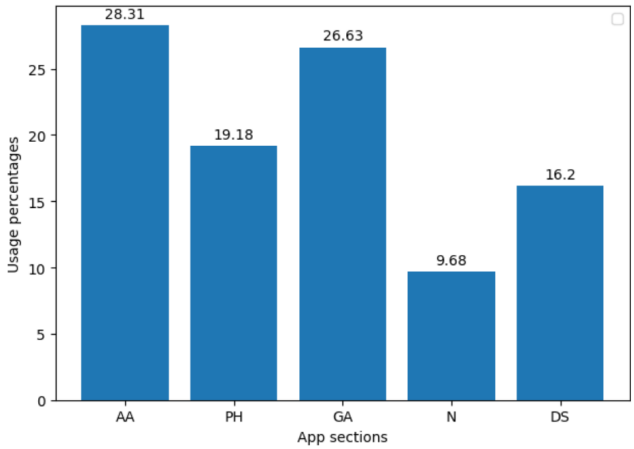



FIGURE 4.10: Percentages of app sections entries from the main screen.

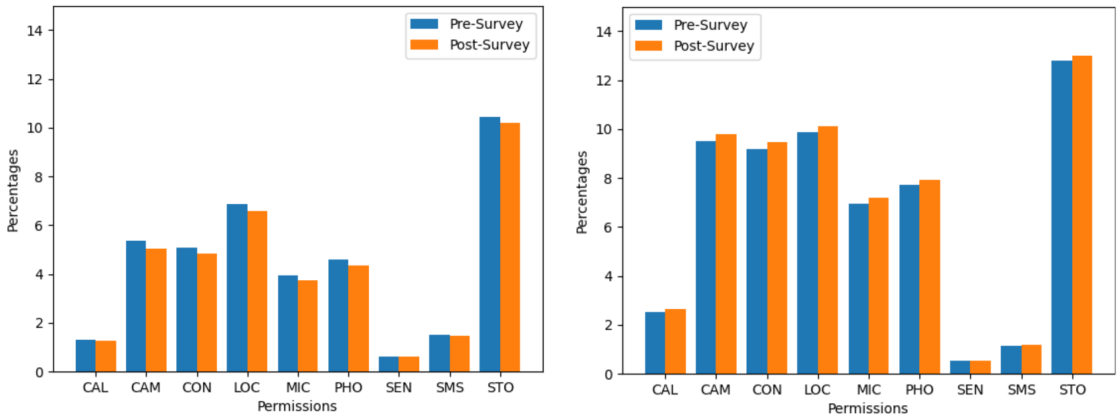
In an analysis of the evolution of the number of applications, analysing the launchable ones, by privacy level at the beginning and at the end of the field-study, it is visible a positive effect of the application. It is important to remember, as explained in the subsection

3.3.4.1, the privacy level of applications can be changed by users by granting or revoking permissions. At the *Dangerous* level were 7.34% of the participants' total applications at the beginning of the field-study, reducing to 6.75% at the end. Such change corresponds to 0.69 fewer apps (on average) at that level per participant. The *Medium* level suffered the main drop from 48.65% to 48.06%, corresponding to 0.97 less applications at this level per participant. Finally, the main change was in the Safe level which increased from 44.01% to 45.19%, corresponding to an increase of exactly 1 app at this level per participant. The mentioned values are contained in table 4.4. It is understandable that the reduction is not as significant in *Dangerous* as in *Medium* since *Dangerous* level apps are usually applications that require many permissions for their correct functioning, as in the case of Phone and SMS apps that deal with some of the most important functions of a mobile device.

TABLE 4.4: Changes in the number of apps by privacy level.

| **Privacy Level** | **Apps distribution at pre-survey submission** | **Apps distribution at post-survey submission** | **Average number of apps changes per participant** |
|---|---|---|---|
| Dangerous | 7.34% | 6.75% | -0.69 |
| Medium | 48.65% | 48.06% | -0.97 |
| Safe | 44.01% | 45.19% | +1 |

Analysing the evolution by permission group of launchable apps we can see there was a decrease, in all permission groups, in the percentage weight of granted permissions. The figure 4.11 shows us the distribution of granted and denied permissions by each of the permission groups, having in each of the graphs the percentages according to the total number of permissions and not only the granted or denied permissions. This distribution allows comparing the values when submitting the two surveys in each graph, as well as the distribution between granted and denied permissions for each permission group, being clear the higher percentage of denied permissions compared to the granted ones. They allow us to see a decrease in the granted permissions in all groups, verifying the opposite in the denied permissions, which saw their percentage weight increase (except for the *Sensors* permission group, in which the denied permissions' percentage weight did not change), as can be seen in table 4.5. These data demonstrate how the application and field-study were conducive to reducing permissions and increasing users' awareness of excessive permissions being granted.




(A) Granted permissions distribution.

(B) Denied permissions distribution.

FIGURE 4.11: Granted and denied permissions distribution by permission group.

(permissions' abbreviations explained in table 4.5)

TABLE 4.5: Average number of app changes by participant by permission group.

| | **Granted** | **Denied** |
|---|---|---|
| **Calendar** (CAL) | -0.28 | +0.47 |
| **Camera** (CAM) | -1.12 | +0.88 |
| **Contacts** (CON) | -1.03 | +0.84 |
| **Location** (LOC) | -1.12 | +0.84 |
| **Microphone** (MIC) | -0.81 | +0.81 |
| **Phone** (PHO) | -0.91 | +0.56 |
| **Sensors** (SEN) | -0.06 | +0 |
| **SMS** (SMS) | -0.25 | +0.19 |
| **Storage** (STO) | -1.12 | +0.62 |

The total number of launchable applications of all participants per Grade was also analysed and the results can be consulted in the table 4.6. For more information on the concept of Grades, consult subsection 3.3.4.3. These changes are due to application installs and uninstalls only, and despite a slight decrease in the number of apps in Grades A and B, there were also decreases in the last two grades, especially in Grade E, with a decrease of about 0.44 apps per participant. Grade D was the one with a higher increase with 0.34 apps per participant. It is not possible to draw many conclusions from this data, and it is understandable that, referring to a classification that users can only change by installing and uninstalling apps, it would have less variation than the analysis by privacy levels.

TABLE 4.6: Changes in the number of apps by participant by Grade.

| Grades | Apps distribution at pre-survey submission | Apps distribution at post-survey submission | Average number of apps changes per participant |
|---|---|---|---|
| A | 11.44% | 11.4% | -0.12 |
| B | 20.99% | 20.85% | -0.28 |
| C | 28.35% | 28.52% | +0 |
| D | 23.96% | 24.42% | +0.34 |
| E | 10.76% | 10.43% | -0.44 |
| F | 4.5% | 4.39% | -0.16 |

To try to understand whether the reduction of granted permissions in the launchable apps happened essentially at the beginning of our application's use or whether throughout the period, we have analysed, for each participant, the evolution of the number of granted permissions, for each app, whose values change in the considered period. We do not collect any information able to identify the participants' apps, just numeric values corresponding to the granted dangerous permissions of each app, focusing here on the launchable applications. These values were obtained once a day and we have noticed that, although the permissions changes are concentrated at the beginning, there are also changes in the rest of the period. Those changes can be seen in figure 4.12 where the total changes of granted permissions compared to the first measure are presented for all participants. Although the figure also contemplates changes caused by apps installations and uninstallations, by analysing the graphs of each participant individually, which we naturally cannot show them all in here, we see several users reducing apps' permissions throughout the field-study period and not only in the beginning. It was then concluded that the application was able to capture participants' attention and increase awareness that was not limited to initial interest and curiosity.

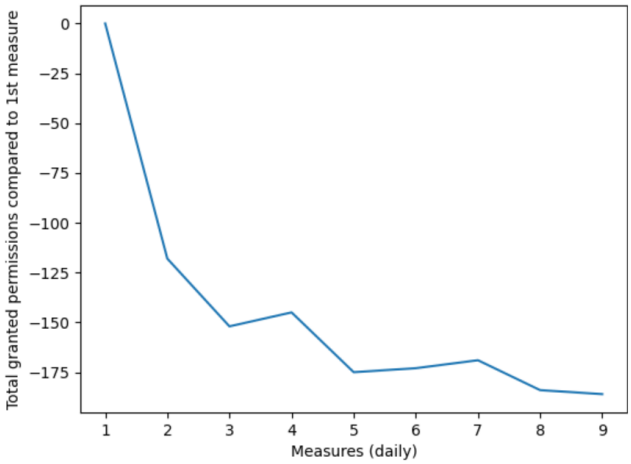



FIGURE 4.12: Changes in the number of total granted permissions compared to the 1st measure for all participants.

