CSEC-729 Human Factors in Security & Privacy

Improving the Usability and Effectiveness of Privacy Indicators in Android

Mehul Sen[1] and Bhavana Avirneni[1]

[1]Golisano College of Computing and Information Sciences, Rochester Institute of Technology

December 13, 2023

1 Abstract

The proliferation of mobile applications utilizing sensitive resources such as cameras and microphones raises significant privacy concerns. Privacy Indicators (PI) have been introduced in Android systems as a visual cue to alert users when such resources are accessed. Despite their potential, the effectiveness and usability of these indicators still need to be explored. This study investigates the effectiveness of PI on Android devices and the feasibility of proposed solutions to enhance their effectiveness. The study had two phases. The first phase involved a questionnaire survey with mobile users to gather their perspectives on existing PI implementations. In the second phase, 20 Android and iOS users participated in a user study. They engaged with four 'naive' note-taking apps that simulated various resource usage scenarios while subtly integrating PI to measure whether and how the participants noticed and reacted to PI during app usage. We found that users claim to have significant concerns about privacy and believe that PI has some impact when managing their privacy. The user study revealed that none of the users could correctly identify resource usage based solely on the PI, indicating that PI in its current implementation is ineffective. Feedback on the proposed changes to PI revealed a clear need for a more proactive, informative, customizable, and noticeable PI implementation.

2 Introduction

In the digital age, mobile applications extensively utilize sensitive resources like cameras and microphones, raising significant privacy concerns. Privacy Indicators (PI) in Android systems serve as visual cues to inform users when such resources are accessed. However, the effectiveness and usability of these indicators need to be sufficiently explored, leading to potential gaps in user awareness and privacy protection.

This study addresses the knowledge gap surrounding the impact of PIs on user awareness and their understanding of privacy in Android devices. The importance of this study lies in its potential to enhance user privacy, trust, and security in an increasingly digital world. It also seeks to answer key research questions:

How effective are current PI implementations in Android systems at informing users? Can improvements in PI design lead to better user understanding and detection of resource access?

The project involves a two-phase approach: a comprehensive questionnaire survey with 111 mobile users to gauge perspectives on current PI implementations and a practical user study involving 20 Android and iOS users. This study uses four simulated 'naive' note-taking apps to observe how users interact with and perceive PIs in real-time scenarios. The research also explores potential enhancements in PI design, such as non-visual indicators and expanded categories like location and storage access, as well as implementing additional vectors to PIs. Key contributions of this study include identifying the shortcomings of current PI implementations and proposing innovative improvement solutions. Preliminary findings suggest that existing PIs are often overlooked or misunderstood, leading to a need for more user awareness about resource usage. In contrast, the proposed PI design improvements show promise in significantly enhancing user understanding and awareness. These insights could play a pivotal role in shaping future Android privacy features, making this study a valuable addition to the field of mobile user privacy and security.

The paper is divided into several sections. In Section 3, we discuss the background of Android and Privacy Indicators. In Section 4, we review relevant work in this field. Section 5 outlines the study design, while Section 6 presents our results. Our findings, and how our study differs from prior works are discussed in Section 7. Finally, in Section 8, we address some of the limitations of our research and future work that can be done in this field.

3 Background

Android is the most popular operating system globally, with over 2.3 billion Android users worldwide. These devices rely on millions of applications to function. Google Play Store, Android's most popular application store alone, has over 2.6 million applications available to users for download [2]. While most of these applications are benign and attempt to assist users in accomplishing specific goals and tasks, malicious applications also exist. These could steal user data without users' knowledge and contain hidden functionality that could use up device resources, harming the users without their knowledge.

The Google Play Store utilizes a 'Google Play Protect' system to audit and review published applications for user safety. However, due to Android's open and flexible nature, malicious apps can still get through. Android 3.0 introduced a permissions system granting applications access to primary internal storage to address these concerns. However, Felt et al. [6] found in 2012 that only 17% of users paid attention to permission warnings during installation, while 42% needed to be made aware. They suggested several Android privacy and usability improvements so users could make more informed decisions. Despite Google Play Protect and the permissions system, exploitation remains possible on Android, indicating a need for further privacy protections like enhanced indicators.

In 2013, Android 4.4 was released, which required apps to declare the resources they intended to use and request permissions for those resources during installation. This was referred to as the Ask on Install (AOI) model. Although this significantly improved the privacy and security of Android, a major underlying issue with this system was that the only alternative to not accepting the permission request was not installing the application. There was a need for a more granular privacy management system that would allow users finer control over what resources an application could access. This resulted in the Ask on First Use (AOFU) system introduced in Android 6.0, which significantly improved compared to AOI. Users were prompted for permission only the first time the application tried to access the data, allowing them to deny permissions

while still having the application. Subsequent iterations focused on increasing contextualization by delaying the decision until the application used the resources and added more categories to the permissions requested [3, 7].

While this system remedied the issue of access control, there was still a need for a system that could let users know which app could access their system resources, such as the camera, microphone, or location data. Android 12.0 addressed this issue by introducing Privacy Indicators (PI). These tiny icons or notifications could passively show the resources utilized and provide a dashboard to increase user privacy awareness. Subsequent versions, like Android 13.0 and 14.0, have improved usability and privacy by adding additional options to users when granting access, expanding the scope of privacy indicators, and allowing users to control which resources share how much data with the applications requesting them. Although these new additions have significantly reduced the improper utilization of resources and malicious applications exploiting device sensors and data, Android malware continues to increase [9]. Malware is designed to use new tactics and bypass any security features Android developers implement. One of the most effective ways to implement security features against these is to inform users better, ensuring they make informed decisions and can identify malicious applications and when their security and privacy are being exploited.

4 Related Work

Several papers have explored the role of privacy in smartphones; while PI is a new addition to the devices, the permission model has seen several iterations of changes and improvements and thorough research has been conducted on them and users' comprehension of them.

4.1 User Awareness and Understanding of Permissions

A foundational study by Felt et al. [6] uncovered a significant gap in user understanding of app permissions, underscoring the urgent need for more explicit permission prompts and enhanced user education. Their research found that users frequently grant permissions without fully understanding the potential consequences. This highlights the need to shift from obtaining user consent to ensuring their informed comprehension of these permissions.

