

# Mobile Application Selection Behavior: Popularity Vs Security

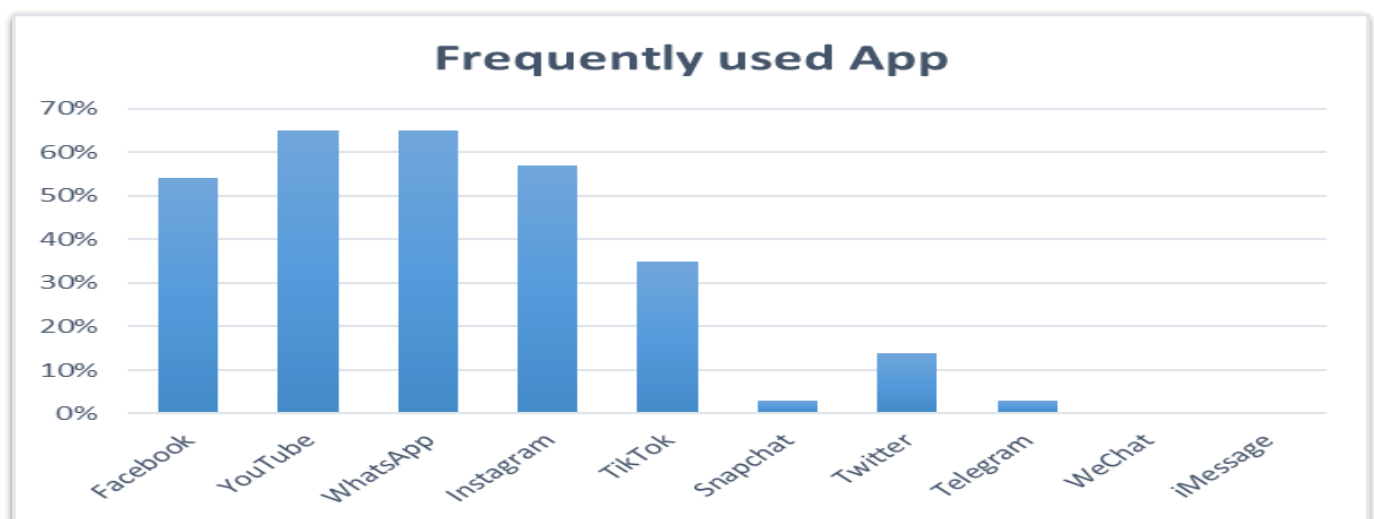
Priyanka Pradhan: Link: [Qualtrics Survey | Qualtrics Experience Management](#)

## Abstract

The study is an analysis of the selection behavior of users while choosing to download a mobile application. It focuses on two main factors: the popularity and security of an application. The motivation to choose is that there have been little to no studies on whether the popularity of an application overpowers the security and privacy features of the application. Research questions explored the usage of social media, widely used mobile applications, awareness of security and privacy, and the factors that affect the user's decision while choosing an application. A survey was conducted to collect data and analyze it based on the research questions. The initial hypothesis was that the majority of participants would prioritize the popularity of an application over its security features, but the results challenged the hypothesis.

## Introduction

Smartphones are arguably one of the most important innovations to come up in recent history, and one of their best features is the ability to use mobile applications. There are multiple factors that influence a user's decision to download an application, of which user reviews, recommendations, security, and privacy features have huge importance. There have been studies on how users choose an application or why users choose a particular application. However, there has been no study focusing on the above-mentioned factors, i.e., the popularity and security of an application, and how they influence the user's decision.



Many popular social media applications like Facebook, TikTok, and Whatsapp have faced problems with data breaches. However, there is a huge user base for these applications, and this raises the question of whether the security and privacy features of such applications impact the user less than the

popularity of the application. So the study analyzes the selection behavior of users while choosing to download a mobile application.

The study encompassed several research questions, of which the major one was about the factors that affect the user's decision while choosing a mobile application. Other questions were about usage, level of awareness about security, and experiences while using other mobile applications. Since the analysis was focused on social media applications, all the research questions were focused on social media applications.

The questions that the study set out to answer were: How often do users use social media applications, and what are the most widely used ones? What are the factors that users think of while choosing an application and the importance of each? How well-informed are users about mobile app security and privacy, and how far are they concerned about overreaching permissions? If users have stopped using an application because of its security and privacy concerns. To collect information and gather data, a survey was conducted. The survey involved asking a series of questions to the participants related to their usage of social media applications, awareness of security and privacy, and previous experiences while using mobile applications. Along with this, the participants were asked to choose an application before and after being given some information regarding the security concerns of the applications.