The conclusions retrieved from figure 4.12 can be complemented with two more studies visible in figures 4.13 and 4.14. The first one proved how the application usage was bigger in the first two days, although the application was able to maintain the users' interest throughout the field-study duration. Apart from these first two days, there seems to be no direct relationship between the application usage and the data obtained in figure 4.12 in the following days. A quick clarification can ease the comparison between figures 4.12 and 4.13, since in the first one, 4.12, each 'measure' in the x-axis shows the evolution compared to the previous day. For example, measure 2 in figure 4.12 presents the evolution from day 1 to day 2 in figure 4.13. The second figure, 4.14, presents the total number of entries per time of day in the application for each interval of 1 hour, and can be used for two types of conclusions. The first is to know in which period of the day users are more receptive to actively participate in field-studies, and from the results it is clear to be the period between 11am and 2pm. This information can be useful for future field-studies. The second conclusion is related to the effect of periodic nudges. By knowing that users will receive daily nudges at 1:30pm and 6:30pm, as demonstrated in table 4.1, a positive impact of them can be denoted in case it is observable these to be the periods in which the users have used the application the most. And in fact this can be observed since the application was most accessed from 1:00pm to 2:00pm, with an average of 1.22 entries per participant, and the second time in which was used the most, apart from the already mentioned interval of 11am to 2pm, was from 6:00pm to 7:00pm, demonstrating that the presented nudges made users interested to access the application.

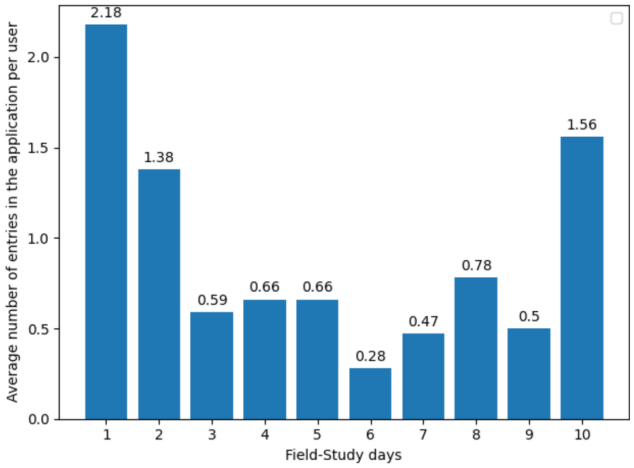



FIGURE 4.13: Average number of entries per participant and per day in the application during the field-study.

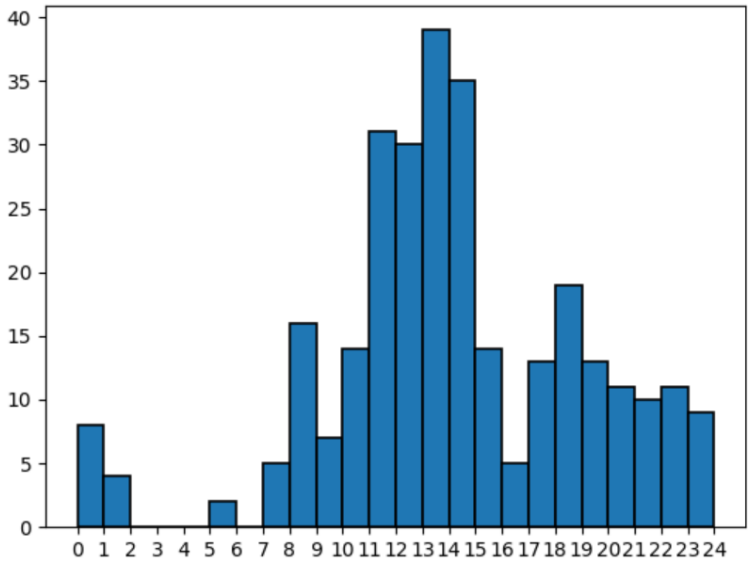



FIGURE 4.14: Total number of entries per time of day in the application during the field-study.

In the table 4.2 in the subsection 4.3.1 there are some hints that suggest alternative applications. To verify its effect, it was analysed if the participants installed the applications that were suggested and even if they uninstalled the original ones. However, the results showed that only 4 participants installed alternative applications, two installing the Silence [82] application as an alternative to the WhatsApp [83] application, one installing ProtonMail [85] as an alternative to Gmail [86] and the other one installing OsmAnd [87] alternatively to Google Maps [88], all keeping the original applications. These results take only into account the changes that were visible when submitting the post-survey, meaning, for example, the participant who answered for question B.18 a replacement of Google

Chrome by Firefox already had Firefox installed and is just in the process of changing the preferred browser, and that some participants may have tried alternative applications but uninstalled them before submitting the post-survey. From the data collected, we know that nudges numbers 2, 5, 7 and 9 from table 4.2, advising users about installing alternative applications, were read, respectively, by 14, 18, 16 and 16 participants. Thus, it appears that, despite the suggestion of alternative applications being praised and requested by some participants in the surveys, it had a very low impact. This is probably due to the difficulty in adapting to new applications, either due to a lack of features or because it is not common among people they know.

An analysis of the status of the locating and locking services in the participants' devices was carried out at the beginning and end of the field-study. All participants had an active locking method on their device both at the beginning and end of field-study. In the *Location* service, only three cases were registered in which participants changed their location status between the beginning and end of the field-study, with two of them deactivating it and another one activating. We then assume that users with *Location* service active in both cases, which was the case of 15 participants, had a strong reason for that, as for 'find my device' services or other security reasons.

Finally, we have also collected information about which of the hints from table 4.2 were read, by how many participants and whether they were consulted by clicking on the nudges or if it was the participant who manually consulted it in the app hints' section. The results show that 69 times the mentioned hints were consulted by clicking on the nudge, against 78 times they were read by manually entering the hints section. It is important to notice that the first value may not be higher since some participants might have had the curiosity to first consult manually the hint, which does not mean they did not click on those hints' nudges afterwards. Although more hints were consulted by participants manually clicking on them, these results demonstrate the important effect of using nudges on better engaging the user.

### 4.5.6 Impact of users' privacy concerns in results

We found it important to make a general comparison of answers from participants according to their answers to question A.10 from the pre-survey, related to the importance given to their information privacy, dividing in twelve participants that answered 5 and the twenty remaining participants that chose lower values. An overview comparison of

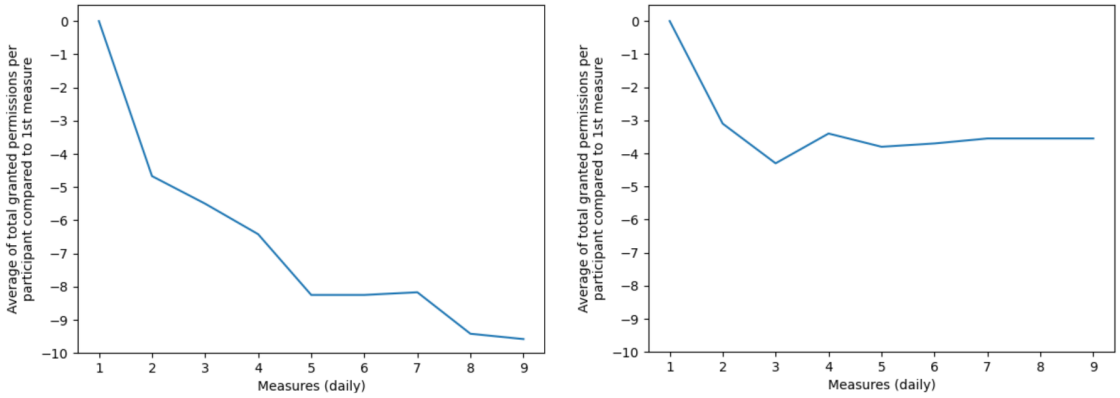
answers allowed us to understand that participants with higher concerns for their information privacy, comparing to the ones that did not value their information privacy so much, already had more precautions towards their data privacy and showed to be more sensible towards privacy related actions to perform in the future, also having a higher level of interest for the application during the field-study.

We have also analysed the evolution of the number of apps by privacy levels, the number of granted permissions by permission group and number of apps by grade, all studies already performed in subsection 4.4, but now performing them to the two already mentioned groups of participants. All the results contribute to obtain the same conclusions, however, we will focus only on the first mentioned study for a matter of simplicity and since its results have the biggest difference between the two participants groups. The results can be seen in table 4.7, where are noticeable the higher efforts of the participants with more privacy concerns to improve their privacy situation. This is visible on both the reduction of applications on *Dangerous* and *Medium* levels and the increase of applications in the *Safe* level.

