

# Unraveling the Complexity of Mobile Application Permissions: Strategies to Enhance Users' Privacy Education

Rena Lavranou<sup>1,\*</sup>, Stylianos Karagiannis<sup>2</sup>, Aggeliki Tsohou<sup>1</sup>, and Emmanouil Magkos<sup>1</sup>


## ABSTRACT

Smartphones and other mobile devices have seamlessly integrated into our daily lives offering a multitude of possibilities through various applications. However, this convenience comes at a cost, due to the excessive usage of device permissions claimed by the applications. The management of information privacy in mobile applications presents a formidable challenge for users. For instance, users are confronted with intricate privacy decisions, including the configuration of application permission settings. Unfortunately, many users lack adequate knowledge about how applications utilize their personal data. This research investigates the permissions of seven most popular mobile applications and provides a program to enable the extraction and categorization of permissions. The extracted information, datasets, and insights enrich the foundation of privacy education. The results can be used by educators who can develop workshops that immerse participants in this challenging topic. Therefore, this research paper contributes to the topics of privacy education and privacy awareness.

**Keywords:** Android Permissions, Android Security, Privacy Awareness, Privacy Education.

Submitted: December 04, 2023

Published: December 29, 2023

 10.24018/ejeng.2023.1.CIE.3141

<sup>1</sup> Ionian University (IURC), Greece.

<sup>2</sup> a) Ionian University (IURC), Greece, b) PDM, Portugal.

\* Corresponding Author:  
e-mail: lavranou@ionio.gr

## 1. INTRODUCTION

In the modern era of the internet, the rapid advancement of technology has improved many aspects of human life [1]. Today, people are using more and more smartphones and tablets, and thus their sales are growing every year [2]. The rapid adoption of mobile devices and applications offers significant opportunities for users to access e-services in many areas, such as communication, commerce, education, and health, but also raises important privacy issues [3].

Nowadays, people disclose a lot of personal information online, but they tend to ignore the fact that in most cases companies share this information with third parties or use it for other purposes, such as advertising [4]. Mobile applications (usually named also as apps) usually are granted access to the users' personal and sensitive data. This is important both for the functionality of the applications, but also for marketing and advertising [5]. In most cases, the access rights regard personal data, including among others phone contacts, location, camera, photos, or microphone, and are granted by the device, through the application permission requests by the users [6].

Regulations regarding privacy rights include the General Data Protection Regulation (GDPR) and require for users to have control over the collection and use of their personal data, such as ensuring informed consent [7]. Users of mobile devices are faced with a multitude of complex privacy decisions on a daily basis, the number of which can be overwhelming, such as configuring the permission settings for the applications they install [8].

Further, users are often unaware of the permission settings or the context of the permissions they have granted to previously installed applications [9], [10]. Only a few people actually read the permission requests of applications, and even fewer understand them correctly [11] or change their settings [10]. Furthermore, as Scoccia *et al.* [12] point out in their work, users do not understand why they are being asked to grant certain permissions. Wijesekera *et al.* [13] conducted an empirical study in which they developed an experimental application and showed that at least 80% of participants in their study would prefer to deny at least one permission requested by this application if they knew the purpose of the request in advance.

In addition, users of mobile devices are often surprised by the ability of various applications to collect and share personal data with third parties [2]. It is surprising and also concerning that, for example, if an application is able to access personal data, such as the list of incoming or outgoing Short Message Service (SMS) messages on the device, it is even possible to obtain information about the emotional state of the entities exchanging these messages as reported in [14].

It is also questionable if users are actually informed by developers about everything an application will do after they agree to install it from the Google Play Store [15]. Solanki *et al.* highlight that some of the most popular applications on the Play Store do not make clear all the permissions they declare [15]. There are cases where application users are misinformed about terms of use and privacy policies, and other cases in which applications share data in violation of their stated terms of service [3]. Feichtner and Gruber [16] talk about the arbitrariness of actual application descriptions and the lack of imposed quality standards.

Users are also faced with overprivileged applications, i.e., applications that ask for more permissions than necessary [12]. Overprivileged applications pose privacy threats to mobile device ecosystems and pose various reputational risks to online markets, such as the Android Marketplace, often arising from the use of ad libraries [2].

As a result, researchers have pointed to a lack of awareness among users of the security risks associated with mobile applications [17], as well as a lack of knowledge about how applications use their personal data [18]. It is therefore clear that many users are vulnerable [18]. Even if some users are concerned about their privacy and are aware of the privacy risks, studies show that they continue to disclose their personal data. This phenomenon is widely known in the literature as the "Privacy Paradox" [19], [20] and according to Barnes [20], the solution lies in user's awareness about how to protect their privacy on the internet.

In light of the above, this work aims to increase user privacy awareness in application permission decisions. To this end, we followed one research question: *What should the user know when making informed privacy decisions about application permissions?* So, we extracted and studied the permissions of seven of today's most popular applications. By analysing these permissions, we aim to highlight the points that a user should be more aware of.

