

UNDERSTANDING THE IMPACT OF APP PERMISSIONS ON SENSITIVE USER INFORMATION

Ashutosh Ramdas Choudhari¹, Pravin Rushikant Jagdale², Onkar Balkrushna Ubhe³

³Department of Computer Application, PVG's College of Science and Commerce, Pune, Savitribai Phule Pune University

⁴Research Guide, Department of Computer Application, PVG's College of Science and Commerce, Pune, Savitribai Phule Pune University

Abstract - Mobile apps are now a basic part of our daily life. We use them for chatting, entertainment, studying, shopping, banking, and many other tasks. To work properly, apps ask for different types of permissions such as location, contacts, camera, microphone, and storage. Some of these permissions are important for the app to function, but many apps ask for extra permissions that are not needed. These unnecessary permissions can put the user's personal data at risk. This research studies how mobile app permissions affect sensitive user information and how they may lead to privacy problems. In this study, 100 Android apps from categories like social media, games, finance, and productivity were analyzed. Tools such as the Android Manifest file, MobSF, and APK Analyzer were used to check what types of permissions each app requested. Permissions were divided into three groups: Normal, Dangerous, and Unnecessary. The results showed that around 65% of apps asked for permissions that were not linked to their main work. Many apps requested high-risk permissions like storage (90%), location (80%), camera (60%), and contacts (40%). These permissions can reveal private data if misused. The study also looked at real cases where apps misused permissions. For example, CamScanner was found to contain malware, Facebook collected background data without need, and Zoom had issues with unauthorized camera and microphone access. These cases show that extra permissions can lead to serious security and privacy problems. The research also found that many apps use third-party libraries that secretly collect user data for advertising and analytics.

Key Words: permissions, privacy, Android, security, user data, mobile apps.

1. INTRODUCTION

Mobile apps have become an important part of our everyday life. We use apps for calling, chatting, watching videos, finding locations, playing games, and completing office or college work. Because apps make our life easier, people install many apps on their phones without thinking much about them. But every app that we install asks for certain permissions. These permissions allow the app to access different parts of our phone, such as contacts, camera, gallery, microphone, or location.

Some permissions are important for the app to work properly. For example, a camera app needs permission to use the camera, and a maps app needs permission to access the location. But in many cases, apps ask for permissions that they do not actually need. When users agree to these permissions without checking, it can create privacy and security risks. Personal information may get collected, misused, or shared with third-party companies without the user knowing.

Many users simply tap on “Allow” when they see permission pop-ups. They do not read what the app wants to access or why. This is known as “permission fatigue,” where users get tired of reading too many permission messages. Because of this, people unknowingly share sensitive information like photos, contact lists, messages, or their exact location. Hackers or malicious apps can misuse this information for identity theft, data leaks, fraud, or spying.

This research focuses on understanding how mobile app permissions work and how they affect user privacy. It also studies how often apps ask for risky permissions, how users react to these requests, and what danger these permissions can cause. Real-life cases such as CamScanner malware and Facebook’s background data collection show that wrong permissions can lead to big privacy problems.

2. OBJECTIVES

- To study how mobile apps use permissions and how this affects user privacy and security.
- To identify which app permissions are necessary and which are unnecessary or risky.
- To examine how often apps request sensitive permissions like location, contacts, camera, and storage.
- To analyse how users behave when granting permissions and how “permission fatigue” affects their decisions.
- To find out whether users understand the risks of giving permissions that apps don’t actually need.
- To study real case examples where apps misused permissions and caused privacy problems.
- To categorize permissions into normal, dangerous, and unnecessary using Android’s permission model.
- To measure how many apps over-request permissions beyond what their main function requires.
- To identify how background data access by apps increases privacy risks for users.
- To study how third-party libraries inside apps collect user data through permissions.
- To raise awareness about how apps collect personal information without users noticing.
- To evaluate whether built-in permission managers in Android and iOS effectively protect user privacy.
- To explore the idea of “privacy nudges” that remind users to check or change their permissions.
- To study the risks of data leaks, identity theft, and unauthorized access caused by excessive permissions.
- To propose solutions for safer permission practices for users, developers, and mobile platforms.