TABLE 4.7: Average number of apps changes by privacy level between participants with higher and lower privacy concerns.

| **Privacy Level** | **Average number of apps changes per participant** (higher privacy concerns) | **Average number of apps changes per participant** (lower privacy concerns) |
|---|---|---|
| Dangerous | -1.17 | -0.4 |
| Medium | -1.42 | -0.7 |
| Safe | +1.08 | +0.95 |

Another study was performed to analyse the average number of changes of total granted permissions per participant compared to the first measure, which occurred when submitting the pre-survey and before using the application. This follows the same line of thinking as in figure 4.12, but now dividing between participants with higher (4.15a) and lower (4.15b) privacy concerns and focusing on average values per participant. It is clear how the first group of participants made greater efforts on reducing dangerous permissions, reaching a reduction of almost 10 dangerous permissions per participant on the ninth measure, while on the other group the same measure presented a value of less than 4 dangerous permissions reduced per participant compared to the first measure. Another aspect to be highlighted is how the reduction of permissions occurred not only on the beginning of the field-study, being this more visible on figure 4.15a.




(A) Average changes for participants with higher privacy concerns.

(B) Average changes for participants with lower privacy concerns.

FIGURE 4.15: Average changes in the number of total granted permissions per participant compared to the 1st measure.

### 4.5.7 Impact of app type of use in results

All 32 participants made proper use of the app, with this being a decision point on whether to consider a participant's contribution valid or not. However, we consider not only possible to divide participants in two groups according to their type of use of the application, but also important to analyse whether this would result in significantly different changes in the given answers and feedback. The decisions on the app type of usage were based on the usage metrics collected for each participant, which also allowed to understand participants are not honest when answering to the question B.10 about the type of use given to the application. To obtain a score for each participant, were considered the number of times they opened the application and the number of read hints and news. After this, a certain value was defined to obtain two groups with a similar amount of participants, according to if each participant score was higher or lower than the defined value. The analysis was then performed with two groups, the first with 17 participants considered to have paid a higher amount of attention to the app, and the second group with the remaining 15 participants.

An overview analysis of participants' answers from both groups allows to understand that users that used the application the most had more interaction with the privacy settings during the field-study, already had greater concerns with this subject and intend to take greater precautions regarding their actions in the future to improve their privacy. Another aspect analysed, is the comparison of answers of users to usability questions B.33 to B.36. The results are visible in table 4.8. Comparing the values in the left (answers from users with higher app usage) with the ones in the right (answers from users with lower

app usage) we observe how users with higher app usage have given better feedback to all questions, demonstrating that lower evaluations frequently are due to low app usage by participants. The fact that users with higher app usage gave more positive feedback means the given answers and evaluations could have been better if participants had used more the application and that, with the amount of provided features, is required that users spend some time with the app to better enjoy it.

TABLE 4.8: Comparison of answers to usability questions between users that paid a higher (left - green) and lower (right - red) amount of attention to the app.

| | Question **A** | Question **B** | Question **C** | Question **D** | Question **E** |
|---|---|---|---|---|---|
| **I fully agree** | 12 / 7 | 9 / 5 | 12 / 5 | 6 / 6 | 9 / 9 |
| **Agree** | 5 / 7 | 8 / 8 | 5 / 6 | 5 / 2 | 8 / 5 |
| **I neither agree nor disagree** | - / 1 | - / 1 | - / 2 | 6 / 4 | - / 1 |
| **Disagree** | - | - / 1 | - / 1 | - / 2 | - |
| **I strongly disagree** | - | - | - | - / 1 | - |

Question **A** (B.32) - I find it easy to navigate between the different pages of the application.

Question **B** (B.33) - I consider that there was a correct visual distribution of the buttons and that they were easy to understand.

Question **C** (B.34) - I consider the graphics of the application in the section 'Grouped Analysis' explanatory and easy to understand.

Question **D** (B.35) - I consider the notifications I received simple and appealing, and with relevant content when clicked.

Question **E** (B.36) - Overall, I consider the use of the application easy to understand.

## 4.6 Conclusions

After wrapping up the field-study, by analysing the answers to the surveys and the collected data from participants' devices, we can now draw some conclusions. For that, we opted to answer each of the questions listed in subsection 2.3.2 as presented below. It is, however, first important to remember that all the data collection happens only on the context of the field-study and not intended to be implemented when releasing the app

publicly.

**Is a permission manager, without any ads or trackers, that has total respect for the user's privacy and intended to raise privacy awareness, an appealing application for users to have installed on their devices to manage their privacy?**

From the obtained feedback, this type of application is very appealing to most users. Several times was praised the capability of aggregating so much information in one app since it helped participants improve their privacy, which is also supported by the collected data. Our effort in developing a user-friendly application with maximum respect for their privacy was very well-received, as can be seen in some citations in the results analysis, achieving our objective of raising privacy awareness and meeting the initial expectations of all participants, even surpassing them in several cases as stated in the answers. As mentioned in the results analysis, when participants were asked if they intended to keep the application installed, they all answered positively, except for one justifying it had no utility for him/her.

Finally, we would like to highlight that the application was also able to catch users' interest and curiosity, for what the hints and mainly the news sections played crucial roles. A citation of part of a participant's answer demonstrates what was said: "The news section makes it more interesting and interactive, creating a desire to visit the app instead of just having it for security reasons.".

**Which aspect of the application proved to be the most valuable to raise privacy awareness and then should be further improved?**

The application section chosen as the more capable of helping to improve privacy was 'Application Analysis', selected by 50% of participants, as seen in figure 4.6. Figure 4.10 demonstrates how section 'Grouped Analysis' was also able to captivate participants' attention and so, from this data and some other answers, we conclude that the two mentioned sections are the ones contributing the most to help manage users' privacy, but that in any way the three others should be neglected as they all had their positive impacts.

**Is there any advantage on regular nudges, essentially the ones related to privacy hints?**

During the field-study, some problems were reported related to nudges, which may have sightly prejudiced its effectiveness analysis. However, we have observed, as mentioned in subsection 4.5.5, that, for the hints present in table 4.2, the number of times participants consulted them through the nudges was very close to the number of times participants consulted them manually in the hints' section of the application. We then conclude that periodic nudges help users be reminded of their privacy, especially if those nudges consist of privacy hints or other alerts to remind and inform them to review their devices' privacy status, which will contribute to answer the next question.

**How is the application effective in improving user awareness as time evolves? Will users focus on the application only the first days, or their interest will remain throughout the field-study duration?**

As it was expected, the greatest attention paid to the application and the majority of changes to permissions occurred on the first days of using it. However, several users have performed some other changes during the period of the field-study and the reduction of granted permissions can be seen in figure 4.12 not just on the beginning. The same was observed when this analysis was performed for the participants with higher concerns for their information privacy, as seen in figure 4.15a. We then assume users tend to focus on these type of privacy applications more on the first days due to the novelty factor, but is possible to further catch their attention by using some techniques like periodic nudges, appealing design, informative hints and news, and others.

**What can be improved?**

There were two aspects that stand out from the feedback. The first is the nudges' system, which was not able to function correctly on some participants, with a few claiming they had never received any nudge. This is a technical aspect that needs to be reviewed. The second aspect is the graphical interface. When analysing the usability feedback, we have cited some participants' answers related to the user interface that, although praising its simplicity and ease to understand, said it could be improved and made more appealing.

From the users answers, we have also understood that users felt the need for a clear explanation on what each permission group gave applications access to. During the field-study, we have detailed two of the permission groups, but it is important for the future to

detail what it means to grant access to any permission group.

# Chapter 5

# Conclusions

Often, users do not have the minimum necessary precautions to better protect their privacy, both by lack of knowledge and motivation. The analysis of the state of the art shows how the market is not able to satisfy the users' needs. More effort must be put into raising users' privacy awareness to make them change their behaviour towards the never ending threats of the online environment.

To assess the gap between what users want and what is currently being offered, we have developed an Android application to raise privacy awareness. By presenting the user with several privacy related aspects of their devices, easing the task of improving their information privacy, also providing hints and news articles.

To evaluate the effectiveness of our application, we have performed a 10-day field-study with 32 participants. The results showed that the application is able to correspond to all the participants expectations, surpassing them in several cases. Except for one of the participants, all the remaining claimed interest in keeping the application installed. The collected data also presented some improvements, mainly in the reduction of permissions, in the device's privacy within the field-study period, which could probably be better if some errors in the nudging system had not occurred. We can then conclude that our application proved to be a strong alternative for the current state of the art and effective on raising privacy awareness. In any project there is always room for improvement, and based on aspects we were not able to implement due to time restrictions, together with the collected feedback from the field-study, we gathered in the next subsection some aspects that can be improved or added in future implementation.