The findings of this research, combined with the proposed strategies, offer a foundational resource for designing training and educational programs tailored to equip students and internet users with a comprehensive familiarity with Android permissions. The heightened privacy awareness of using this analysis fosters a propensity for privacy-conserving online conduct, underscored by more judicious and well-informed privacy decisions in the context of permissions allocation.

The approach can help educators initiate workshops by showcasing the applications, and exercise the classification into their functional categories. Leveraging the outcomes and insights from this research paper, they can facilitate

interactive sessions wherein participants engage in permission categorization exercises. This not only bolsters engagement but also facilitates an enhanced understanding of permission dynamics. Through immersive case studies and hands-on tasks, participants can then be empowered to scrutinize application permissions, conjecturing their usage scenarios. This cultivates the requisite acumen to navigate application permissions with prudence, fortifying a proactive approach to privacy preservation.

The remainder of this paper is structured as follows: Section 2 provides an overview of the Android Permissions and the types of them, as well as the related work to the permissions requests. Section 3 describes our research methodology, and Section 4 presents our results. We discuss our findings in Sections 5 and 6 concludes the paper.

## 2. LITERATURE REVIEW

### 2.1. Android Permissions

Recent research has shown that Android is the fastest growing mobile operating system with the highest number of users worldwide. Android's popularity is driven by factors such as ease of use, open source, low cost compared to mobile operating systems such as iOS, and the launch of new models due to 5G inventions [21].

Permissions are a key part of the Android security mechanism to protect privacy-sensitive device functionality. If an application requires dangerous permission, i.e., access to the user's calendar, camera, contacts, location, etc. that could potentially affect the user's privacy or the normal operation of the device, the permission must be explicitly granted by the user. The permissions required by an application must be listed in the application's manifest file [6].

Until 2015, Android users had no control over what resources were made available to applications during runtime [2]. Users could either accept all the requested permissions to be able to install the application or deny them and not install it. A major change to the permissions system came in 2015 with the 6th version of Android. From Android 6 onwards, as with iOS, the first time an application tries to use a sensitive resource, the system will display a dialogue message asking the user to grant or deny access. This is the ask-on-first-use (AOFU) permission model.

The user's response to this request for permission will be carried over to all future requests for this permission from that application. Modern versions of the most popular operating systems (Android and iOS) now come with permission management systems. This allows users to revoke access to resources at any time via the phone's settings [2]. On newer versions of Android (since Android version 11), the permissions automatically revert to the denied state after a few months of non-use of the application [22].

The AOFU model can theoretically lead to increased privacy awareness among users [2]. However, the effectiveness of Android's permission system depends primarily on the end user, who is responsible for granting permissions to applications, which is probably the weakest link in Android's security mechanism [23]. Sometimes the user cannot distinguish between the set of permissions

requested by an application and the risk it poses, putting their privacy and security at risk.

## 2.2. Types of Permissions

Android categorizes permissions into different types including install-time, runtime permissions, and special permissions. Each type indicates the scope of restricted data that an application can access, and the scope of restricted actions that an application can perform when the system grants an application that permission [22].

Some permissions, known as install-time permissions, are automatically granted when an application is installed and can be viewed on the details page of an application in the app store. Install-time permissions include normal permissions and signature permissions. Normal permissions allow access to data and actions outside of an application's sandbox and pose very little risk to the user's privacy [22].

Signature permissions are granted by the system and can be accessed by applications that have the same certificate as the applications that define the permission. Most often, signature permissions are used by applications installed by the mobile operator [23]. Other permissions, known as runtime permissions, require an application to go one step further and request permission at runtime [22].

Runtime permissions, also known as dangerous permissions, pose a higher risk to the user's privacy and must be explicitly granted by the user [23]. Many of these access the user's private data, a special type of restricted data that includes potentially sensitive information, such as microphone, camera, location, and contact information. The system therefore helps the user to understand why an application is accessing this information [22].

On newer versions of Android (since Android 11), there are also one-time permissions. Whenever the permission request is related to location, microphone or camera, the user has three options—deny access, accept only this time, or accept while using the application. If the user selects the option “Only this time” in the dialogue, the application is granted a temporary one-time permission [22].

Special permissions correspond to specific application operations and are related to resources that are particularly sensitive or not directly related to user privacy. Special permissions differ from install-time and runtime permissions. Some examples of special permissions include scheduling exact alarms, displaying and drawing over other applications, and accessing all storage data. Unlike runtime permissions, the user must grant special permissions from the Special App Access page in system settings [22].

## 2.3. Permissions Requests and Related Work

There have been several types of research dealing with permission requests. Gruschka *et al.* [24] dealt with the evaluation of application permissions. They used machine learning to cluster permissions to determine whether they were appropriate for a particular category of app, and how they varied between similar applications.

On the other hand, Solanki *et al.* [15] proposed a technique called MAPPER to mark overprivileged permissions declared in the Play Store. Application permissions can be extracted from the textual description. They also present a prototype that establishes the correspondence between

information from the application description and information from the application manifest file. Feichtner and Gruber present a machine learning-based approach to identify critical differences between developer-described application behavior and permission usage. They develop a system that can infer permission usage from the functionality described in text segments [16].