Nourah et al. [1] investigated the discrepancies between user awareness and actual practices regarding smartphone permissions. Their findings revealed that many users need help managing privacy settings across different platforms. This often leads to overlooking key privacy regulations or misinterpreting the implications of granting specific permissions to apps. The study underscored the necessity for straightforward and effective communication tools and a comprehensive approach to educating users about smartphone privacy to bridge this knowledge gap.

Tahaie et al. [13] approached the privacy issue differently by providing insights into developers' perspectives on privacy issues in smartphone apps. The study revealed that most developers recognize specific permissions, such as access to calendars and locations, as significant privacy concerns, mainly when apps operate in the background. While developers acknowledge the importance of implementing robust security measures like multi-factor authentication and limiting data collection to protect user privacy, there is a perception that consumers are often indifferent about permissions as long as the App functions as intended.

Bal et al. [4] researched methods of improving communication regarding privacy risks. They designed a novel 'Styx' system to provide users with more intuitive and meaningful privacy information about their applications. This system's approach centered on monitoring long-term data access behavior, thereby aiding

users in comprehending the broader implications of resource access by applications. The goal of Styx was to move beyond just identifying individual data access events and to consider the cumulative impact of such access over time.

4.2 Privacy Indicators and Notifications

Stover et al. [12] experimented with an innovative approach to privacy indicators by representing the monetary value of the data collected as a potential indicator. The hypothesis was that users might be more conscious and careful in their choices if they understood the financial value of their data. However, their study encountered challenges in effectively communicating this monetary value to users, suggesting that these indicators need further refinement and development to enhance user comprehension and decision-making.

Sven et al. [5] focused on the impact of displaying application privacy levels in app stores and how these levels influence user decision-making. Their study highlighted the significant role these privacy levels play in guiding users through the app selection process, emphasizing the crucial role of such privacy indicators in mitigating the risks associated with data collection, processing, and transmission by apps. The research demonstrated that well-designed privacy levels could effectively assist users in assessing the trustworthiness of applications.

Addressing the timing and design of privacy notifications, Veljko Pejović and Mirco Musolesi [11] argued that interruptions on mobile devices are not always effective in conveying information to users. To tackle this issue, they proposed a context-sensing solution, utilizing machine learning algorithms to determine the most opportune moments for delivering such notifications. This approach is particularly relevant for Privacy Indicators (PI), suggesting that notifying users at the right moments could significantly enhance their awareness and understanding of privacy issues.

Hazim [8] researched privacy visualizations by investigating F-Droid's use of 'anti-feature' labels to shed light on the challenges of making privacy practices understandable to regular users. By proposing a two-layer model combining simple icons with descriptive labels, this research suggested a more effective way to communicate privacy-related information, ensuring that users are better informed about when and how applications access device resources.

A recent and pivotal addition to this body of research is the study by Guerra et al. [7] in 2023. They found that privacy indicators have limited effectiveness when informing users about resource access, especially for latent resource access. They proposed an enhanced design called 'POP-UP' that significantly improved user awareness and resource usage by increasing the visibility of privacy indicators. Privacy indicators were expanded into notifications informing which apps were using which resources, which lasted for five seconds. Their research identified critical aspects of privacy and permissions, but this research only evaluated two resources containing privacy indicators: camera and microphone. Although this approach marked a crucial step in enhancing privacy and permissions awareness, it also presented limitations, such as its potentially obtrusive nature and the transient visibility of notifications.

5 Study Design

As part of our research, we aimed to assess the effectiveness of PI on Android devices. Our objective was to determine whether these indicators can assist users in identifying when an application is utilizing system resources while preoccupied with other tasks. Furthermore, we sought insights into how users perceive different proposed solutions to enhance privacy indicators.

5.1 Research Questions

Our research was designed to answer the following four research questions:

1. *RQ1:* How effective is the current implementation of PI on Android?
2. *RQ2:* What are the shortcomings of the current implementation of PI on Android?
3. *RQ3:* What changes can be made to PI on Android?
4. *RQ4:* How effective are these proposed changes in improving the effectiveness of PI on Android?

To answer our questions, we conducted a user study and a survey. The user study consisted of tasks that helped us to understand how effective PI is and an interview with mock-up designs to understand the potential solutions and their viability. The survey collected quantitative data about user behavior and PI to understand how users perceive PI's effectiveness. It also included open-ended questions for feedback on the issues and potential solutions to improve PI. The following two sections provide a detailed description of both the user study and the survey.

5.2 User Study

We conducted a formative study on the effectiveness of PI in Androids. Our study was split into two parts:

5.2.1 Tasks

The first part of our study comprised of a set of simulated tasks. We tested four note-taking applications that were designed to function similarly with minor differences in their user interface. We used PI in varying degrees in each application as the variable study factor. Here is a brief explanation of the tasks and applications used in the study:

- **Astrovane:** This application used resources and displayed PI like a traditional one. The corresponding task required participants to open the application from the home screen, record a new note with the phrase 'This is the content for Task#', save the note, and return to the home screen.
- **Quasaris:** This application used the microphone every time it was open in the foreground, displaying PI whenever the app was actively being used. The corresponding task required participants to open the application from the home screen, write a new note with the phrase 'This is the content for Task#', save the note, and return to the home screen.
- **Nebulight:** This application used the microphone as soon as it was opened and continued using it even in the background, continuously displaying PI even if the participant returned to the home screen. The corresponding task required participants to open the application from the home screen, write a new note with the phrase 'This is the content for Task#', save the note, and return to the home screen.
- **Stellarix:** This application was similar in functionality to Astrovane, and its corresponding task required participants to open the application from the home screen, write a new note with the phrase 'This is the content for Task#', save the note, and return to the home screen. This task did not display its PI and was solely intended to test if participants could identify PI use in the previous application.