## 5.1 Future Work

Several aspects possible to be included or improved were already mentioned throughout the document. Below we list and explain the main aspects we consider important to be considered in future work:

- Do not retrieve all the hints or news when opening the corresponding section on the application. There are several ways of obtaining this, but the simplest, which would avoid having the server as a middleware between database and application, is for each hint and news to have a *modification date* field. The only constraint is that developers must change manually this field every time they had to make any modification to a hint or news in the database. This approach allows the app to easily ask for newly updated or inserted hints/news on the database.
- Following the same idea from the project 'A Personalized Privacy Assistant for Mobile App Permissions', described in subsection 2.2.7, we believe that the creation of privacy profiles, assigning users to them through questions and other information like their device's apps, could bring a significant benefit on the personalization of our awareness techniques, improving our hints/news and our nudges content.
- From the feedback obtained with the field-study, we can point out some aspects to be improved/added:
  - improve the design;
  - improve the nudges system stability;
  - describe what each permission group give applications access to.

# Appendix A

# Pre-Survey

This survey is the first of two that will be conducted under the COP-MODE research project, which aims to develop a privacy manager for smartphones. If you want to know more about the project, you can see here: https://cop-mode.dei.uc.pt/

By answering this survey, the participant consents to the use of his/her answers for research purposes in the COP-MODE project. In the context of the campaign, the participant also consents to the automatic collection of some numerical data, not constituting sensitive information, which will be analysed to evaluate its progress in the period of the campaign and thus assess the effectiveness of the application to raise awareness about the topic of privacy. Some of the participant's interaction with this application will also be known.

The data that will be collected for the purposes of analysis in the context of these campaigns are:

• Number of applications assessed at the following privacy levels by our application: 'Dangerous', 'Medium', 'Safe'.
• Number of applications that grant and deny the following permission groups: 'Calendar', 'Camera', Contacts ',' Location ',' Microphone ',' Phone ',' Sensors ',' SMS ',' Memory '.
• Number of applications assigned to each grade by our application, from A to F.
• Numbers of permissions granted and denied, status of the location and locking service, and installation of suggested apps.
• Data related to the general use of the application.

☐ I declare to be 18 or older and accept the collection of the information mentioned above. *

We begin by thanking you for your participation in this 10 day campaign, which begins with the completion of this short survey.

We ask you to provide us in the following text field with the email address you used for this campaign as an identifier. It is not in any way in our interest to relate the answers with the participant, we just need to be able to make the relationship between the 1st and 2nd surveys conducted and ensure that all participants answer the surveys. *

Insert here the email used by you for the purpose of this campaign.

FIGURE A.1: Survey 1: Question 1

Age: *

◯ 18-24
◯ 25-39
◯ 40-60
◯ >60

FIGURE A.2: Survey 1: Question 2

**Education:** *

Highest level of education already completed

- ◯ Basic
- ◯ Secondary
- ◯ Degree
- ◯ Masters
- ◯ Doctorate

FIGURE A.3: Survey 1: Question 3

Gender: *

- ◯ Female
- ◯ Male
- ◯ Not Applicable

FIGURE A.4: Survey 1: Question 4

Occupation: *

- ◯ Administration
- ◯ Art/Writing/Journalism
- ◯ Entrepreneurship/Management/Finance
- ◯ Computer Science/Engineering
- ◯ Education
- ◯ Engineering (other than computers)
- ◯ Housemaker
- ◯ Law
- ◯ Health
- ◯ Services
- ◯ Technician
- ◯ Unemployed
- ◯ Retired
- ◯ Exact Sciences (other than engineering)
- ◯ Humanities
- ◯ Other

FIGURE A.5: Survey 1: Question 5

How long have you been using smartphones? *

- ◯ < 1 year
- ◯ 1 - 3 years
- ◯ 3 - 5 years
- ◯ > 5 years

FIGURE A.6: Survey 1: Question 6

**On average, how many hours do you spend per day on your smartphone?***

If you have more than one smartphone, consider the smartphone where you installed this app

- ◯ < 1 hour
- ◯ 1 - 3 hours
- ◯ 3 - 6 hours
- ◯ > 6 hours

FIGURE A.7: Survey 1: Question 7

**What is your knowledge in computer technology?***

1 - virtually none ; 5 - in-depth knowledge in the area

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|

FIGURE A.8: Survey 1: Question 8

**What is your knowledge in privacy/information security on smartphones?***

1 - virtually none ; 5 - in-depth knowledge in the area

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|

FIGURE A.9: Survey 1: Question 9

**How important do you consider to be your information privacy?***

1 - nothing important ; 5 - very important

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|

FIGURE A.10: Survey 1: Question 10

**How do you think your smartphone manages your privacy?***

1 - very badly, I feel that my privacy is in no way assured ; 5 - very satisfied with the management of the privacy of smartphones, I feel perfectly safe

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|

FIGURE A.11: Survey 1: Question 11

Based on your experience in smartphones, what do you think could be done/improved for better management of your privacy?*

FIGURE A.12: Survey 1: Question 12

Tell us what is/are your expectation(s) when you signed up for this campaign and what do you expect to learn?*

FIGURE A.13: Survey 1: Question 13




FIGURE A.14: Survey 1: Question 14

If selected **Yes** on question A.14:

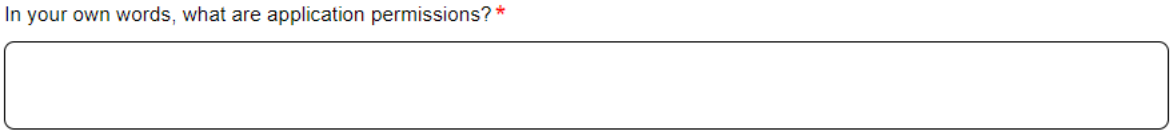



FIGURE A.15: Survey 1: Question 15

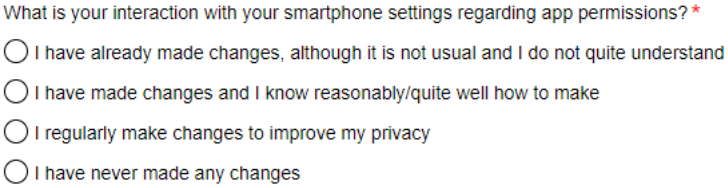



FIGURE A.16: Survey 1: Question 16

If selected **No** on question A.14:

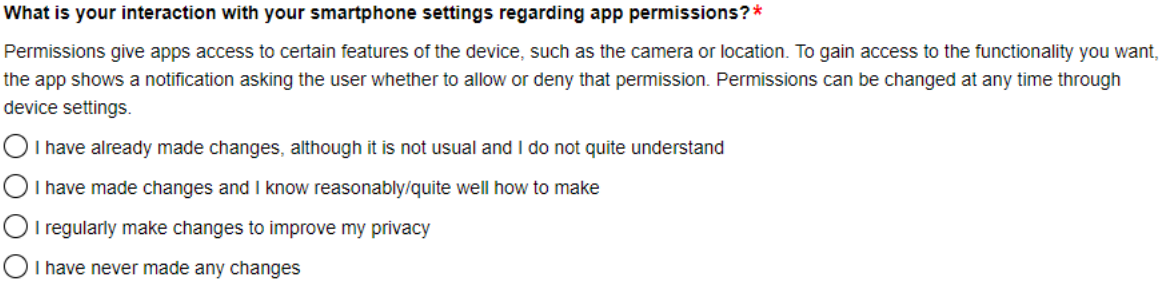



FIGURE A.17: Survey 1: Question 17

—End of conditional questions—

An application asking for the "SMS" permission will ask "Allow X to send and view SMS messages?". If this permission is allowed, what do you think this permission will allow the application to do? *

- [ ] View the contact list
- [ ] Read MMS messages
- [ ] Read incoming messages
- [ ] View your contact's email
- [ ] Read incoming emails
- [ ] Read sent messages
- [ ] Send messages
- [ ] None of the previous answers

FIGURE A.18: Survey 1: Question 18

An application asking for the "Phone" permission will ask "Allow X to make and manage phone calls?". If this permission is allowed, what do you think this permission will allow the application to do? *

- [ ] View the contact list
- [ ] View and change call history
- [ ] Send and read received messages
- [ ] Know your mobile number
- [ ] Record calls
- [ ] Make calls
- [ ] Identify the user only through obtained identifiers
- [ ] Hang up calls and redirect them to other numbers
- [ ] None of the previous answers

FIGURE A.19: Survey 1: Question 19

An application asking for the "Contacts" permission will ask "Allow X to access your contacts?". If this permission is allowed, what do you think this permission will allow the application to do? *

- [ ] See your contact list
- [ ] See your call log
- [ ] Delete contacts
- [ ] Make calls
- [ ] See contacts email addresses
- [ ] None of the previous answers

FIGURE A.20: Survey 1: Question 20

Are you concerned about granting only the necessary permissions to your applications? *