Many works in the literature use permission requests to detect Android malware. In [23], the researchers focus on the use of permissions declared in the Android manifest file. They extracted all Android permissions to investigate their use as a means to quickly and effectively distinguish between benign and malicious applications. Drebin gathers many features of an application from the manifest file and disassembled code, including requested and used permissions, to identify malicious applications directly on the smartphone [25].

Ashawa and Morris proposed the Android Permission Classifier, a framework for classifying Android malware permission requests based on their protection and threat levels using deep learning. Their work focused on normal and dangerous permissions [21]. Li *et al.* [26] also extracted significant permissions from Android applications and used them to detect malicious applications using machine learning algorithms, developing a malware detection system called Significant Permission Identification (SigPID). Wang *et al.* [27] studied permission-induced risks in Android applications, identifying subsets of risky permissions and detecting malicious applications.

APK Auditor [28] is also a permission-based Android malware detection system that extracts an application's permissions from a manifest file and classifies suspicious applications as benign or malicious, by calculating a Permission Malware Score (PMS) for each permission. McLaughlin *et al.* proposed an Android malware detection model based on a machine learning algorithm using permission request information and various features of Android Package Kit (APK) files [29]. Similarly, the research by Saxe and Berlin [30] and David and Netanyahu [31] obtains the permissions requested by malicious applications on Android-based platforms.

Furthermore, the literature suggests several ways to support users in their privacy decisions. In [17], better visualization of permissions and their associated privacy risks is suggested, allowing the user to decide on each permission. Biswas *et al.* highlight the need to reduce the user burden of complex permission decisions [32]. There have been many approaches to overcome this user burden by automating the configuration of privacy settings [17].

Many researchers propose different mechanisms for predicting users' privacy decisions, using machine learning techniques, based on a relatively small number of factors, such as previous privacy decisions or answers to privacy-related questions [33], [34]. Software agents can then use these machine learning models to provide personalized privacy recommendations to users, helping them to better control their privacy [35], while reducing the number of decisions that users have to make themselves.

In this work, we do not intend to approach permissions from a malware detection perspective, nor to predict the users' application permission settings. Our goal is to guide

TABLE I: BRIEF DESCRIPTION OF THE STUDIED APPS

Applications	Brief description
Facebook	Social networking, sharing news and photos, marketplace, etc.
Messenger	Communication with text, voice, and video calls.
WhatsApp messenger	Communication with private (fully encrypted) messages and calls.
Instagram	Social networking, based on photo and video sharing, messaging and video chat.
TikTok	Short-form video streaming service with user-submitted videos.
Spotify	Audio streaming with music and podcasts.
YouTube	Video streaming platform with various themes such as music, games, fashion, beauty, news, learning, and more.

users through an analysis of the permission requests of seven of today's most popular applications, so they can address the privacy challenges of modern technology in their daily lives.

### 3. METHODOLOGY

#### 3.1. Selection of Mobile Apps

We selected seven of today's most popular applications, which are in the top 15 of the globally most downloaded applications of all time [36]. We tried to include applications from different categories, and then, we extracted and studied the permissions they require from users, both for functionality and for other, mainly advertising purposes (targeted advertising).

The seven applications that we selected are Facebook [37], Messenger [38], WhatsApp Messenger [39], Instagram [40], TikTok [41], Spotify [42] and YouTube [43]. Facebook, Instagram, and TikTok are social media applications, Messenger and WhatsApp are communication and messaging applications, whereas Spotify and YouTube are media streaming applications. We also included Facebook Lite [44], which is a version of the Facebook application that works on slower networks, uses less data, and comes in a smaller package. Table I provides a brief description of the applications we studied in this work. The information presented in Table I is based on the websites of the applications in the Google Play App Store.

#### 3.2. Method for Retrieval and Categorization of Permissions

The methodology for the retrieval and categorization of the permissions from the selected Android applications is described as follows

1. *Android Package Kit (APK) Decompilation*: APK is the file format used for distributing and installing applications on Android devices. It contains all the necessary components of an Android application, including code, resources, manifest, and permissions. APK files are decompiled to gain access to manifest.xml, the application source code, and relevant resources.
2. *App Manifest and Permissions Overview*: The file manifest.xml contains important information about the application, including requested permissions.
3. *Permission Validation Process*: The actual permissions that are handled by the device can vary based on several factors, including the Android version

of the operating system and the hardware capabilities of the device. To validate the accuracy the extracted permissions were cross verified directly from the user's device. This involved accessing the application's permission settings on the device and comparing them with the extracted permissions from *manifest.xml*. This process also contributed to the categorization logic described in the following step.