3. LITERATURE REVIEW

In this literature review, I have highlighted crucial results from the research on the security and privacy issues related to mobile application permissions. I focus on the user’s behavioral patterns, the problems arising from data harvesting, and the shortcomings of existing privacy protection mechanisms to delineate the research scope. As much as mobile device have been adopted, mobile application usage, too, have curved its niche into the daily routines for many individuals. There is, however, a downside to this convenience – the ever-increasing privacy and security concerns. Mobile applications require users to allow many permissions which include sensitive device options and personal data access, such as contact, geographical location as well as the camera. There

are situations where these permissions are crucial to the effective running of the application, however, these are also situations where data misuse and unauthorized third-party sharing are more probable.

According to a study by Degirmenci in 2020, there is a big challenge with how much mobile app users worry about their privacy, and other researchers may not have paid enough attention to this issue. The study surveyed 775 people and found that concerns about app permissions were a very strong sign of a user's overall privacy worries.

This is especially true for mobile apps, which is why the study calls this "app permission anxiety." Another study cited by Degirmenci, a Pew Research Center Survey, supports this idea. That survey found that 54% of mobile users decided not to install an app, and 30% uninstalled one they already had, all because they were worried about their privacy.

Throughout the literature, one persistent theme is the gap between user concern and user action. Although many users express discomfort with the permissions their apps request, the number of requests can be staggering. This is termed "permission fatigue" or "privacy fatigue," and it describes a state in which users acquiesce to permissions without consideration of the full consequences. Investigations indicate that users are prompted to grant requests simply for the sake of expediency or because of a disorientation to the issues being addressed. This lapse in protocol is the first major failure in protecting one's privacy, as users are completely oblivious to the risks of a data breach, leakage, or misuse. Amirulbahar and Ruldeviyani (2023) examine this dynamic through case studies of a money transfer application. Their studies revealed that users' concerns about privacy and trust on the app are very correlated and influenced by the user's fatigued awareness of privacy. This implies that the user's concern about app permissions is more than a standalone issue; it is part of a user's extensive apprehension toward information sharing and trust toward the service provider.

In regard to the issue of privacy which is a growing concern mobile operating systems such as Android and iOS have put in place solutions which inform the user and which also give them a degree of control over which permissions are granted. This includes just in time permission dialogs which appear at the point of an app's request for access to a certain resource and also built in privacy and permission managers.

Regardless of the advancements made in data privacy tools, the effectiveness of the tools has been a crucial point of discussion in surrounding frameworks and articles. These permissions offer finer-grained controls, but they "substantially increase the number of choices users must consider". Researchers have found out that its permission managers which alone have proven to be inadequate in the ability to guarantee the satisfactory level of privacy a user desires.

As different approach research has looked into the use of "privacy nudges" which we put forward as a way to support users' decisions. Nudges are what we may term light touch interventions which put forth to the user the chance to think through their privacy settings without taking away from their choices. We see that these types of nudges which inform the user of how often apps access personal data do in fact raise awareness and cause them

to go in and review and adjust their permissions. While they may be the answer we are looking for, they at this time have not seen large scale implementation.

Overall, research shows that mobile app permissions are a big problem for privacy and security. Even though users know about these risks, they often feel overwhelmed by how complicated it is to manage permissions. This leads to "privacy fatigue", where users tend to simply agree to requests without much thought. While mobile operating systems have added features like built-in permission managers and pop-up requests, these solutions often don't work as well as intended in real-life situations. Studies by Ghogare et al. (2024) suggest we need to analyze risks and find solutions, while work by Liu et al. (2016) and Degirmenci (2020) points to the need for more proactive, user-friendly solutions like personal assistants or "privacy nudges" to help users make better decisions. While the issue of mobile app permission security and user awareness is reported on extensively, we see a great need for practical, effective, and wide spread solutions in the area of data protection in the digital world.

