

# Poster: Understanding User Acceptance of Privacy Labels: Barriers and Enhancements

Jingwen Yan<sup>†</sup>, Mohammed Aldeen<sup>†</sup>, Jalil Harris<sup>†</sup>, Kellen Grossenbacher<sup>†</sup>

Aurore Munyaneza<sup>‡</sup>, Song Liao<sup>‡</sup>, Long Cheng<sup>†</sup>

<sup>†</sup>Clemson University, {jingwey, mshujaa, jalilh, kgrosse, lcheng2}@clemson.edu

<sup>‡</sup>Texas Tech University, {amunyane, song.liao}@ttu.edu

**Abstract**—As the number of mobile applications continues to grow, privacy labels (e.g. Apple’s Privacy Labels and Google’s Data Safety Section) emerge as a potential solution to help users understand how apps collect, use and share their data. However, it remains unclear whether these labels actually enhance user understanding to build trust in app developers or influence their download decisions. In this paper, we investigate user perceptions of privacy labels through a comprehensive analysis of online discussions and a structured user study. We first collect and analyze Reddit posts related to privacy labels, and manually analyze the discussions to understand users’ concerns and suggestions. Our analysis reveals that users are skeptical of self-reported privacy labels provided by developers and they struggle to interpret the terminology used in the labels. Users also expressed a desire for clearer explanations about why specific data is collected and emphasized the importance of third-party verification to ensure the accuracy of privacy labels. To complement our Reddit analysis, we conducted a user study with 50 participants recruited via Amazon Mechanical Turk and Qualtrics. The study revealed that 76% of the participants indicated that privacy labels influence their app download decisions and the amount of data practice in the privacy label is the most significant factor.

## I. INTRODUCTION

In 2020, Apple launched its Apple Privacy Label (APL) to help users understand the app’s privacy practices [1]. Following this, in 2022, Google introduced the Data Safety Section (DSS) to show how developers collect, share, and protect user data [2]. However, with the emergence of privacy labels, associated issues have also increased. Therefore, we aim to gain deeper insights into users’ perspectives on privacy labels. In this study, we focus on user perceptions of privacy labels, with our primary research question being: **RQ1:** How do users perceive app privacy labels? **RQ2:** How do negative perceptions shape their trust and app download decisions? **RQ3:** What are users’ expectations for privacy labels?

To answer the above questions, we made the following contributions: 1) We collected 216 posts containing 17,651 comments and identified 583 comments exhibiting negative sentiment towards privacy labels. Then we manually analyzed 93 comments related to privacy labels directly to identify

users’ concerns and suggestions. 2) We conducted a user study with 50 participants to explore their understanding of privacy labels, the aspects of privacy labels that most influence their app download decisions, and expectations for privacy labels.

## II. UNDERSTANDING THE USER PERCEPTION OF PRIVACY LABELS ON REDDIT

### A. Data Collection

In this study, we collected data from Reddit using ICOAR platform [3], specifically targeting discussions related to privacy labels using the keywords “privacy labels” and “privacy nutrition labels.” We collected 216 posts containing 17,651 comments. We first filtered the negative sentiment comments using *VADER-Sentiment* model [4]. Then we manually labeled each of the negative comments to determine whether it directly discussed privacy labels. We ended up with 93 comments that were directly relevant to privacy labels.

### B. Users’ Concerns and Suggestions

Our manual analysis reveals several key concerns that users express regarding privacy labels. First, users frequently mentioned distrust of the self-reporting mechanisms about privacy labels from the developers. One user stated “*Privacy labels don’t necessarily describe what Apple allows an app to do*”. Another concern is users believe that privacy labels are designed to give the appearance of accountability without actually providing meaningful protection for their data. For example, one user stated, “*They have every incentive to pretend to do it but not really make a difference*”. Moreover, users point out inconsistencies and gaps in how privacy labels are implemented across different platforms and regions. Also, users raised concerns about how app updates or changes to terms of service could make privacy labels irrelevant.

On the other hand, some users provided suggestions aimed at enhancing the effectiveness of privacy labels. Many users emphasized the need for clearer and more detailed explanations of the permissions listed in privacy labels. They seek straightforward descriptions that demystify technical jargon (e.g., “*Does anyone know what sensitive information mean?*”). Another predominant suggestion is the implementation of more stringent verification processes for privacy labels, such as third-party assessments. Users also proposed that app developers should be required to provide clear and valid reasons when requesting access to sensitive data.

### III. USER STUDY

To further understand users' attitudes toward privacy labels, we conducted a user study via Amazon Mechanical Turk (MTurk) [5] and Qualtrics [6]. We received 50 valid responses from participants. The user study was approved by our University's Institutional Review Board (IRB).