4. *Android Permission Categorization Logic*: The categories of permissions in the official documentation do not include a standardized and universal taxonomy. Instead, this responsibility typically falls to individual device manufacturers, who aim to organize permissions into user-friendly categories. Nevertheless, the categorization scheme for Android applications primarily revolves around three categories: a) install-time permissions, b) runtime permissions, and c) special permissions. One plausible approach to proceed with the classification involves the implementation of an automated algorithmic process, wherein permission categorization hinges upon the detection of specific keywords embedded within the permission names. This heuristic process maps permissions to the corresponding thematic groups based on the identified keywords (e.g., LOCATION, WIFI, PHONE, etc.). Below is an explanation of the categorization logic:

- *Location*: Grant access to the geographic positioning data of the device, enabling applications to determine the location.
- *Calendar*: Ability to access and manipulate calendar events and schedules.
- *Contact*: Access and manage the address book of the device.
- *Music and Audio Permissions*: Enable and control audio resources and relevant applications including playback and audio recording.
- *Microphone*: Access to the microphone of the device and permit audio recording.
- *Nearby Devices*: Enable interactions with other devices including Bluetooth connectivity.
- *Photos and Videos*: Access and manage media files such as photos and videos.
- *Notifications*: Enable the ability for the application to display notifications to the user.
- *Camera*: Enable the application to access the camera.
- *Call Logs*: Access and manage the call history of the device and give access to the call logs.

- *SMS*: Allow access to text messages and give the ability to retrieve information or send SMS messages.
- *Media and Storage*: Access and manage media files including photos and videos.
- *Security and Authentication*: Permissions related to biometric sensors, fingerprint authentication, and other security-related functionalities.
- *Internet and Connectivity*: Permit the application to connect to the internet, retrieve data, and interact with various network services.
- *Networking*: Network-specific operations, including network management, access to the network connections and network protocols.
- *Audio and Camera Recording*: Allow the application to capture audio and video and interact with audio-related functionalities.
- *Account Management*: Access and manage user accounts and related operations.
- *Other Permissions*: In case the permission does not match any of the above it is classified on this category. This category includes permissions that may be less common or do not fit within the predefined groups.

The proposed categorization is a simplified approach, however, customization is possible to expand or enable additional keywords or criteria in order to create more refined permission groups. Once the permissions are extracted, they are compiled into JavaScript Object Notation (JSON) files in a structured format. This allows the integration with other systems and applications allowing the data to be suitable for further analysis and processing.

There are specific benefits deriving from the permission categorization. For example the permissions are matched to permission groups enhancing the user experience by simplifying the complexity of the application permissions. Furthermore, the categorization enhances the transparency of the applications allowing the users to grasp the needs and requirements of the applications.

Overall, users can easily identify the specific aspects of their device, hardware, and the application intend to access, therefore fostering trust and informed decision-making. This includes the potential risks that are associated with granting permissions and enables users to make more informed choices about which applications they allow and the level of access.

## 4. RESULTS

**Table II** provides a summary of the permissions extraction results, utilizing “x” to denote the presence of a permission in the manifest file of the applications and “-” to signify its absence. The table encompasses Audio and Camera permissions, along with permission categories Calendar, Location, Security and Authentication, Networking, and Internet and Connectivity. The rest of the Tables are available on GitHub [45] due to the space limitations of the paper. Above, we present the analysis of the results based on **Table II** and the rest Tables that are available on GitHub.

### 4.1. Facebook Lite

Facebook Lite, designed for low-end devices and slower internet connections, offers data usage and performance benefits but poses privacy trade-offs. Access to the microphone and camera raises concerns about potential audio and video surveillance without explicit consent. However, limitations on background camera usage and audio access mitigate these risks. A privacy advantage of Facebook Lite is its limited access to calendar data. However, there are certain mitigating factors to consider including the fact that the application is unable to use the camera as a background service and cannot access media audio, which slightly reduces the risks associated with background camera usage and unauthorized audio manipulation. Furthermore, Facebook Lite does not have access to modify users' events protecting schedules from potential unwanted viewing or tampering. In terms of connectivity and network permissions, Facebook Lite uses Bluetooth and grants access to the network states allowing the change of the Wi-Fi state. Whereas some of the permissions are important for the core functionalities of the applications, users should exercise extra caution and be informed of such activities, especially those that are running in the background.

### 4.2. Facebook

Facebook is the main mobile application of the popular social network which offers a comprehensive social media experience but raises more privacy concerns compared to Facebook Lite. Both versions grant access to the microphone and camera, however, introducing audio and video surveillance risks. For example, the full version of Facebook allows the application to modify audio settings and access the calendar. This functionality enables users to be informed from their local calendar about future events, however, the calendar information might be possible to be intercepted. In terms of networking permissions, Facebook grants access to the Bluetooth and network access. Even if the above are necessary for the core functionalities they should be carefully managed to avoid potential security and privacy risks.