- ◯ Yes, I usually only grant the necessary permissions for the type of use I have of the application
- ◯ It depends on the application. For some I have this concern, for others I do not and I grant all permissions
- ◯ No, I always grant all the permissions that the application asks for because I consider that if they are requested it is because they are important
- ◯ No, I usually always grant all the permissions that the application asks for because I do not want to waste time analyzing whether they are important

FIGURE A.21: Survey 1: Question 21

Have you ever used apps to manage and improve your privacy? If so, tell us which by the app name or link in the Google Play Store. *

FIGURE A.22: Survey 1: Question 22

Do you use antivirus, firewall or privacy managers on your smartphone? *

- ◯ No, I do not think these tools will help me protect and maintain the privacy of my data
- ◯ No, I do not think I have anything to protect on my device
- ◯ No, although I think I should use
- ◯ Yes, but as I do not give much importance I use any
- ◯ Yes, I think it is very important so I use one that I consider good

FIGURE A.23: Survey 1: Question 23

Below are some actions aimed at improving privacy and security in the use of your smartphone. Select the ones you remember you have already done:

- ☐ Change privacy permissions in your own app settings
- ☐ Always keep your smartphone version up to date
- ☐ Update your apps regularly
- ☐ Check whether the applications used by default are reliable or should be changed
- ☐ Avoid having the location service active except when strictly necessary
- ☐ Turn off ads personalization
- ☐ Check Google service settings on your device by changing how your Google account(s) controls your data
- ☐ Use incognito mode for privacy reasons (e.g. in browsers, Youtube, Google Maps, etc.)
- ☐ Uninstall some application to install another similar one with fewer permissions
- ☐ Uninstall an application because of permissions

FIGURE A.24: Survey 1: Question 24

In addition to the privacy/security actions mentioned, are there any more you have ever done? If so, please indicate which one(s): *

FIGURE A.25: Survey 1: Question 25

# Appendix B

# Post-Survey

We thank you for your participation in this campaign that ends with the realization of this survey.

We ask for special attention in completing this survey, which, although brief and simple, is extremely important to be able to compare with the first one and analyze the effectiveness of the application.

How do you think this experience has contributed to improving your knowledge in this area? *

- ◯ I feel that now I am much more knowledgeable in the area and that in the future I will know better how to ensure my privacy
- ◯ It was good, I gained knowledge about this area, though I feel it could have instructed me more
- ◯ It was good, I gained knowledge about this area, but I believe that I was not able to enjoy the app enough
- ◯ Little or almost nothing

FIGURE B.1: Survey 2: Question 1

Can you justify/clarify your choice in the last question? If you think you have learned something new, give us an example. *

FIGURE B.2: Survey 2: Question 2

**How do you now assess your knowledge in privacy/information security on smartphones?** *

1 - virtually none ; 5 - in-depth knowledge in the area

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|

FIGURE B.3: Survey 2: Question 3

**How important do you consider to be your information privacy?** *

1 - nothing important ; 5 - very important

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|

FIGURE B.4: Survey 2: Question 4

**How do you now think that your smartphone manages your privacy?** *

1 - very badly, I feel that my privacy is in no way assured ; 5 - very satisfied with the management of privacy on smartphones, I feel perfectly safe

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|

FIGURE B.5: Survey 2: Question 5

Still on how your smartphone manages your privacy: *

- ◯ Better than I expected, I think it is enough
- ◯ It could manage better, however, good privacy can be achieved if the user manages his/her settings correctly, as well as the applications he/she uses and their privacy settings
- ◯ I think it shows little regard for the privacy of its users

FIGURE B.6: Survey 2: Question 6

An application asking for the "SMS" permission will ask "Allow X to send and view SMS messages?". If this permission is allowed, what do you think this permission will allow the application to do? *

- ☐ View the contact list
- ☐ Read MMS messages
- ☐ Read incoming messages
- ☐ View your contact's email
- ☐ Read incoming emails
- ☐ Read sent messages
- ☐ Send messages
- ☐ None of the previous answers

FIGURE B.7: Survey 2: Question 7

An application asking for the "Phone" permission will ask "Allow X to make and manage phone calls?". If this permission is allowed, what do you think this permission will allow the application to do? *

- ☐ View the contact list
- ☐ View and change call history
- ☐ Send and read received messages
- ☐ Know your mobile number
- ☐ Record calls
- ☐ Make calls
- ☐ Identify the user only through obtained identifiers
- ☐ Hang up calls and redirect them to other numbers
- ☐ None of the previous answers

FIGURE B.8: Survey 2: Question 8

An application asking for the "Contacts" permission will ask "Allow X to access your contacts?". If this permission is allowed, what do you think this permission will allow the application to do? *

- [ ] See your contact list
- [ ] See your call log
- [ ] Delete contacts
- [ ] Make calls
- [ ] See contacts email addresses
- [ ] None of the previous answers

FIGURE B.9: Survey 2: Question 9

Which of the options is closest, on average, to the type of use you gave the application? *

- ◯ Once a day
- ◯ Every three days
- ◯ Every five days
- ◯ Once a week

FIGURE B.10: Survey 2: Question 10

From what you learned, how would you describe your interaction with your smartphone settings regarding app permissions? *

- ◯ I did not interact with these settings during the time I used the app so I did not learn anything else
- ◯ I did not interact with these settings but it was made clear what kind of changes I can make to application permissions
- ◯ I have come to visit these settings but I still feel a little confused about how they work
- ◯ I have visited these settings and feel now confident to make changes in the future when necessary
- ◯ I visited these settings and made changes to better protect my privacy

FIGURE B.11: Survey 2: Question 11

Do you think you will acquire the custom of making changes to the settings to increase your privacy/security on your smartphone? *

- ◯ I did not have the habit, and I still think there is no need to do it
- ◯ I did not have the habit but I was sensitized to the need to make changes to these settings and so I will change my behavior
- ◯ I already had this habit and nothing will change
- ◯ I already had this habit but I will intensify my attention to these settings

FIGURE B.12: Survey 2: Question 12

Regarding the granting of necessary permissions to your applications: *

- ◯ I did not have the habit, and I still do not think there is any need to do it
- ◯ I did not used to worry about it, however I am going to change the way I give applications permissions so they only access the features they need
- ◯ I have already made some changes, but now I am going to be even more attentive
- ◯ I already had this habit and nothing will change

FIGURE B.13: Survey 2: Question 13

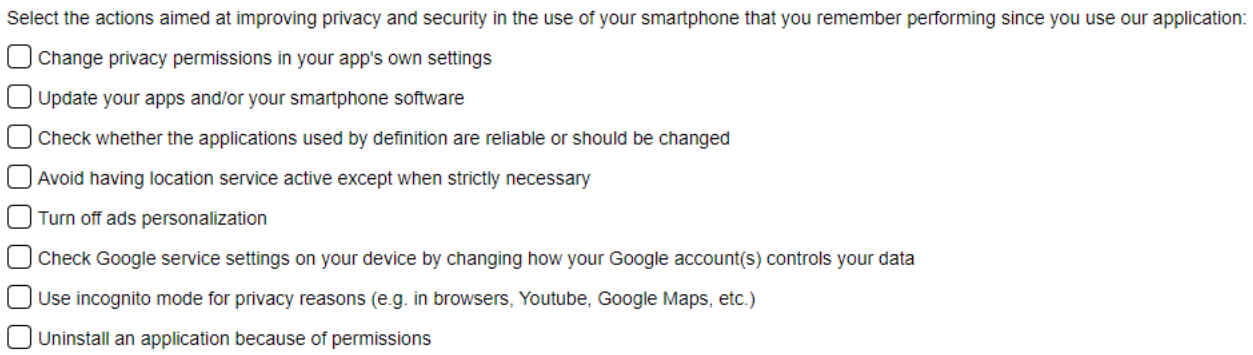



FIGURE B.14: Survey 2: Question 14

If selected option '**Change privacy permissions in your app's own settings**' on question B.14:

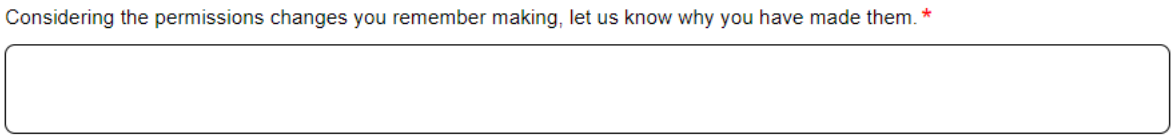



FIGURE B.15: Survey 2: Question 15

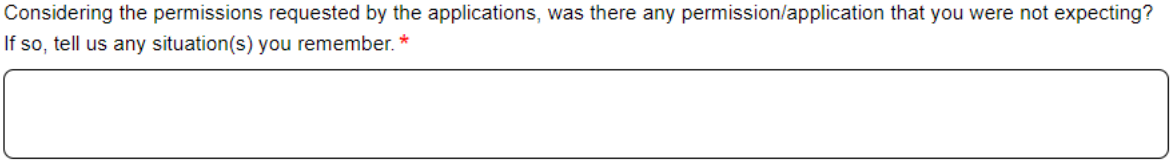



FIGURE B.16: Survey 2: Question 16

—End of conditional questions—

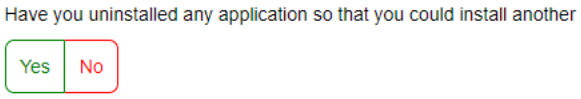



FIGURE B.17: Survey 2: Question 17

If selected **Yes** on question B.17:

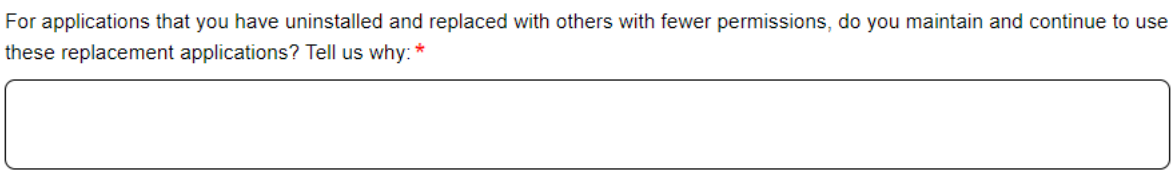



FIGURE B.18: Survey 2: Question 18

—End of conditional questions—

In addition to the privacy/security actions mentioned, is there any more you have taken due to the use of the application (e.g. something learned through the privacy hints)? If so, please indicate which: *

FIGURE B.19: Survey 2: Question 19

Below are some actions aimed at improving privacy and security in the use of your smartphone. Select the ones you think you will be worried about in the future:

- [ ] Change privacy permissions in your app's own settings
- [ ] Always have the version of my smartphone up to date
- [ ] Update your apps regularly
- [ ] Check whether the applications used by definition are reliable or should be changed
- [ ] Avoid having location service active except when strictly necessary
- [ ] Turn off ads personalization
- [ ] Check Google service settings on your device by changing how your Google account(s) controls your data
- [ ] Use incognito mode for privacy reasons (e.g. in browsers, Youtube, Google Maps, etc.)
- [ ] Uninstall some application to install another similar one with fewer permissions
- [ ] Uninstall an application because of permissions
- [ ] Use an antivirus, firewall or privacy manager

FIGURE B.20: Survey 2: Question 20

Of the top 5 sections of the app, which one do you think is the one that most helps you manage your device's privacy? *

- ◯ Application Analysis
- ◯ Grouped Analysis
- ◯ Device Settings
- ◯ Privacy Hints
- ◯ News

FIGURE B.21: Survey 2: Question 21

Do you think the available features and presented information were sufficient to help you improve your privacy, or at least learn how to do so? *

Yes | No

FIGURE B.22: Survey 2: Question 22

I consider the hints and news helpful in helping to improve my privacy. *

- ◯ I fully agree
- ◯ Agree
- ◯ I neither agree nor disagree
- ◯ Disagree
- ◯ I strongly disagree

FIGURE B.23: Survey 2: Question 23

I consider the customization of hints and news based on my device and applications helps me to know how to improve my privacy. *

- ◯ I fully agree
- ◯ Agree
- ◯ I neither agree nor disagree
- ◯ Disagree
- ◯ I strongly disagree

FIGURE B.24: Survey 2: Question 24

Tell us if you consider any important functionality that you think should be added to the app. *

FIGURE B.25: Survey 2: Question 25

Tell us now if we were able to meet your initial expectations for the application: *

FIGURE B.26: Survey 2: Question 26

Do you consider keeping the app you tested installed on your device? Tell us why: *

FIGURE B.27: Survey 2: Question 27

Is there any application error you remember occuring during its use? If so, tell us which one(s). *

FIGURE B.28: Survey 2: Question 28

Have you received daily notifications from our application? If not, tell us more or less how many times a week you have received them or if they have just stopped appearing at a certain point in time. *

FIGURE B.29: Survey 2: Question 29

Tell us how you evaluate the overall application? *



FIGURE B.30: Survey 2: Question 30

Finally, please give us your opinion on the application and campaign you have participated in and why you gave the above evaluation. Any improvement suggestions you want to provide will be welcome! *

FIGURE B.31: Survey 2: Question 31

I find it easy to navigate between the different pages of the application. *

- ◯ I fully agree
- ◯ Agree
- ◯ I neither agree nor disagree
- ◯ Disagree
- ◯ I strongly disagree

FIGURE B.32: Survey 2: Question 32

I consider that there was a correct visual distribution of the buttons and that they were easy to understand. *

- ◯ I fully agree
- ◯ Agree
- ◯ I neither agree nor disagree
- ◯ Disagree
- ◯ I strongly disagree

FIGURE B.33: Survey 2: Question 33

I consider the graphics of the application in the section 'Grouped Analysis' explanatory and easy to understand. *

- ◯ I fully agree
- ◯ Agree
- ◯ I neither agree nor disagree
- ◯ Disagree
- ◯ I strongly disagree

FIGURE B.34: Survey 2: Question 34

I consider the notifications I received simple and appealing, and with relevant content when clicked. *

- ◯ I fully agree
- ◯ Agree
- ◯ I neither agree nor disagree
- ◯ Disagree
- ◯ I strongly disagree

FIGURE B.35: Survey 2: Question 35

Overall, I consider the use of the application easy to understand. *

- ◯ I fully agree
- ◯ Agree
- ◯ I neither agree nor disagree
- ◯ Disagree
- ◯ I strongly disagree

FIGURE B.36: Survey 2: Question 36

How do you evaluate the design of the application? *



FIGURE B.37: Survey 2: Question 37

Please justify the less positive answers given above. Feel free to provide improvements on the aspects mentioned or any other related to the usability, design and ease of understanding of the application: *

FIGURE B.38: Survey 2: Question 38

# References


[1] Perficient, "Mobile vs. desktop usage in 2020," accessed on: May 2021. [Online]. Available: https://www.perficient.com/insights/research-hub/mobile-vs-desktop-usage [Cited on page 1.]

[2] statCounter, "Privacygrade: Grading the privacy of smartphone apps," accessed on: May 2021. [Online]. Available: https://gs.statcounter.com/platform-market-share/desktop-mobile-tablet [Cited on page 1.]

[3] statsCounter, "Mobile operating system market share worldwide," accessed on: May 2021. [Online]. Available: https://gs.statcounter.com/os-market-share/mobile/worldwide/#monthly-202004-202104 [Cited on page 1.]

[4] IDC, "Smartphone market share," accessed on: May 2021. [Online]. Available: https://www.idc.com/promo/smartphone-market-share [Cited on page 1.]

[5] Net MarketShare, "Operating system market share," accessed on: May 2021. [Online]. Available: https://netmarketshare.com/operating-system-market-share.aspx?options={"filter":{"%24and":[{"deviceType":{"%24in":["Mobile"]}}]},"dateLabel":"Trend","attributes":"share","group":"platform","sort":{"share":-1},"id":"platformsDesktop","dateInterval":"Monthly","dateStart":"2019-11","dateEnd":"2020-10","segments":"-1000"} [Cited on page 1.]

[6] Liam Frost, "Apple and google's coronavirus app is a 'global mass surveillance tool'," accessed on: May 2021. [Online]. Available: https://decrypt.co/25338/apple-and-googles-coronavirus-app-is-a-global-mass-surveillance-tool [Cited on page 1.]

[7] Carole Cadwalladr and Emma Graham-Harrison, "Facebook accused of conducting mass surveillance through its apps," accessed on: May 2021. [Online].

Available: https://www.theguardian.com/technology/2018/may/24/facebook-accused-of-conducting-mass-surveillance-through-its-apps [Cited on page 1.]

[8] BABU MOHAN, "Whatsapp sues the indian government to stop 'mass surveillance'," accessed on: May 2021. [Online]. Available: https://www.androidcentral.com/whatsapp-sues-indian-government-stop-mass-surveillance [Cited on page 1.]

[9] J. D. Biersdorfer, "How your phone knows where you have been," accessed on: June 2021. [Online]. Available: https://www.androidcentral.com/whatsapp-sues-indian-government-stop-mass-surveillance [Cited on page 2.]

[10] Alfred Ng, "These cheap phones come at a price – your privacy," accessed on: June 2021. [Online]. Available: https://www.cnet.com/news/these-cheap-phones-are-costing-you-your-privacy/ [Cited on page 2.]