The study was conducted within subjects, meaning each participant was asked to perform a task on each application in a randomized order to avoid bias, except Stellarix, which always succeeded Nebulight. Participants were not informed about the true nature of the study before completing their tasks. Before starting the tasks, the participants were introduced to Android devices and instructed to observe and remember any interactions between the applications, the device, and any notifications or indicators that might appear during their tasks. After completing their tasks, the participants were asked about their perceived differences in each application and whether they believed any of the applications used the device microphone. Additionally, they were asked to provide feedback on whether they felt PI effectively conveyed when an application uses device resources. After getting their responses, the true nature of the study was explained to the participants, and feedback was collected on how they felt about the effectiveness of PI. Additional details about the user study can be found in Section 9.1

5.2.2 Mock up Interview

To address some of the changes that can be made to PI on Android, we designed three concept mockups, each with a different rationale. These mockups were designed to address some of the significant issues that we believed existed in the current implementation of PI.

Here is a breakdown of the mockups and their purposes:

1. **Mockup 1 - Alternative Privacy Indicators:** This mockup suggests using different indicators, such as vibration or haptics, to improve the effectiveness and user-friendliness of privacy indicators.

2. **Mockup 2 - Additional Privacy Indicators:** This mockup proposes adding new resources or tools to the existing privacy indicators framework, expanding its capabilities. For instance, PI can be used for location services and internal storage access.

3. **Mockup 3 - Additional Vectors in Privacy Indicators:** This mockup suggests expanding the functionality of privacy indicators by including additional vectors. This change adds new dimensions to the current PI system on Android. For example, a risk/trust score in PI for apps or resources could be added.

Additional details about the user study can be found in Section 9.2

The participants were shown each mockup design and were given a detailed explanation of how these proposed mockups would function. They were then asked to share their opinions on each of the designs. The purpose of this study was to gain a better understanding of how users interact with their devices and to identify shortcomings that a solution to PI would have to address. For each design, the participants had to rank them on the System Usability Scale (SUS) to evaluate how usable they speculate a solution might be.

5.3 Survey

Besides the user study, we also developed a self-reported online survey to gather quantitative data about PI on Android. Our survey was about 12 questions long and collected information on the following metrics:

1. **User Experience:** The average years the participants have used their smartphones and their familiarity with Android.

2. **Privacy Concerns:** The average concern about privacy amongst users and the percentage of users in our study with a technological background (and how much this would influence privacy).

3. **Awareness of PI:** The percentage of users aware of PI's existence and their frequency of noticing the PI on their smartphones.
4. **Effectiveness of PI:** The percentage of users who feel that PI helps them understand resource usage and the percentage of users who changed their permission settings based on PI.
5. **Desired Changes:** Lastly, we presented the users with an open-ended question asking if they had any ideas to improve PI on Android.

The complete list of survey questions can be found in 9.3

6 Study Results

We had the following hypotheses going into our research:

1. *H1:* The current implementation of PI is ineffective at informing users when their device resources are being accessed by an application.
2. *H2:* The current implementation lacks contextual information necessary to inform users which apps are accessing the resource. Many users are not aware of PIs on their devices, or the PI fails to grab their attention while they are preoccupied with other tasks.
3. *H3:* Some changes that can be made to PI include changing the way PI is presented (alternate PI), expanding the resources within existing PI (additional PI), and expanding the functionality of PI (additional vectors in PI).
4. *H4:* The implementation of proposed changes to PI would improve the effectiveness in informing users about resource access by applications.

The following sections describe the findings of the user study and the survey.

6.1 User Study Results

6.1.1 Demographics

Our user study was performed with 20 participants, of whom 15 were Android users, and 5 were iOS users. The majority of Android users ensured that we received the most feedback from the perspective of Android users. However, considering that the PI should work for both accustomed and new users to be practical and usable, we also decided to include a few iOS users to obtain their insights. Our study was conducted in our university graduate lab, so most participants were university students with technical backgrounds.

6.1.2 Effectiveness of the Current Implementation of PI

During the Tasks phase of the study, the users were randomly presented with the four applications to interact with and later questioned about resource usage. Table 1 presents the observations from the tasks in our user study. None of the participants were able to correctly identify all resource usage. Additionally, only fifteen participants recognized resource usage with the application that actively required the users to access the resource(Astrovane). Lastly, five participants failed to recognize any resource usage at all. Five participants said that during the study, they observed the PI light at least once, and six participants believed that PI was effective before the true functionality of the applications were revealed.

Observations	Participants (N=20)
Resource Usage	
All resources identified	0
Some resources identified	15
No resources identified	5
Privacy Indicator	
Observed PI during tasks	5
Believed PI were effective	6