### 4.3. Messenger

Facebook Messenger is the dedicated messaging application from Facebook providing instant messaging, voice calls, and audio/video sharing capabilities. However, granting permission to access the microphone, and camera raises significant privacy concerns. The application maintains the ability to access the microphone and camera which means that it can potentially listen to conversations or record audio and video without explicit user consent, especially if they are granted permission to run in the background. This poses serious privacy risks since conversations can be intercepted and information can be retrieved specifically to enhance marketing or promotional advertisements improving the commercial identity of the user. On a positive note, Messenger does not maintain the ability to use the camera in the background service, reducing the risk of unauthorized camera access without users' knowledge. Additionally, it does not have access to calendar data,

TABLE II: APP PERMISSIONS OVERVIEW

Permissions	Facebook lite	Facebook	Messenger	WhatsApp	Instagram	TikTok	Spotify	YouTube
Category: Audio and camera recording								
RECORD_AUDIO	x	x	x	x	x	x	x	x
CAMERA	x	x	x	x	x	x		x
MODIFY_AUDIO_SETTINGS	–	x	x	x	x	x	x	x
READ_MEDIA_AUDIO	–	–	x	x	–	x	x	–
FOREGROUND_SERVICE_CAMERA	–	–	x	–	–	–	–	–
Category: Calendar								
WRITE_CALENDAR	x	x	–	–	–	–	–	–
READ_CALENDAR	x	x	–	–	–	–	–	–
Category: Location								
ACCESS_COARSE_LOCATION	x	x	x	x	–	x	–	x
ACCESS_FINE_LOCATION	x	x	x	x	x	–	–	x
ACCESS_MEDIA_LOCATION	–	x	–	x	x	–	–	–
Category: Security and authentication								
AUTHENTICATE_ACCOUNTS	x	x	x	x	–	–	–	–
USE_BIOMETRIC	–	x	x	x	x	–	–	x
USE_FINGERPRINT	–	x	x	x	x	–	–	x
Category: Networking								
BLUETOOTH	x	–	x	x	x	x	x	–
ACCESS_NETWORK_STATE	x	x	x	x	x	x	x	x
CHANGE_NETWORK_STATE	x	x	x	x	–	x	–	–
CHANGE_WIFI_STATE	x	x	x	x	–	–	–	–
ACCESS_WIFI_STATE	x	x	x	x	–	x	x	x
BLUETOOTH_ADVERTISE	x	x	–	–	–	–	x	–
BLUETOOTH_SCAN	x	x	–	–	–	–	x	–
BLUETOOTH_ADMIN	x	x	–	–	–	–	x	–
BLUETOOTH_CONNECT	x	x	–	–	–	x	x	–
CHANGE_WIFI_MULTICAST_STATE	x	x	–	–	–	x	x	–
NEARBY_WIFI_DEVICES	x	x	–	x	–	–	–	–
Category: Internet and connectivity								
INTERNET	x	x	x	x	x	x	x	x

which means it cannot view or modify users' events, providing some level of event privacy.

#### 4.4. WhatsApp

WhatsApp is a proprietary instant messaging application for mobile phones. In addition to exchanging text messages, users can send each other images, videos, sounds, and multimedia messages. However, it grants access to the microphone and camera to achieve the above. If run in the background these permissions introduce potential security and privacy risks. Regarding the access to networking permissions, WhatsApp maintains access to Bluetooth, network state, and Wi-Fi-related permissions.

#### 4.5. Instagram

Instagram is a photo and video sharing social media platform that among others offers instant messaging between users and live video uploading. Instagram is granted access to the microphone and camera possible to be run as a background service. The capability of the application to access the microphone in the background raises concerns about potential audio interception. Instagram is granted also access to media which can lead to security and privacy implications, as it may gather information from media files that users share or upload. However, it does not grant the ability to use the camera as a background service, which reduces the risk of unauthorized background

camera usage. Finally, Instagram does not maintain any access to calendar data, safeguarding users' events from unauthorized viewing or changes.

#### 4.6. TikTok

TikTok is a popular video-sharing platform where users can upload and watch short videos. The application grants access to the device's microphone, camera, and media. Therefore, it maintains the capability to access personal media files or audio which could lead to data privacy implications, as it may extract information from the media files that are uploaded. However, the camera is not accessed as a background service, reducing the risk of unauthorized background camera usage. The networking permissions are associated mostly with Bluetooth and network access.

#### 4.7. Spotify

Spotify is a music streaming application that offers a very large library of songs and access to playlists. Unlike social media applications and other media applications, Spotify do not access the microphone or camera. However, it collects audio data for conducting analytics and targeted advertising purposes related to the music experience. Users should be aware that their audio preferences and listening habits may be used for these purposes. Regarding networking permissions, Spotify maintains access to Bluetooth to allow interaction with Bluetooth devices including wireless

headphones and speakers. Spotify also maintains access to network and Wi-Fi states, necessary for streaming music and connecting to the internet. However, it should be noted that Spotify does not have the ability to change network or Wi-Fi settings, which reduces the risk of unauthorized changes to the device's connectivity.