4. METHODOLOGY

This research focuses on understanding how mobile app permissions affect the privacy and security of user data. The study follows a qualitative and analytical approach, centered on analyzing app behavior and permission use.

- ***App Selection and Permission Analysis:***

1. A total of 100 Android applications were selected from common categories such as social media, Productivity, Entertainment, and Games.
2. Each app was studied to identify:
 1. The type of permissions requested during installation and usage.
 2. Whether these permissions were necessary for the app's main functionality.
 3. The possible privacy or security risks associated with each permission.
 4. Permission data were collected through the Android Manifest file using Mobile Security

Framework (MobSF) and APK Analyzer tools.

5. Each permission was categorized as normal, dangerous, or unnecessary, based on Google's Android permission classification.

- ***Case Study Observation:***

1. To understand how permissions can lead to misuse, a few well-known apps were reviewed as case examples.
2. These included:

1. CamScanner (2019): Found to contain hidden malware that misused storage and network permissions.
2. Facebook (2020): Collected location and contact data even when not required for core functions.
3. Zoom (2021): Faced issues with unauthorized camera and microphone access.
4. Through these examples, the research aimed to identify patterns of over- permission requests and analyze how they relate to user data exposure.

5. MODELING AND ANALYSIS

This research's analytical model depends on foundational works surrounding the classification of security and privacy risks. In particular, we have utilized the Google Android permission model, which sorts the access permission requests into three tiers of risk: Normal, Dangerous, and Unnecessary. This model sits at the foundation of our analytical framework for estimating the threat value of mobile apps. This classification also determines the ‘material’ of our study: Normal Permissions: These enjoy the classification of low risk, and offer access to the features of the application at a relatively isolated and independent level, and have little risk to the privacy of the user and the privacy of their other apps. Like permissions for network access, or wallpaper setting, which have become a utility app wallpaper. These are considered baseline requirements for most utility apps.

1. *Dangerous Permissions:*

This classification identifies which permissions can gain access to very sensitive personal information and give some control over the user’s variable stored information and functioning device features. This includes the use of the camera, the microphone, contacts, or accurate geolocation. Our model identifies the use of such permissions as critical vulnerabilities, especially when they are not essential to the primary function. Unnecessary/Over-Permissions (Material Overlap): This is not an official definition by Google, but for operational purposes, this is incorporated as permissions the app requests that are completely irrelevant to its primary stated function. The model identifies the existence of such “over-permissions” as strong evidence of disregard for the Least Privilege principle. This practice not only increases the app's attack surface but also contributes directly to "permission fatigue," which was identified as a key behavioral factor in the Literature Review. This theoretical model we present which is based on well-known permission hierarchies which we in turn augmented with the element of practical necessity (or its absence) puts forth a very robust framework for the assessment of both the quantitative and qualitative aspects of privacy exposure in the set of studied applications. We go on to report on the results of that which looks at the frequency of these three risk factors in the 100 studied applications. A look at which permissions are distributed and also, we look at and report on behavioral patterns and risk.

2. *Permission Distribution Analysis:*

In the analysis of the 100 applications, we saw a large trend toward risk bearing permissions. The aggregated data series, based on the total number of permissions identified, demonstrated that the combined proportion of Dangerous and Unnecessary permissions significantly outweighs the baseline Normal requirements.

The results of the distribution were as follows:

1. *Normal Permissions:*

These permissions made up 22% of the total permissions asked for. While they are for basic functions which is great, their small size in the request set indicates that out of the 100 apps' requests for permissions which we looked at, the bulk of the time they are asking for more than what is necessary. Also, we see What I will term as dangerous permissions to be at 18% of the total. That large a proportion proves out that there is a very real issue with what data may be exposed. That almost one fifth of all permissions which are asked for fall into this category is a red flag that developers are asking for access to very private features of the device (like location, storage, and camera) which the app may not actually need based on what it is supposed to do.