Table 1: User Study Task Results

6.1.3 Mockup Solutions of PI

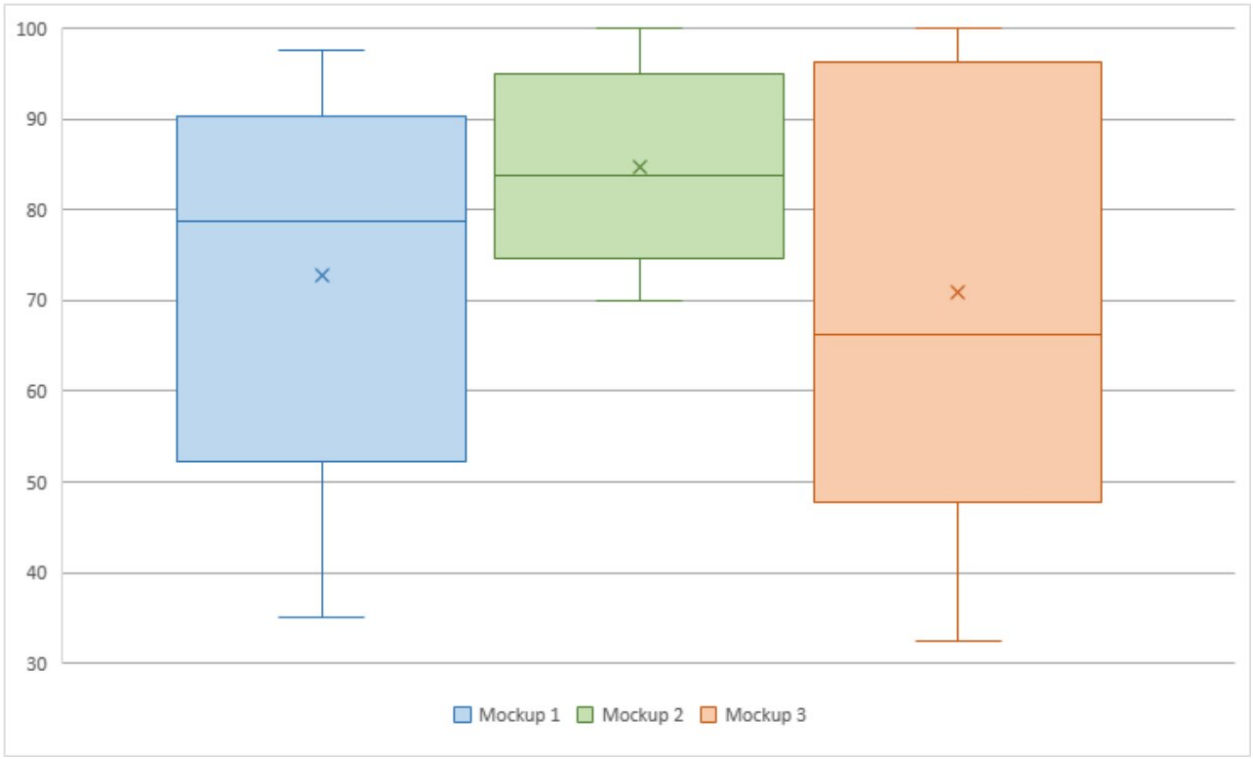

Figure 1: SUS scores for Mockups

SUS scores were identified for each of the proposed mockups to perceive the usability of the different designs. Figure 1 shows all three mockups' SUS scores. The following observations were made:

1. **Highest SUS Score(Mockup 2: 85.25):** Mockup 2 involving additional PIs received the highest SUS score. This suggests that participants likely found the additional privacy indicators related to location and storage valuable and potentially more effective in conveying information about resource usage.

2. **Lower SUS Scores(Mockup 1: 74.875 and Mockup 3: 73):** Both Mockup 1(Alternative Privacy Indicators) and Mockup 3(Additional Vectors in Privacy Indicators) received lower SUS scores compared to Mockup 2. This suggests that while these mockups might have their merits, they must be implemented in ways that do not compromise usability or user satisfaction.

We also received qualitative feedback on the suggested mockups, and the following are some of the issues and concerns we identified:

1. **Mockup 1 - Alternative Privacy Indicators:** Five participants found alternative indicators like vibrations/chimes annoying or distracting. Several users expressed the need for customization in identifying resource use. Three participants doubted the improvement in usability or noticeability with these additions. Some noted that keeping their phone on mute or low volume could diminish the effectiveness of these indicators. Lastly, they expressed the need for customization in identifying resource use.

2. **Mockup 2 - Additional Privacy Indicators:** Four participants deemed incorporating more prominent location privacy indicators helpful. Internal storage use indicators were considered potentially redundant, though helpful if they could highlight suspicious file access. Some participants were concerned about the possibility of overcrowding and overstimulation with additional indicators.

3. **Mockup 3 - Additional Vectors in Privacy Indicators:** Five participants felt that adding more vectors could confuse users and having vectors. Several noted the complexity and potential technicality of these indicators.

The SUS scores align with the feedback received, suggesting that additional privacy indicators(Mockup 2) related to location and storage were more positively received and deemed more beneficial as compared with the potential annoyance and complexity of alternative indicators(Mockup 1) and the added vectors(Mockup 3).

The participants were also asked for other solutions and suggestions to improve the effectiveness and usability of privacy indicators. Most participants suggested enhancing the noticeability by using pop-ups, highlighting the notification bar, or changing the LED colors. They also suggested associating PI LED colors with resources or applications.

6.2 Survey Results

6.2.1 Demographics

Table 2 shows the demographic distribution of our survey. One hundred eleven participants took our survey. Most participants were 18-24(39.6%), followed by equal distribution in 25-34, 35-44, and 45 or older categories(19%-20%). Most participants held a Master's Degree(38.7%), followed by those with a Bachelor's Degree(35.1%), Doctoral Degree(17.1%), and High School education(9%). Most participants did not have a technical background(53.2%) but a considerable amount of smartphone experience(83.8%).

Figure 2 shows the distribution of participant familiarity with Android smartphones. We can observe that participants were quite familiar with Android smartphones, with an average rating of 4.14 out of 5. Figure 3 shows the distribution of participants that used Android. Most participants had an Android(61.3%), and very few had never used an Android(4.5%). Lastly, most of the population participating in our survey had used an Android smartphone after privacy indicators were publicly released in October 2021(80.2%).

6.2.2 Privacy Concern and Awareness of PI

Figure 4 shows the participants' smartphone privacy concerns. On average, participants rated their concern about privacy at 4.08 out of 5, indicating a high level of concern. PI's average rating of noticeability was

Demographic	Distribution
Age	
18-24	39.6%
25-34	20.7%
35-44	19.8%
45 or older	19.8%
Education Level	
High School	9.0%
Bachelor's Degree	35.1%
Master's Degree	38.7%
Doctoral Degree	17.1%
Technical Background	
Yes	46.8%
No	53.2%
Smartphone Experience	
More than 6 years	83.8%
5-6 years	9.9%
3-4 years	4.5%
1-2 years	0.9%
Less than 1 year	0.9%

Table 2: Participant Demographics

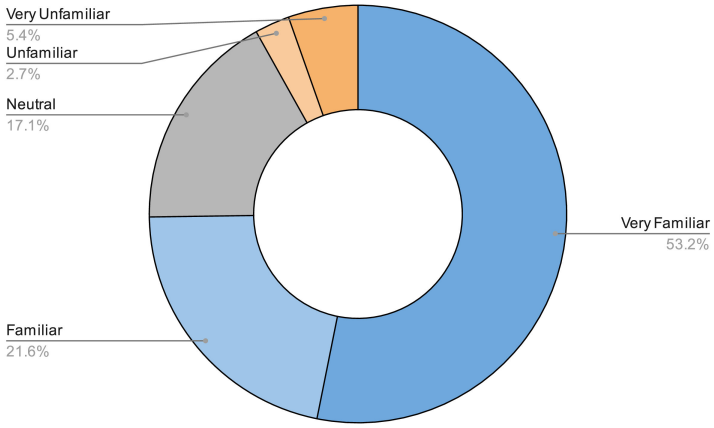

Figure 2: User Familiarity with Android

3.26, suggesting that while some users notice these indicators, there is room for improvement. Additionally, most participants were previously aware of PI(68.5%).