#### 4.8. YouTube

YouTube is a video-sharing platform where users can watch, and share videos. The application has access to the microphone, and camera, and it is possible to modify audio settings, raising concerns about potential unauthorized audio and video surveillance. Regarding networking permissions, YouTube maintains access to Bluetooth, network states, and access to nearby Wi-Fi devices. Whereas these permissions are essential for video streaming and connecting to the internet, users should be cautious about potential security and privacy risks, especially concerning Bluetooth and Wi-Fi device change states and access in the background.

### 5. DISCUSSION

The results from the analysis reveal that each application possesses distinct functionalities regarding the device hardware. This results in specific advantages or disadvantages concerning the security and privacy risks of the users. Whereas some applications offer benefits such as restricted access to specific permissions and end-to-end encryption, they share common concerns regarding potential audio and video surveillance, audio manipulation, and data privacy implications. Nevertheless, certain applications effectively mitigate specific risks related to media access and background camera usage. Therefore, it is imperative for users to meticulously scrutinize and comprehend the permissions and features of each app, enabling them to make informed decisions regarding their privacy and security.

Furthermore, we recommend key strategies for enhancing online privacy. We amalgamate the primary attributes that define an "Information Privacy Aware User," as delineated by Soumelidou and Tsohou [46], with protective strategies for online users of the third domain of the InfoPrivacy CBK [47]. Initially, users should thoroughly examine the privacy policy, terms, and other vital information found on the App Store description's details page before selecting and installing an app. It is essential to closely inspect the app's requested permissions and the types of user data it may collect. Opting for applications that either require minimal permissions or none at all represents the safest and least risky choice.

Once the application is installed, they should pay attention to the various requests, as these are mainly dangerous permissions that concern their personal data, and this is how the system tries to explain to them why the application is accessing this source. This is a way for them to understand the purpose of the permission request and then judge for themselves whether it is related to the functionality of the app, in which case they should accept it, or if it is related to advertising purposes, in which case they should reject it.

At this point, it is worth remembering that whether the permission request is related to location, microphone, or camera, the user is faced with three options, deny access, accept only this time, or accept while using the application. In this case, it is preferable to select the "Only this time" option, as it will limit the data offered to the application unless we deny the request. In any case, it is good to be careful and avoid careless clicks out of haste or carelessness. We also recommend that users make use of their smartphone's permission manager so that they can always see the permissions granted to the various applications and configure them accordingly to better align with their privacy objectives.

In addition to permissions, users need to be aware of the privacy settings that are available in their profile in the various applications and modify them accordingly. One prominent example is to limit the audience to which their posts are addressed, etc. In conclusion, users should be more concerned about any use of their data, unwilling and suspicious about providing them to the applications. They also need to be aware of the laws that protect their right to privacy as well as the potential threats and associated consequences of disclosing their personal information. Furthermore, users should be familiar with privacy enhancing mechanisms and strategies to address information privacy issues not only in applications but in their online habits in general.

Our research findings, coupled with the aforementioned strategies, can serve as the foundation for training and educational programs aimed at imparting a comprehensive understanding of Android permissions, their significance, and their implications for information privacy to students and internet users. Participants can acquire valuable knowledge and skills related to application permissions, gain heightened awareness of privacy threats, and ultimately adopt more privacy-conscious online behaviors by making well-informed decisions when granting permissions.

Indicatively privacy trainers can begin a workshop by presenting the seven most popular applications or similar and categorize them according to their functions, namely social media, communication, or media streaming. The results and insights from this research can be utilized to group permissions into categories, facilitating interactive exercises that encourage participants to categorize permissions. Discussions about privacy concerns associated with different permission categories will raise awareness of potential risks. Through case studies and hands-on activities, participants can analyze permissions requested by applications and speculate on their usage, empowering them to make informed decisions about application permissions.

### 6. CONCLUSION

Managing mobile privacy is an increasingly challenging task for today's users. They have to make many complex privacy decisions about application permissions on a daily basis, but they do not seem to be well prepared and equipped for that. By extracting and analysing the permissions of seven of today's most popular applications,

we aim to stress the knowledge and skills that a user should have about them so that they are more aware and able to protect their privacy online. Our ultimate goal is to help users make more informed decisions, enhance their awareness, and strengthen the protection of their privacy in the various applications and on the internet in general.

Future work encompasses several pivotal milestones built upon the insights garnered from our research. Initially, we plan to create and refine the workshop content, tailoring it to diverse audiences and integrating hands-on experiences into university courses that relate to information privacy. Our efforts will extend beyond the classroom through interactive sessions, ensuring accessibility for a global audience. A dynamic feedback loop between research and practice will facilitate continuous improvement and further exploitation of the results and the validation of the conducted workshops. Long-term assessment will ensure the needed refinements in terms of education and learning impact, and the dissemination of best practices will contribute to the broader field of privacy education.

Although our work is limited by the fact that we only studied a small number of applications, our approach can be useful because it relates to seven of the most popular and most downloaded applications of all time. Our work can be beneficial for internet users, privacy awareness and training programs developers, teachers, the academic community in general as well as the industry.

#### ACKNOWLEDGMENT

This work was partially supported by EU ECSEL project DAIS which has received funding from the ECSEL JU under grant agreement No. 101007273.