2. *Unnecessary Permissions:*

This in which we put forth our own definition and which is of low value made up 10% of the requests. Although the smallest group this 10% represents permissions which do not add to the core function of the system and which instead contribute to privacy issues and risk without in fact adding value to the user. This distribution also shows that 28% of all permissions identified (18% Dangerous and 10% Unnecessary) either present a large-scale threat to data or are brought up without reason which in turn goes against best practice in security. Behavioral and Risk Pattern Analysis. In addition to the raw numbers, we identified a few key behavioral trends and issues which present risk.

6. SURVEY QUESTIONS

1. Age Group
 1. Below 18
 2. 18-25
 3. 26-35
 4. 36-45
 5. Above 45
2. Smartphone Type
 1. Android
 2. iOS
 3. Other
3. How often do you check app permissions before installing an app?
 1. Always
 2. Sometimes
 3. Never
 4. Rarely
4. Do you understand what 'dangerous permissions' mean?
 1. Yes
 2. No
 3. Not Sure
5. Which permissions do you think are most sensitive?
 1. Location
 2. Camera
 3. Microphone
 4. Contacts
 5. Storage
 6. SMS / Call logs
6. Do you allow app permissions without reading them?
 1. Yes
 2. Sometimes
 3. No
7. Have you ever uninstalled an app due to too many permissions?
 1. Yes
 2. No

8. How concerned are you about data privacy?

1. Not concerned

2. 1

3. 2

4. 3

5. 4

6. 5

7. Extremely concerned

9. Do apps often request unnecessary permissions?

1. Yes

2. No

3. Not Sure

10. Have you faced privacy issues due to apps?

1. Yes

2. No

11. Do you manually review and change app permissions?

1. Yes

2. No

3. Sometime

12. Which type of apps over-request permissions the most?

1. Social Media

2. Games

3. Finance

4. Entertainment

5. Utility Apps

6. Others

13. Do you know about third-party libraries collecting data?

1. Yes

2. No

3. Not Sure

14. Are you aware that some apps access data in the background?

1. Yes

2. No

Which risky permissions have you seen apps request?

3. Background Location
4. Camera
5. Storage
6. Contacts
7. Microphone
8. SMS/Call logs

15. Do you trust apps from Play Store/App Store?

1. Completely
2. Somewhat
3. Not at all

16. Should Android/iOS give clearer permission warnings?

1. Yes
2. No

17. How do you protect your digital privacy?

1. Avoid unknown apps
2. Deny unnecessary permissions
3. Use antivirus
4. Read reviews
5. Change permissions regularly
6. None

18. Who is responsible for data privacy?

1. Users
2. Developers
3. App Stores (Google/Apple)
4. All equally

7. RESULTS

Demographic and Device Information

Data Point	Category	Percentage	Count
Smartphone Type	Android	90.90%	N/A
	iOS	9.10%	N/A
Age Group	Below 18	N/A	N/A
	18-25	78.80%	N/A
	26-35	15.20%	N/A

1. User Behavior Regarding Permissions

Question	Response	Percentage
How often do you check app permissions before	Sometimes	48.50%

installing an app?	Always	45.50%
Do you allow app permissions without reading them?	Sometimes	51.50%
	No	39.40%
	Yes	9.10%
Do you manually review and change app permissions?	Yes	51.50%
	No	15.20%
	Sometimes	33.30%
Have you ever uninstalled an app due to too many permissions?	Yes	84.80%
	No	15.20%