#### A. Basic understanding towards privacy labels

88% of participants reported having seen privacy labels. We then introduced privacy labels and showed examples of DSS and APL. Next, we asked participants whether they know who provides the privacy labels for apps. Surprisingly, only 30% correctly identified app developers as the providers. Another 34% believed the labels were provided by Google or Apple and 10% thought third-party certification companies were responsible. Finally, we asked do they think the information provided in the privacy labels would influence your decision to download the app. 76% of participants stated it would influence their decision.

#### B. Aspects of Privacy Labels That Most Influence Participants' App Downloads

We focus on 4 aspects based on our Reddit analysis results. The overall results are shown in Figure 1.

**Confusing terms:** We first asked participants whether they found the section names in DSS and APL confusing. The majority of participants (76% for DSS and 78% for APL) reported that the section names were clear. Next, we presented specific terms from the privacy labels and asked participants if they found them confusing. Overall, participants indicated that most terms were clear. Finally, we asked participants whether the clarity or confusion of the privacy label content would affect their decision to download an app. 80% of participants stated that it would influence their decision.

**Amount & types of data practice:** We presented participants with the *Data Linked to You* section of the Apple Privacy Label for Facebook Messenger, which includes nearly 100 data practices, and asked for their first impressions. 26 participants (52%) felt there was too much information, and 29 participants (58%) expressed concern about the amount of data collected. Some participants found the information to be very detailed and comprehensive (48%). 84% of participants stated that the amount of *Data Linked to You* in a privacy label would affect their decision to download an app.

**Honesty & trust:** Next, we asked participants whether they think developers are honest when providing privacy labels. Most participants (74%) believed that most or some developers are honest and 70% of participants stated that a developer's honesty would influence their decision to download an app. From our analysis of Reddit comments, we found that some users mentioned distrust towards developers from certain countries. Therefore, we also asked participants questions regarding countries and trust. The results indicate that over half of the participants (64%) reported trusting or distrusting developers from certain countries.

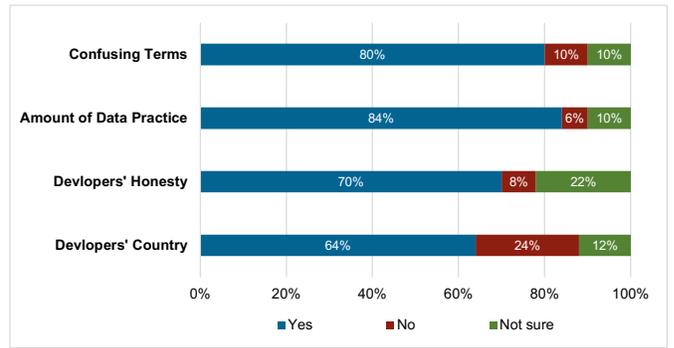


Fig. 1: Aspects of Privacy Labels That Influence Participants' App Downloads

#### C. Participants' Expectations for Privacy Labels

Based on our analysis of Reddit discussions about privacy labels, we observed significant negative comments, and these negative perceptions could indeed impact users' decisions to download apps. To address users' negative feedback, we evaluated their expectations for privacy labels from three perspectives: configurability, adaptability, and kid-friendly design. For configurability, 88% of participants stated they would be willing to use such apps if the privacy label shows that some information is collected but certain permissions can be denied without losing full functionality. For Adaptability, 82% of participants expressed support for region-specific adjustments and 92% of participants stated they want privacy labels to notify them of app update. For kid-friendly design, 16 participants suggested using simple text, 14 participants recommended enhancing visuals with animations and icons, and 3 participants proposed using audio formats.

### IV. CONCLUSION

In this study, we collected and analyzed Reddit posts and comments to understand users' perceptions of privacy labels. Our analysis revealed that users have skepticism about self-reported privacy labels provided by developers and struggle to understand confusing terms in privacy labels. Users expressed a desire for clearer explanations and emphasized the importance of third-party verification. To validate these findings, we conducted a user study and discovered that 76% of participants indicated that privacy labels influence their app download decisions. Among these factors, the amount of data practices disclosed in a privacy label was found to have the most significant impact on users' decisions.

### REFERENCES

- [1] Transparency is the best policy. <https://www.apple.com/privacy/labels/>.
- [2] Provide information for Google Play's Data safety section. <https://support.google.com/googleplay/android-developer/answer/10787469?hl=en>.
- [3] Integrative cyberinfrastructure for online abuse research(icoar). <https://cuseclab.computing.clemson.edu/icoar/>. Accessed: 2024-12-09.
- [4] Anton Borg and Martin Boldt. Using vader sentiment and svm for predicting customer response sentiment. *Expert Systems with Applications*, 162:113746, 2020.
- [5] Amazon Mechanical Turk. <https://www.mturk.com/>.
- [6] Qualtrics. <https://www.qualtrics.com/>.