#### CONFLICT OF INTEREST

Authors declare that they do not have any conflict of interest.

#### REFERENCES

- Lin CS. Educating students' privacy decision making through information ethics curriculum. *Creat Educ*. 2016;07(01):171–9. doi: 10.4236/ce.2016.71017.
- Andriotis P, Li S, Spyridopoulos T, Stringhini G. A comparative study of android users' privacy preferences under the runtime permission model. *Lect Notes Comput Sci*. 2017;10292:604–22. doi: 10.1007/978-3-319-58460-7\_42.
- Brandtzaeg PB, Pultier A, Moen GM. Losing control to data-hungry: a mixed-methods approach to mobile app privacy. *Soc Sci Comput Rev*. 2018 May 31;37(4):466–88. doi: 10.1177/0894439318777706.
- Affonso EP, Sant'Ana RCG. Privacy awareness issues in user data collection by digital libraries. *IFLA J*. 2018 Aug 21;44(3):170–82. doi: 10.1177/0340035218777275.
- Lin J, Amini S, Hong JI, Sadeh N, Lindqvist J, Zhang J. Expectation and purpose. *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, 2012 Sep 5. doi: 10.1145/2370216.2370290.
- Alecakir H, Can B, Sen S. Attention: there is an inconsistency between android permissions and application metadata! *Int J Inf Secur*. 2021 Jan 7;20(6):797–815. doi: 10.1007/s10207-020-00536-1.
- Freire-Garabal y Nuñez M. *General Vision of the Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016*. Al-Khalifa Business School; 2020 Jun 21. 10.21428/18d9181c.39ae71fc.
- Smullen D, Feng Y, Aerin Zhang S, Sadeh N. The best of both worlds: mitigating Trade-offs between accuracy and user burden in capturing mobile app privacy preferences. *Proc Priv Enh Technol*. 2020 Jan 1;2020(1):195–215. doi: 10.2478/popets-2020-0011.
- Almuhimedi H, Schaub F, Sadeh N, Adjerid I, Acquisti A, Gluck J, et al. Your location has been shared 5,398 times! *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2015 Apr 18. doi: 10.1145/2702123.2702210.
- Baarslag T, Alan AT, Gomer RC, Liccardi I, Marreiros H, Gerding EH, et al. Negotiation as an interaction mechanism for deciding app permissions. *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, 2016 May 7. doi: 10.1145/2851581.2892340.
- Felt AP, Ha E, Egelman S, Haney A, Chin E, Wagner D. Android permissions. *Proceedings of the Eighth Symposium on Usable Privacy and Security*, 2012 Jul 11. doi: 10.1145/2335356.2335360.
- Scoccia GL, Ruberto S, Malavolta I, Autili M, Inverardi P. An investigation into android run-time permissions from the end users' perspective. *Proceedings of the 5th International Conference on Mobile Software Engineering and Systems*, pp. 45–55, 2018, May.
- Wijesekera P, Baokar A, Tsai L, Reardon J, Egelman S, Wagner D, et al. The feasibility of dynamically granted permissions: aligning mobile privacy with user preferences. *IEEE Symposium on Security and Privacy (SP)*, 2017 May. doi: 10.1109/sp.2017.51.
- Andriotis P, Takasu A, Tryfonas T. Smartphone message sentiment analysis. *Lect Notes Comput Sci*. 2014;433:253–65. doi: 10.1007/978-3-662-44952-3\_17.
- Solanki RK, Laxmi V, Gaur MS. MAPPER: mapping application description to permissions. *Risks Secur Internet Syst*. 2020;12026:84–98. doi: 10.1007/978-3-030-41568-6\_6.
- Feichtner J, Gruber S. Understanding privacy awareness in android app descriptions using deep learning. *Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy*, 2020 Mar 16. doi: 10.1145/3374664.3375730.
- Raber F, Krueger A. Towards understanding the influence of personality on mobile app permission settings. *Lect Notes Comput Sci*. 2017;10516:62–82. doi: 10.1007/978-3-319-68059-0\_4.
- Lutaaya M. Rethinking app permissions on iOS. *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, Montréal, QC, Canada, 2018 Apr 20. doi: 10.1145/3170427.3180284.
- Kokolakis S. Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon. *Comput Secur*. 2017 Jan;64:122–34. doi: 10.1016/j.cose.2015.07.002.
- Barnes SB. A privacy paradox: social networking in the United States. *First Monday*. 2006 Sep 4;11. doi: 10.5210/fm.v11i9.1394.
- Ashawa M, Morris S. Android permission classifier: a deep learning algorithmic framework based on protection and threat levels. *Secur Priv*. 2021 May 5;4(5):1–26. doi: 10.1002/spy2.164.
- Android.com. Permissions on Android. [Accessed 01-10-2023]. Available from: <https://developer.android.com/guide/topics/permissions/overview>.
- Saleem MS, Mišić J, Mišić VB. Android malware detection using feature ranking of permissions. 2022. arXiv preprint arXiv:2201.08468.
- Gruschka N, Iacono LL, Tolsdorf J. Classification of android app permissions: Tell me what app you are and I tell you what you are allowed to do. *17th European Conference on Cyber Warfare and Security (ECCWS 2018)*, Jøsang Ed. Oslo, Norway, 28–29 June 2018, pp. 181–189, Curran.
- Arp D, Spreitzenbarth M, Hübner M, Gascon H, Rieck K, Drebin: effective and explainable detection of android malware in your pocket. *Proceedings 2014 Network and Distributed System Security Symposium*, 2014. doi: 10.14722/ndss.2014.23247.
- Yan LK, Yin H. {DroidScope}: seamlessly reconstructing the {OS} and dalvik semantic views for dynamic android malware analysis. *21st USENIX Security Symposium (USENIX security 12)*, 2012. doi: 10.1109/mprv.2013.43.
- Wang W, Wang X, Feng D, Liu J, Han Z, Zhang X. Exploring permission-induced risk in android applications for malicious application detection. *IEEE Trans Inf Foren Sec*. 2014 Nov;9(11):1869–82. doi: 10.1109/tifs.2014.2353996.
- Dash SK, Suarez-Tangil G, Khan S, Tam K, Ahmadi M, Kinder J, et al. DroidScribe: classifying android malware based on runtime behavior. *2016 IEEE Security and Privacy Workshops (SPW)*, 2016 May. doi: 10.1109/spw.2016.25.
- McLaughlin N, Martinez del Rincon J, Kang B, Yerima S, Miller P, Sezer S, et al. Deep android malware detection. *Proceedings of the Seventh ACM Conference on Data and Application Security and Privacy*, 2017 Mar 22. doi: 10.1145/3029806.3029823.