[11] Stuart A. Thompson and Charlie Warzel, "Smartphones are spies. here's whom they report to." accessed on: June 2021. [Online]. Available: https://www.nytimes.com/interactive/2019/12/20/opinion/location-tracking-smartphone-marketing.html [Cited on page 2.]

[12] Stefan Achleitner and Chengcheng Xu, "Android apps leaking sensitive data found on google play with 6 million u.s. downloads," accessed on: June 2021. [Online]. Available: https://unit42.paloaltonetworks.com/android-apps-data-leakage/ [Cited on page 2.]

[13] Brian Reed, "Test of 250 popular android mobile apps reveals that 70% leak sensitive personal data," accessed on: June 2021. [Online]. Available: https://www.nowsecure.com/blog/2019/06/06/test-of-250-popular-android-mobile-apps-reveal-that-70-leak-sensitive-personal-data/ [Cited on page 2.]

[14] Thomas Claburn, "New lawsuit: Why do android phones mysteriously exchange 260mb a month with google via cellular data when they're not even in use?" accessed on: June 2021. [Online]. Available: https://www.theregister.com/2020/11/14/google_android_data_allowance/ [Cited on page 2.]

[15] Dan Goodin, "Beware of ads that use inaudible sound to link your phone, tv, tablet, and pc," accessed on: June 2021. [Online].

Available: https://arstechnica.com/tech-policy/2015/11/beware-of-ads-that-use-inaudible-sound-to-link-your-phone-tv-tablet-and-pc/ [Cited on page 2.]

[16] Joseph Cox, "I gave a bounty hunter $300. then he located our phone," accessed on: June 2021. [Online]. Available: https://www.vice.com/en/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile [Cited on page 2.]

[17] Stuart A. Thompson and Charlie Warzel, "How to track president trump," accessed on: June 2021. [Online]. Available: https://www.nytimes.com/interactive/2019/12/20/opinion/location-data-national-security.html [Cited on page 2.]

[18] ——, "Twelve million phones, one dataset, zero privacy," accessed on: June 2021. [Online]. Available: https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html [Cited on page 2.]

[19] Andy Greenberg, "It takes just $1,000 to track someone's location with mobile ads," accessed on: June 2021. [Online]. Available: https://www.wired.com/story/track-location-with-mobile-ads-1000-dollars-study/ [Cited on page 2.]

[20] Martina Frascona 'Sochurkova, "New study reveals users' lack of knowledge on personal data collection," accessed on: June 2021. [Online]. Available: https://newsfeed.org/new-study-reveals-users-lack-of-knowledge-on-personal-data-collection/ [Cited on page 2.]

[21] S. Pötzsch, "Privacy awareness: A means to solve the privacy paradox?" in *IFIP Summer School on the Future of Identity in the Information Society*. Springer, 2008, pp. 226–236, accessed on: June 2021. [Cited on page 2.]

[22] COP-MODE, "The project cop-mode," accessed on: March 2021. [Online]. Available: https://cop-mode.dei.uc.pt/ [Cited on page 3.]

[23] Trident Inc., "Google play store - app permissions," accessed on: March 2021. [Online]. Available: https://play.google.com/store/apps/details?id=com.mykapp.permissionviewer [Cited on page 6.]

[24] Vnova Mobile, "Google play store - permission manager," accessed on: March 2021. [Online]. Available: https://play.google.com/store/apps/details?id=com.agooday.permission [Cited on page 6.]

[25] Morsol Technology, "Google play store - permission manager for android," accessed on: March 2021. [Online]. Available: https://play.google.com/store/apps/details?id=com.permission.manager.android [Cited on page 6.]

[26] Shexa Technolabs, "Google play store - app permission manager," accessed on: March 2021. [Online]. Available: https://play.google.com/store/apps/details?id=com.shexa.permissionmanager [Cited on page 6.]

[27] NeonApps Studio, "Google play store - app permission manager (no root)," accessed on: March 2021. [Online]. Available: https://play.google.com/store/apps/details?id=com.permissionmanager.neonapps [Cited on page 6.]

[28] PrivacyGrade, "Privacygrade: Grading the privacy of smartphone apps," accessed on: March 2021. [Online]. Available: http://privacygrade.org/ [Cited on page 7.]

[29] J. Lin, S. Amini, J. I. Hong, N. Sadeh, J. Lindqvist, and J. Zhang, "Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing," in *Proceedings of the 2012 ACM conference on ubiquitous computing*, 2012, pp. 501–510. [Cited on page 7.]

[30] Amazon, "Amazon mechanical turk," accessed on: March 2021. [Online]. Available: https://www.mturk.com/ [Cited on page 8.]

[31] P. Hornyack, S. Han, J. Jung, S. Schechter, and D. Wetherall, "These aren't the droids you're looking for: retrofitting android to protect data from imperious applications," in *Proceedings of the 18th ACM conference on Computer and communications security*, 2011, pp. 639–652, accessed on: March 2021. [Cited on page 8.]

[32] J. Lin, B. Liu, N. Sadeh, and J. I. Hong, "Modeling users' mobile app privacy preferences: Restoring usability in a sea of permission settings," in *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, 2014, pp. 199–212, accessed on: March 2021. [Cited on pages xiii, 8, and 9.]

[33] AndroGuard, "Reverse engineering, malware analysis of android applications ... and more (ninja) !" accessed on: March 2021. [Online]. Available: https://github.com/androguard [Cited on page 8.]

[34] Android Developers, "App manifest overview," accessed on: June 2021. [Online]. Available: https://developer.android.com/guide/topics/manifest/manifest-intro [Cited on page 9.]

[35] N. Gerber, P. Gerber, H. Drews, E. Kirchner, N. Schlegel, T. Schmidt, and L. Scholz, "Foxit: enhancing mobile users' privacy behavior by increasing knowledge and awareness," in *Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust*, 2018, pp. 53–63, accessed on: March 2021. [Cited on page 10.]

[36] W. Enck, P. Gilbert, S. Han, V. Tendulkar, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth, "Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones," *ACM Transactions on Computer Systems (TOCS)*, vol. 32, no. 2, pp. 1–29, 2014, accessed on: March 2021. [Cited on page 11.]

[37] TaintDroid, "Realtime privacy monitoring on smartphones," accessed on: March 2021. [Online]. Available: http://www.appanalysis.org/index.html [Cited on page 11.]

[38] K. Olejnik, I. Dacosta, J. S. Machado, K. Huguenin, M. E. Khan, and J.-P. Hubaux, "Smarper: Context-aware and automatic runtime-permissions for mobile devices," in *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2017, pp. 1058–1076, accessed on: March 2021. [Cited on page 12.]

[39] SmarPer, "Smarper project: Context-aware and automatic runtime-permissions for mobile devices," accessed on: March 2021. [Online]. Available: https://spism.epfl.ch/smarper/ [Cited on page 12.]

[40] M66B, "Xprivacy," accessed on: March 2021. [Online]. Available: https://github.com/M66B/XPrivacy [Cited on page 12.]

[41] XDA-Developers, "Xposed framework hub," accessed on: March 2021. [Online]. Available: https://www.xda-developers.com/xposed-framework-hub/ [Cited on page 13.]

[42] Y. Agarwal and M. Hall, "Protectmyprivacy: detecting and mitigating privacy leaks on ios devices using crowdsourcing," in *Proceeding of the 11th annual international conference on Mobile systems, applications, and services*, 2013, pp. 97–110, accessed on: March 2021. [Cited on page 13.]

[43] S. Chitkara, N. Gothoskar, S. Harish, J. I. Hong, and Y. Agarwal, "Does this app really need my location? context-aware privacy management for smartphones," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 1, no. 3, pp. 1–22, 2017, accessed on: March 2021. [Cited on page 13.]

[44] synergylabscmu, "Xposed module repository - protect my privacy (pmp)," accessed on: March 2021. [Online]. Available: https://repo.xposed.info/module/org.synergylabs.pmpandroid [Cited on page 13.]

[45] H. Almuhimedi, F. Schaub, N. Sadeh, I. Adjerid, A. Acquisti, J. Gluck, L. F. Cranor, and Y. Agarwal, "Your location has been shared 5,398 times! a field study on mobile app privacy nudging," in *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, 2015, pp. 787–796, accessed on: March 2021. [Cited on page 15.]

[46] B. Liu, M. S. Andersen, F. Schaub, H. Almuhimedi, S. A. Zhang, N. Sadeh, Y. Agarwal, and A. Acquisti, "Follow my recommendations: A personalized privacy assistant for mobile app permissions," in *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, 2016, pp. 27–41, accessed on: March 2021. [Cited on page 16.]

[47] A. Boutet and S. Gambs, "Inspect what your location history reveals about you: Raising user awareness on privacy threats associated with disclosing his location data," in *Proceedings of the 28th ACM International Conference on Information and Knowledge Management*, 2019, pp. 2861–2864, accessed on: March 2021. [Cited on page 23.]