6.2.3 Perceived Effectiveness of PI

Figure 5 shows the participants' perceived awareness, effectiveness, and desire for PI changes. Participants rated their effectiveness in understanding when sensitive resources are accessed through PI at 3.80 out of 5. Additionally, participants rated the impact of PI on permission settings at 3.31, suggesting that PI has somewhat influenced users to change app permissions. However, participants rated the information adequacy of current privacy indicators at 2.96 out of 5, suggesting that current indicators do not provide sufficient information about data usage. A high average of 4.15 indicated a strong desire for more detailed

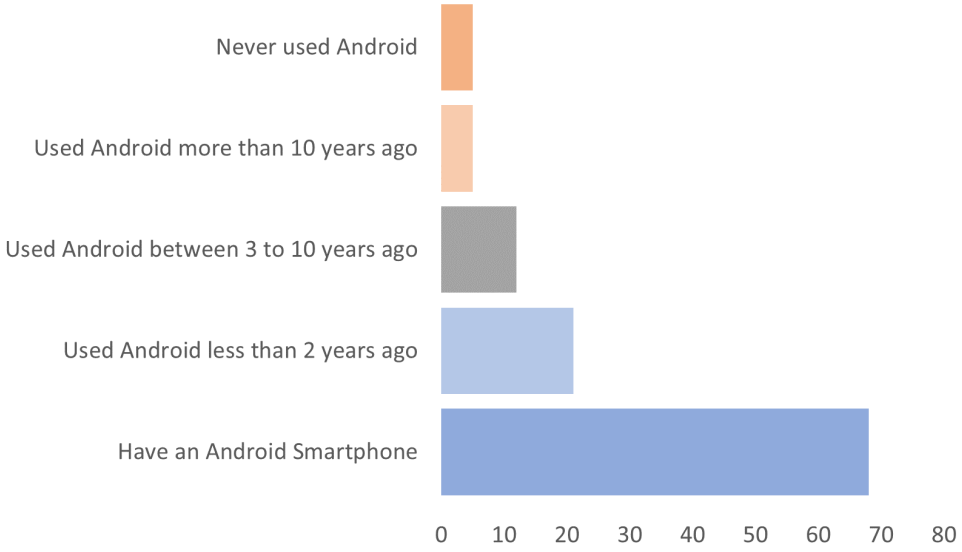

Figure 3: Android Usage

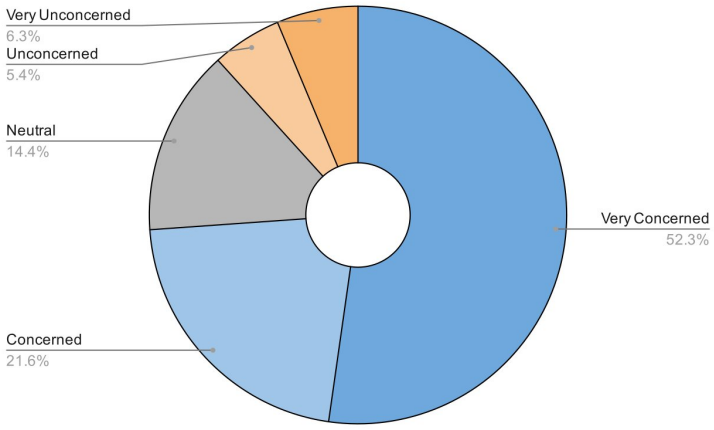

Figure 4: Smartphone Privacy Concerns

or customizable privacy indicators.

6.2.4 Proposed Solutions of PI

Through the open-ended response question asking for any improvements for PI, the participants suggested the following modifications to PI:

1. **Warning for every Privacy Compromise:** Participants desired timely warnings whenever privacy was potentially compromised by an application.
2. **Duration of Notification:** The duration for which the indicator was displayed was a concern; suggestions include extending the duration for better noticeability.

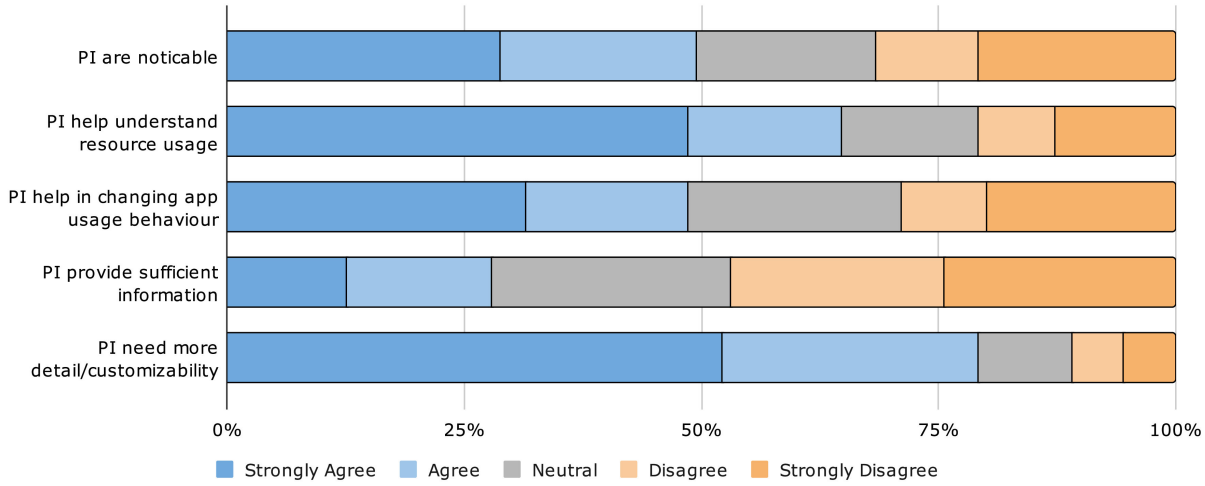

Figure 5: PI Analysis

3. **App-Specific Permission Requests:** Several participants wanted apps to request permission for data tracking each time it was needed.