- [30] Saxe J, Berlin K. Deep neural network based malware detection using two dimensional binary program features. *2015 10th International Conference on Malicious and Unwanted Software (MALWARE)*, 2015 Oct. doi: 10.1109/malware.2015.7413680.
- [31] David OE, Netanyahu NS. DeepSign: deep learning for automatic malware signature generation and classification. *2015 International Joint Conference on Neural Networks (IJCNN)*, 2015 Jul. doi: 10.1109/ijcnn.2015.7280815.
- [32] Biswas S, Haipeng W, Rashid J. Android permissions management at app installing. *Int J Secur Its Appl*. 2016 Mar 31;10(3):223–32. doi: 10.14257/ijasia.2016.10.3.21.
- [33] Liu B, Andersen MS, Schaub F, Almuhimedi H, Zhang SA, Sadeh N, et al. Follow my recommendations: a personalized privacy assistant for mobile app permissions. *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, 2016.
- [34] Lin J, Liu B, Sadeh N, Hong JI. Modeling {Users'} mobile app privacy preferences: restoring usability in a sea of permission settings. *10th Symposium on Usable Privacy and Security (SOUPS 2014)*, 2014.
- [35] Lee H, Kobsa A. Privacy preference modeling and prediction in a simulated campuswide IoT environment. *IEEE International Conference on Pervasive Computing and Communications (PerCom)*, 2017 Mar. doi: 10.1109/percom.2017.7917874.
- [36] SoftwareTestingHelp. 15 globally most downloaded apps of all time [2023 List]. 2023. [Accessed 01-10-2023]. Available from: <https://www.softwaretestinghelp.com/most-downloaded-apps/>.
- [37] Facebook—Facebook.com. [Accessed 01-10-2023]. Available from: <https://www.facebook.com>.
- [38] Messenger. [Accessed 01-10-2023]. Available from: <https://www.messenger.com>.
- [39] WhatsApp—Secure and reliable free private messaging and calling. [Accessed 01-10-2023]. Available from: <https://www.whatsapp.com/>.
- [40] Instagram—Instagram.com. [Accessed 01-10-2023]. Available from: <https://www.instagram.com>.
- [41] Explore—Find your favourite videos on TikTok—tiktok.com. [Accessed 01-10-2023]. Available from: <https://www.tiktok.com>.
- [42] Spotify—Web player: music for everyone—spotify.com. [Accessed 01-10-2023]. Available from: <https://spotify.com>.
- [43] YouTube—Youtube.com. [Accessed 01-10-2023]. Available from: <https://www.youtube.com>.
- [44] Facebook Lite. [Accessed 01-10-2023]. Available from: <https://lite.facebook.com>.
- [45] GitHub-ionianCTF/privacy-permission-analysis: privacy: permission analysis for Android Applications—github.com. [Accessed 01-10-2023]. Available from: <https://github.com/ionianCTF/privacy-permission-analysis>.
- [46] Soumelidou A, Tsohou A. Towards the creation of a profile of the information privacy aware user through a systematic literature review of information privacy awareness. *Telemat Inform*. 2021;61:101592.
- [47] Lavranou R, Tsohou A. Developing and validating a common body of knowledge for information privacy. *Inf Comput Secur*. 2019;27(5):668–86.