[48] Electronic Frontier Foundation, "Surveillance self-defense," accessed on: May 2021. [Online]. Available: https://ssd.eff.org/ [Cited on page 23.]

[49] S. Schöbel, T. Barev, A. Janson, F. Hupfeld, and J. M. Leimeister, "Understanding user preferences of digital privacy nudges–a best-worst scaling approach," in *Proceedings of the 53rd Hawaii International Conference on System Sciences*, 2020, accessed on: April 2021. [Cited on page 24.]

[50] E. K. Choe, J. Jung, B. Lee, and K. Fisher, "Nudging people away from privacy-invasive mobile apps through visual framing," in *IFIP Conference on Human-Computer Interaction*. Springer, 2013, pp. 74–91, accessed on: April 2021. [Cited on page 24.]

[51] A. Acquisti, I. Adjerid, R. Balebako, L. Brandimarte, L. F. Cranor, S. Komanduri, P. G. Leon, N. Sadeh, F. Schaub, M. Sleeper *et al.*, "Nudges for privacy and security: Understanding and assisting users' choices online," *ACM Computing Surveys (CSUR)*, vol. 50, no. 3, pp. 1–41, 2017, accessed on: April 2021. [Cited on page 24.]

[52] Exodus Privacy, "Exodus privacy - trackers," accessed on: March 2021. [Online]. Available: https://reports.exodus-privacy.eu.org/en/info/trackers/ [Cited on page 25.]

[53] Rahul Patel, "Warden : App management utility," accessed on: March 2021. [Online]. Available: https://gitlab.com/AuroraOSS/AppWarden [Cited on page 25.]

[54] Exodus Privacy, "Exodus privacy - analyzes privacy concerns in android applications." accessed on: March 2021. [Online]. Available: https://exodus-privacy.eu.org/en/ [Cited on page 25.]

[55] FileInfo.com, "Dalvik executable file," accessed on: June 2021. [Online]. Available: https://fileinfo.com/extension/dex [Cited on page 25.]

[56] Yale Privacy Lab, "Yale privacy lab - tracker profiles," accessed on: March 2021. [Online]. Available: https://github.com/YalePrivacyLab/tracker-profiles [Cited on page 25.]

[57] FacettsOpen, "Exodify," accessed on: March 2021. [Online]. Available: https://github.com/FacettsOpen/exodify [Cited on page 25.]

[58] Konrad Kollnig, "About trackercontrol," accessed on: March 2021. [Online]. Available: https://github.com/OxfordHCC/tracker-control-android [Cited on page 25.]

[59] Mozilla-Services, "shavar-prod-lists," accessed on: March 2021. [Online]. Available: https://github.com/mozilla-services/shavar-prod-lists [Cited on page 25.]

[60] CAP-A Project, "Innovation project on digital privacy in mobile apps," accessed on: March 2021. [Online]. Available: https://cap-a.eu/ [Cited on page 26.]

[61] IN2 Digital Innovations GmbH, "Google play store - cap-a," accessed on: March 2021. [Online]. Available: https://play.google.com/store/apps/details?id=com.in2.cap_a [Cited on page 26.]

[62] A. Stan, K. Geramani, G. Ioannidis, I. Chrysakis, G. Flouris, M. Makridaki, T. Patkos, Y. Roussakis, G. Samaritakis, N. Tsampanaki, E. Tzortzakakis, and E. Ymeralli, "Capa: A community-driven approach to privacy awareness," accessed on: April 2021. [Cited on page 26.]

[63] CAPrice Project, "Caprice," accessed on: April 2021. [Online]. Available: https://www.caprice-community.net/ [Cited on page 26.]

[64] F. Breitinger, R. Tully-Doyle, and C. Hassenfeldt, "A survey on smartphone user's security choices, awareness and education," *Computers & Security*, vol. 88, p. 101647, 2020, accessed on: April 2021. [Cited on page 27.]

[65] A. Ferrari and S. Giordano, "A study on users' privacy perception with smart devices," *arXiv preprint arXiv:1809.00392*, 2018, accessed on: April 2021. [Cited on page 27.]

[66] altexsoft, "The good and the bad of java programming," accessed on: May 2021. [Online]. Available: https://www.altexsoft.com/blog/engineering/pros-and-cons-of-java-programming/ [Cited on page 38.]

[67] Michael, "Android 101: Java or python. what's best for android apps?" accessed on: May 2021. [Online]. Available: https://www.appinessworld.com/blogs/172/android-101-java-or-python-whats-best-for-android-apps [Cited on page 38.]

[68] Meghavi Vyas, "Benefits of using java for mobile app development," accessed on: May 2021. [Online]. Available: https://www.openxcell.com/blog/benefits-of-java-for-app-development/ [Cited on page 38.]

[69] Shibaji Debnath, "Shibaji debnath," accessed on: May 2021. [Online]. Available: https://www.shibajidebnath.com/java-android-development/ [Cited on page 38.]

[70] Marcos Placona, "Storing your secure information in the ndk," accessed on: June 2021. [Online]. Available: https://androidsecurity.info/storing-your-secure-information-in-the-ndk/ [Cited on page 40.]

[71] SHISHIR, "Securing api keys in android app using ndk (native development kit)," accessed on: June 2021. [Online]. Available: https://medium.com/programming-lite/securing-api-keys-in-android-app-using-ndk-native-development-kit-7aaa6c0176be [Cited on page 40.]

[72] A. K. Purohit and A. Holzer, "Functional digital nudges: Identifying optimal timing for effective behavior change," in *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019, pp. 1–6. [Cited on page 61.]

[73] MongoDB, "The database for modern applications," accessed on: May 2021. [Online]. Available: https://www.mongodb.com/ [Cited on page 64.]

[74] studytonight.com, "Advantages of mongodb," accessed on: May 2021. [Online]. Available: https://www.studytonight.com/mongodb/advantages-of-mongodb [Cited on page 64.]

[75] Javatpoint, "Mongodb advantages over rdbms," accessed on: May 2021. [Online]. Available: https://www.javatpoint.com/mongodb-advantages-over-rdbms [Cited on page 64.]

[76] TutorialsPoint, "Mongodb - advantages," accessed on: May 2021. [Online]. Available: https://www.tutorialspoint.com/mongodb/mongodb_advantages.htm [Cited on page 64.]

[77] MongoDB, "Mongodb compass," accessed on: May 2021. [Online]. Available: https://www.mongodb.com/products/compass [Cited on page 64.]

[78] Kiran Malvi, "The positive and negative aspects of node.js web app development," accessed on: May 2021. [Online]. Available: https://www.mindinventory.com/blog/pros-and-cons-of-node-js-web-app-development/ [Cited on page 65.]

[79] altexsoft.com, "The good and the bad of node.js web app development," accessed on: May 2021. [Online]. Available: https://www.altexsoft.com/blog/engineering/the-good-and-the-bad-of-node-js-web-app-development/ [Cited on page 65.]

[80] The Tor Project, "Google play store - tor browser: Official, private, & secure," accessed on: june 2021. [Online]. Available: https://play.google.com/store/apps/details?id=org.torproject.torbrowser [Cited on page 84.]

[81] Google LLC, "Google play store - google chrome," accessed on: june 2021. [Online]. Available: https://play.google.com/store/apps/details?id=com.android.chrome [Cited on page 84.]

[82] Silence, "Google play store - silence," accessed on: june 2021. [Online]. Available: https://play.google.com/store/apps/details?id=org.smssecure.smssecure [Cited on pages 84 and 97.]

[83] WhatsApp LLC, "Google play store - whatsapp messenger," accessed on: june 2021. [Online]. Available: https://play.google.com/store/apps/details?id=com.whatsapp [Cited on pages 84 and 97.]

[84] Mozilla, "Google play store - firefox browser," accessed on: june 2021. [Online]. Available: https://play.google.com/store/apps/details?id=org.mozilla.firefox [Cited on page 84.]

[85] Proton Technologies AG, "Google play store - protonmail encrypted email," accessed on: june 2021. [Online]. Available: https://play.google.com/store/apps/details?id=ch.protonmail.android [Cited on page 97.]

[86] Google LLC, "Google play store - gmail," accessed on: june 2021. [Online]. Available: https://play.google.com/store/apps/details?id=com.google.android.gm [Cited on page 97.]

[87] OsmAnd, "Google play store - osmand — offline maps, travel & navigation," accessed on: july 2021. [Online]. Available: https://play.google.com/store/apps/details?id=net.osmand [Cited on page 97.]

[88] Google LLC, "Google play store - google maps," accessed on: july 2021. [Online]. Available: https://play.google.com/store/apps/details?id=com.google.android.apps.maps [Cited on page 97.]