4. **User-Friendly Language:** Simplifying technical language used in privacy settings was requested for better understanding.

5. **Clear Pre-Use Messages:** Users prefer clear messages displayed before using the app, particularly regarding privacy.

7 Discussion

7.1 Findings

7.1.1 Literature Review

Previous research has identified several areas that require further investigation and has suggested ways to enhance their effectiveness. The suggested improvements are four-fold. Firstly, there is a need to educate users about permissions and privacy risks so they can better understand the consequences of their choices and the risks associated with data sharing. Secondly, creating a more user-friendly and transparent privacy interface is vital. This would make privacy settings more accessible and understandable to all users, leading to informed decision-making. Thirdly, the timing and context of privacy notifications should be carefully considered to ensure they are as effective as possible. Proper timing and relevant context can significantly influence how users perceive and respond to these notifications. Lastly, it is essential to consider both user and developer perspectives when developing privacy communication tools. This approach ensures that the tools created are technically sound and meet user expectations and needs, leading to a more secure and trustworthy digital environment.

7.1.2 User Study

Based on the findings from the user study, several important aspects regarding privacy indicators on Android were as follows:

1. **Low Awareness and Identification:** Given that none of the participants could correctly identify all resource usage, some did not notice any, suggesting a general low awareness or visibility of PI. This implies that PI's current implementation may not effectively capture user attention or be too subtle to be noticed during regular app usage.

2. **Need for Customization and User Control:** Several participants desired customization in PI and a more user-centric design. This suggests that users want to control how they are alerted about resource usage, preferring methods aligned with their usage patterns and preferences.

3. **Effectiveness vs. Intrusiveness:** The feedback that alternative indicators could be annoying or overstimulating points to a delicate balance between effectiveness and intrusiveness. Users seek PIs that are noticeable without being disruptive to the Android usage experience.

4. **Complexity vs. Simplicity:** Concerns about the complexity of additional vectors in PI(Mockup 3) indicate a preference for simplicity. Users may find overly technical or detailed indicators confusing, preferring straightforward and easy-to-understand alerts.

5. **Overreliance on Permission Models:** The heavy reliance on permission models for privacy indicates a potential lack of understanding or trust in other privacy measures. Users may not fully grasp the role of PI or see them as secondary to permissions.

6. **Improvements:** Suggestions for enhanced noticeability (e.g., pop-ups, color changes) reveal opportunities for design improvements. There is a clear demand for more intuitive, noticeable, and informative PI.

7.1.3 Survey

Based on the findings from the self-reported survey, users claim to have a significant awareness and concern about privacy among users, especially among younger and highly educated demographics. While PI on Android is noticed and has some impact, there is a clear need for detail, customization, and usability enhancements. Participants were seeking more proactive and transparent measures from apps regarding privacy, indicating a gap in the current implementation.

7.1.4 Comprehensive Analysis

Based on both the user study, surveys, and our literature review, we establish the following key findings:

1. **User Awareness and Preferences:** Both the survey and user study reveal that users are conscious of PI but have diverse preferences and awareness levels. There is a clear interest in more detailed and customizable PI, as indicated by higher SUS scores for mockups with additional PI.

2. **Usability vs Overload:** While users seek more detailed PI, there is also a concern about overstimulation and complexity. It is essential to balance the amount and type of information provided without overwhelming or confusing the user.

3. **Potential for Improvement:** The survey, user study, and literature review collectively suggest a need for improvement in the current PI. Users are looking for more proactive, informative, and customizable features.

7.2 Prior Works

While not a lot, there have been works done to evaluate the effectiveness of PI in Androids [7]. Our study aims to evaluate the effectiveness of PI in unfamiliar applications, which sets it apart from previous research that focused on popular applications. This approach presents a more realistic scenario for attackers who might create applications to exploit user device resources while appearing benign. Our findings will provide insights on how PI can be improved to prevent such instances.

Additionally, in contrast to [7], our study did not require participants to use their own devices. We evaluated the effectiveness of PI when observed through unfamiliar devices. We reasoned that unfamiliar devices could help users assess the effectiveness without any prior assumptions, thereby providing a broader range of results.

8 Limitations and Future Work

8.1 Limitations

Through our research, we worked under certain assumptions and limitations. These are outlined in this section.

1. **Technical Limitations:** We faced certain technical limitations during our study as we were restricted from using the technology available. We had to rely on a single Android device to conduct the user study tasks, and we also had to simulate the study in the Graduate Study lab at our university. Though we obtained results, these may not completely capture the nuances of how users interact with PI in their everyday device usage, which could lead to different results.

2. **iOS vs Android:** We decided to research the Android platform due to its popularity, ease of developing applications, and accessibility. It is worth noting that each platform has a unique mental model that drives user expectations. For instance, IOS consumers expect a higher level of privacy than Android users, even though both populations are concerned about privacy risks [10]. Therefore, conducting the study on iOS devices could lead to different results.

3. **User Study Recruitment:** The majority of our participants in the user study were university students with technical backgrounds. Although we did have some variations, we designed our study to avoid leading users or giving them assumptions to work under and using deception to avoid biasing them towards privacy indicators. However, the results could represent a bias towards the technically inclined. Therefore, the general population might perform worse than our user study results.

4. **Self-Reported Survey:** We conducted our survey using Google Forms, and it did not require users to provide personal information. Although we used participant emails to ensure there were no duplicate responses, the survey was done online in a self-reported way. Therefore, the responses stated by users might not reflect what happens and could be influenced by various factors.

8.2 Future Work

Our research has identified several areas where further investigation could provide valuable insights. These areas include:

1. **iOS PI Effectiveness:** We recommend additional research to compare the effectiveness of privacy indicators on iOS and Android devices. Specifically, we suggest exploring differences in their workings and whether one is more or less effective than the other.