2. User Awareness and Perception of Risk

Question	Response	Percentage
Do you understand what "dangerous permissions" mean?	Yes	75.80%
	Not Sure	18.20%
How concerned are you about data privacy? (Scale 1-5, 5 being most concerned)	5 (Most Concerned)	54.50%
	4	15.20%
	3	18.20%
Do apps often request unnecessary permissions?	Yes	66.70%
	Not Sure	21.20%
	No	12.10%
Are you aware that some apps access data in the background?	Yes	87.90%
Do you know about third-party libraries collecting data?	Yes	60.60%
	No	24.20%
	Not Sure	15.20%
Should Android/iOS give clearer permission warnings?	Yes	84.80%

3. Specific Permission Risks and App Types

Permission/App Type	Percentage of Users Citing as Sensitive/Over-requesting
Most Sensitive Permission: Camera	84.80%
Most Sensitive Permission: Microphone	66.70%
Most Sensitive Permission: Storage	66.70%
Most Sensitive Permission: Location	63.60%
Most Sensitive Permission: Contacts	63.60%
Most Sensitive Permission: SMS/Call logs	60.60%
Risky Permission Seen: Camera	63.60%
Risky Permission Seen: Background Location	60.60%
Risky Permission Seen: Contacts	57.60%
App Type Over- requesting: Social Media	60.60%
App Type Over- requesting: Games	48.50%

4. Security Practices and Trust

Question	Response	Percentage
How do you protect your digital privacy? (Top 2 responses)	Avoid unknown apps	75.80%
	Deny unnecessary permissions	72.70%
Do you trust apps from Play Store/App Store?	Somewhat	57.60%
	Completely	24.20%
	Not at all	18.20%
Have you faced privacy issues due to apps?	Yes	54.50%
	No	45.50%
Who is responsible for data privacy?	All equally	69.70%
	Users	18.20%

8. DISCUSSION

- The study highlights that the main challenge with app permissions is unnecessary data access combined with low user awareness.
- User Behavior: Most users allow permissions automatically without checking why they are needed. This results in privacy exposure, especially for sensitive data such as contacts, photos, or location.
- Developer Practices: Developers sometimes include extra permissions for analytics or ads. This creates privacy risks and shows a lack of proper permission control.
- Platform Role: Android and iOS provide permission controls, but users rarely explore these settings. App stores and operating systems must make permission explanations clearer and more visible.
- The problem is not only technical but also behavioral — balancing user convenience and security is crucial.
-

9. CONCLUSION

This research concludes that mobile app permissions play a major role in user data privacy. While permissions are necessary for proper app functioning, many applications misuse them or request more than required. Such behavior leads to privacy breaches and potential data exploitation.

To reduce these risks:

1. Developers should follow the least privilege principle and only request essential permissions.
2. Users should regularly check app permission settings and deny unnecessary access.
3. App platforms should monitor and warn users about apps that misuse or over-request permissions.
4. Awareness campaigns should educate people on data privacy and responsible digital use.

If both users and developers act responsibly, the mobile ecosystem can become far more transparent and secure.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the guidance, encouragement, and valuable feedback provided by **Dr. Swati Joshi**, along with faculty mentors and peers throughout the course of this research. We extend our sincere thanks to PVG's College of Science & Commerce, Pune, and collaborating institutions for providing the necessary resources and support. Their insights and constructive suggestions were instrumental in shaping the quality and direction of this study.

REFERENCES

1. Baldonado, M., Chang, C.-C.K., Gravano, L., Paepcke, A.: The Stanford Digital Library Metadata Architecture. *Int. J. Digit. Libr.* 1 (1997) 108–121
2. Bruce, K.B., Cardelli, L., Pierce, B.C.: Comparing Object Encodings. In: Abadi, M., Ito, T. (eds.): *Theoretical Aspects of Computer Software*. Lecture Notes in Computer Science, Vol. 1281. , (1997) 415–438
3. van Leeuwen, J. (ed.): *Computer Science Today. Recent Trends and Developments*. Lecture Notes in Computer Science, Vol. 1000. , (1995)
4. Michalewicz, Z.: *Genetic Algorithms + Data Structures = Evolution Programs*. 3rd edn. , (1996)