2. **Changes to Study Design:** To better understand how effective privacy indicators are, future research should evaluate their effectiveness in more realistic scenarios. Conducting long-term studies rather than deception studies could also yield valuable insights.

3. **Evaluating Proposed Solutions:** While we received feedback on proposed solutions to privacy indicators on Android devices through mock-ups, additional research could focus on implementing these solutions and directly comparing their effectiveness to that of Android.

References

[1] Nourah Alshomrani, Steven Furnell, and Ying He. "Assessing User Understanding, Perception and Behaviour with Privacy and Permission Settings". In: *HCI for Cybersecurity, Privacy and Trust*. 2023, pp. 557–575. URL: https://link.springer.com/content/pdf/10.1007/978-3-031-35822-7_36.pdf.

[2] *Android – statistics and facts*. Accessed: 2023-10-15. Sept. 2023. URL: https://www.statista.com/topics/876/android/#topicOverview.

[3] *Android Version History*. Accessed: 2023-10-15. Oct. 2023. URL: https://en.wikipedia.org/wiki/Android_version_history.

[4] Gökhan Bal, Kai Rannenberg, and Jason I. Hong. "Styx: Privacy risk communication for the Android smartphone platform based on apps' data-access behavior patterns". In: *Computers & Security* 53 (2015), pp. 187–202. URL: https://api.semanticscholar.org/CorpusID:27726471.

[5] Sven Bock and Nurul Momen. "Nudging the User with Privacy Indicator: A Study on the App Selection Behavior of the User". In: *Association for Computing Machinery*. 2020. URL: https://doi.org/10.1145/3419249.3420111.

[6] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. "Android permissions: User attention, comprehension, and behavior". In: *Symposium on Usable Privacy and Security (SOUPS)*. 2012, pp. 1–14. URL: https://dl.acm.org/doi/pdf/10.1145/2335356.2335360.

[7] Michele Guerra, Simone Scalabrino, Fausto Fasano, and Rocco Oliveto. "An Empirical Study on the Effectiveness of Privacy Indicators". In: *IEEE Transactions on Software Engineering* (2023). URL: https://api.semanticscholar.org/CorpusID:261325581.

[8] Antonios Hazim. "Privacy Visualizations: Introducing an interactive visualization of privacy indicators based on Exodus Privacy to F-Droid". In: *Bachelorarbeit*. 2023. URL: http://dx.doi.org/10.17169/refubium-37861.

[9] Anton Kivva. *IT threat evolution in Q3 2023, Mobile statistics*. Accessed: 2023-10-15. Aug. 2023. URL: https://securelist.com/it-threat-evolution-q2-2023-mobile-statistics/110427/.

[10] Jialiu Lin, Shahriyar Amini, Jason I Hong, Norman Sadeh, Janne Lindqvist, and Joy 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.

[11] Veljko Pejović and Mirco Musolesi. "InterruptMe: designing intelligent prompting mechanisms for pervasive applications". In: *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. 2014. URL: https://api.semanticscholar.org/CorpusID:16951235.

[12] Alina Stöver, Nina Gerber, Sushma Kaushik, Max Mühlhäuser, and Karola Marky. "Investigating simple privacy indicators for supporting users when installing new mobile apps". In: *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*. 2021, pp. 1–7.

[13] Mohammad Tahaei, Ruba Abu-Salma, and Awais Rashid. "Stuck in the Permissions With You: Developer & End-User Perspectives on App Permissions & Their Privacy Ramifications". In: *ACM Conference on Human Factors in Computing Systems*. 2023, pp. 1–24. URL: https://api.semanticscholar.org/CorpusID:255942018.

9 Appendix

9.1 User Study Task Details

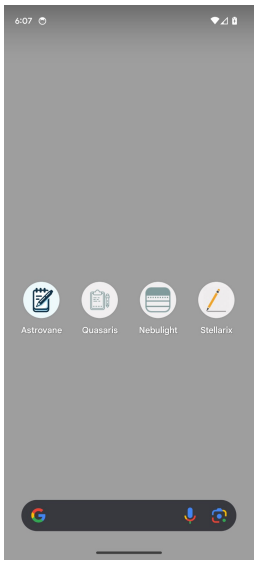

Figure 6: Home Screen of Device

We developed four notetaking applications using Android Studio for Android 14 in order to test the effectiveness of privacy indicators (PI). All four applications were written in Kotlin and their source code can be found on Github (https://github.com/ms1450/NoteTaker). The users were provided with a list of tasks they had to perform, the order of each task, as well as the device with the applications installed as seen in Figure 6.

The following are the details of each of the four applications as shown in Figure 7:

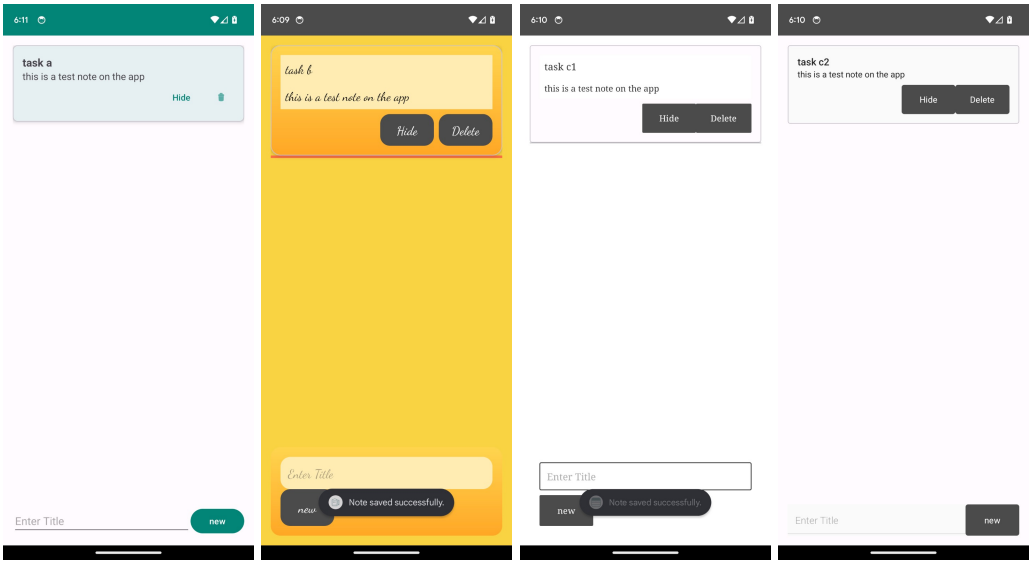

Figure 7: Notetaking Applications (Astrovane, Quasaris, Nebulight, Stellarix)

1. **Astrovane:** This application displayed the privacy indicators properly when accessing the microphone. It was designed to be a benign application that a user might normally interact with in their day-to-day life. The task associated with this application involved the user creating a new note and recording a short audio clip. The objective was to have the user interact with the microphone of the device and observe the correct functioning of PI on Android.

2. **Quasaris:** This application displayed the privacy indicators even when it was in the foreground, even if the user did not select the 'Record' interaction. It was designed as a somewhat malicious application that accessed the microphone without the user's direct consent, but only when the user was interacting with the application. The task associated with this application involved the user creating a new note and writing a short text note. The objective was to have the user interact with the application, but not the microphone of the device, and observe if PI was effective at communicating its usage.

3. **Nebulight:** This application displayed the privacy indicators as soon as it was opened, even if subsequently placed in the background. It was designed as a malicious application that accessed the microphone without the user's direct consent and continued to access it until it was closed. The task associated with this application involved the user creating a new note and writing a short text note. The objective was to have the user interact with the application, but not the microphone of the device, and observe if PI was effective at communicating its usage.

4. **Stellarix:** This application displayed the privacy indicators properly when accessing the microphone. It was designed to be a benign application that a user might normally interact with in their day-to-day life. The task associated with this application involved the user creating a new note and writing a short text note. The objective was to have the user interact with the application, but not the microphone of the device, and observe if PI was effective at communicating its usage.

Each application had minor user-interface and color changes to make them noticeably different from each other, however the core functionality was kept identical. The order of the tasks and applications was randomized for each participant. However, we designed it so that the Nebulight application was always

followed directly by the Stellarix application. We did this to determine if users were able to identify the PI staying on throughout the task of Nebulight, as well as that of Stellarix, and associate it with the correct application causing the indicator to light up.

9.2 User Study Mockups

We presented users with three distinct mockups that propose to improve the effectiveness of privacy indicators in Androids. A detailed description of these mockups is presented below.

9.2.1 Mockup 1 - Alternative Privacy Indicators

This mockup suggests that besides the visual LED in Androids, PI could implement non-visual cues as a way to increase user awareness and effectivenss. This could be in the form of a vibration or haptics. Alternatively this could be implemented through sounds, via chimes or a recognizable notification sound. The idea was to present the user with alternative approaches such that they could reinforce the LED.

9.2.2 Mockup 2 - Additional Privacy Indicators

This mockup suggested implementing the use of PI to more than just camera and microphone access. As an example, PI could be implemented to location services, notifying users every time an application made use of the device's GPS or location information. Additionally, another PI could be implemented for internal storage access, notifying users every time an application makes use of the device's sensitive data.

9.2.3 Mockup 3 - Additional Vectors in Privacy Indicators

This mockup suggested that instead of a binary on/off privacy indicator, if a risk/trust score or additional vectors could be associated with PI improving its effectiveness. This would be governed by an authority that would rate each application based on its resource usage, and if the resource usage was justified, it would represent that via a green LED PI. If the usage was unjustified, the device would represent it via a bright red LED PI. Lastly, if the authority was unsure about the usage, a yellow or orange LED PI would appear instead.

9.3 Survey Questions

9.3.1 About User Behavior

1. What is your age?
    A. Under 18
    B. 18-24
    C. 25-34
    D. 35-44
    E. 45 or older
2. What is the highest level of education you have completed?
    A. Middle School

B. High School

C. Bachelor's Degree

D. Master's Degree

E. Doctoral Degree

3. Do you have a background in computer science or technology?

   A. Yes

   B. No

4. For how many years have you been using a smartphone?

   A. Less than 1 year

   B. 1-2 years

   C. 3-4 years

   D. 5-6 years

   E. More than 6 years

5. How concerned are you about your privacy on your smartphone?

   A. Very concerned

   B. Somewhat concerned

   C. Neither concerned nor unconcerned

   D. Somewhat unconcerned

   E. Very unconcerned

6. How familiar are you with using an Android smartphone?

   A. Very familiar

   B. Somewhat familiar

   C. Neither familiar nor unfamiliar

   D. Somewhat unfamiliar

   E. Very unfamiliar

7. When was the last time you used an Android smartphone?

   A. I have an Android smartphone

   B. Less than 2 years ago

   C. Between 3 to 10 years ago

   D. More than 10 years ago

   E. I have never used an Android smartphone

9.3.2 About Privacy Indicators

8. Were you previously aware that Android uses privacy indicators like camera, microphone and location icons?
    A. Yes
    B. No
9. You notice the Privacy Indicators when using your Android device.
    A. Agree
    B. Somewhat Agree
    C. Neutral
    D. Somewhat Disagree
    E. Disagree
10. Privacy Indicators help you understand when your camera, microphone or location is being accessed.
    A. Agree
    B. Somewhat Agree
    C. Neutral
    D. Somewhat Disagree
    E. Disagree
11. Privacy Indicators have caused you to change your app permissions or other permission settings.
    A. Agree
    B. Somewhat Agree
    C. Neutral
    D. Somewhat Disagree
    E. Disagree
12. Current Privacy Indicators provide enough information about how your data is used.
    A. Agree
    B. Somewhat Agree
    C. Neutral
    D. Somewhat Disagree
    E. Disagree
13. Current Privacy Indicators need more detail or customizability.
    A. Agree
    B. Somewhat Agree
    C. Neutral
    D. Somewhat Disagree

E. Disagree

14. What are some of the issues you face with privacy indicators, and if you could rework them, what changes would you make to make them more effective? (Long Answer Text Response)