The survey was designed using web-based software called Qualtrics and distributed using a platform called Prolific. It was distributed to participants all over the world. A total of 37 participants were recruited, with each receiving monetary compensation for their participation. Later, an analysis was conducted on the collected data. The data showed that the majority of the participants used social media a great deal, and Instagram, Youtube, and Whatsapp were the top 3 widely used applications. The factors popularity and security were focused on, and the results showed that the majority of the participants changed the importance of the factors after being provided with information regarding the security concerns about the chosen applications. The importance of security was increased. The results also revealed that the participant's choice of applications was affected by the information about security concerns.

The findings of the analysis challenge the initial hypothesis of the participants giving the popularity of an application more importance than its security and privacy features. This was shown by the change in importance of the factors after providing the participants with security concerns. The findings of this research could be used as a base for future research on other factors and user preferences, as well as by app developers to give equal importance to both popularity and security features.

## **Related Work**

In the context of our research on the interplay between popularity and security considerations in users' choices of mobile applications, several relevant studies have been examined. *Elsantil, Yasmeen*.

(2020). *User Perceptions of the Security of Mobile Applications*. This study provides insights into user perceptions of security, particularly in the context of different types of mobile applications. It sets the stage for understanding the concerns users may have regarding the security of mobile apps, forming a basis for further exploration.

Taylor, David G.; Voelker, Troy A.; Pentina, Iryna. (2011). *Mobile Application Adoption by Young Adults: A Social Network Perspective*. This article emphasizes the impact of social networks on mobile application adoption, supporting our research hypothesis that popularity within one's social network influences app downloads. It broadens the perspective on user behavior by emphasizing the social context of app adoption. It is relevant as it contributes to understanding the dynamics between popularity and security concerns in the decision-making process.

F. Parker, J. Ophoff, J.-P. Van Belle, R. Karia. (2015). *Security awareness and adoption of security controls by smartphone users*. It challenges the common notion of a lack of security awareness among users. This directly relates to the research's focus on the paradox between user concerns and their actions. It emphasizes the need for user-friendly education, aligning with the research's consideration of user perceptions and knowledge acquisition in the context of popularity vs. security.

In summary, these works collectively contribute to the research by providing insights into user perceptions of security, the impact of social networks on app adoption, and the challenges related to security awareness. Understanding these aspects is crucial for the overarching investigation into the interplay between popularity and security considerations in users' choices of mobile applications.

## **Methodology**

Conducting a comprehensive investigation into user perceptions of social media application security, this study employed a survey method facilitated through Qualtrics and hosted on Prolific, a participant recruitment platform. The survey integrated both open-ended and closed-ended questions, with a median completion time of 10 minutes.

Prior to engaging participants in the survey questions, the methodology initiated with a consent form, ensuring voluntary participation. Only upon confirming their agreement were participants directed to the subsequent survey sections. Contextual information about the study was presented to participants, providing a foundation for their responses.

The survey was thoughtfully structured in two distinct phases to comprehensively investigate user perceptions of social media mobile application security and popularity. In the initial phase, participants were presented with two sets of social media applications, each containing two options. Following their selections, detailed follow-up questions were posed to understand decision-making processes. A midpoint segment intervened, probing into participant ranking preferences and their previous experiences with other applications. Transitioning to the second phase, participants received additional information concerning security concerns associated with their chosen applications. This phase aimed

to gauge how newfound security insights influenced their decisions. Revisiting the ranking of factors allowed for a dynamic understanding of participant perspectives. The survey concluded with demographic inquiries, ensuring a holistic understanding of the participant base. Notably, the debriefing process promptly followed, enlightening participants about the fictionalized nature of security concerns presented and providing them with the option to submit their responses or withdraw from the survey. This methodological approach facilitated a nuanced exploration of user decision-making dynamics, shedding light on the intricate relationship between security information and participant choices in the realm of social media mobile applications.

For participant recruitment, a global approach was adopted, opening the survey to individuals worldwide. Prolific served as the platform of choice for recruitment. The participant pool comprised 37 individuals, with a gender distribution of 43% female and 57% male. Educational backgrounds were diverse, ranging from high school to four years or more of a degree. The majority of survey participants fell within the 18-24 age range (49%), followed by the 25-34 age group (27%), with smaller proportions in the 35-44 (11%) and 45-54 (14%) age brackets. The geographic diversity of our participants was notable, with representation from countries such as Poland, Portugal, South Africa, the United Kingdom, Mexico, and others. However, despite this global reach, a significant concentration of respondents emerged in specific regions, notably Portugal (35%), South Africa (13%) etc.

The survey's findings are drawn from a relatively small group of 37 participants, indicating limitations in the generalizability and conclusive nature of the results. The small sample size restricts the broader applicability of our findings and may influence the robustness of our conclusions.

The concentration of respondents in specific geographical regions introduces challenges related to regional bias and imbalance. The disproportionate representation raises questions about the generalizability of our results to a broader global context.

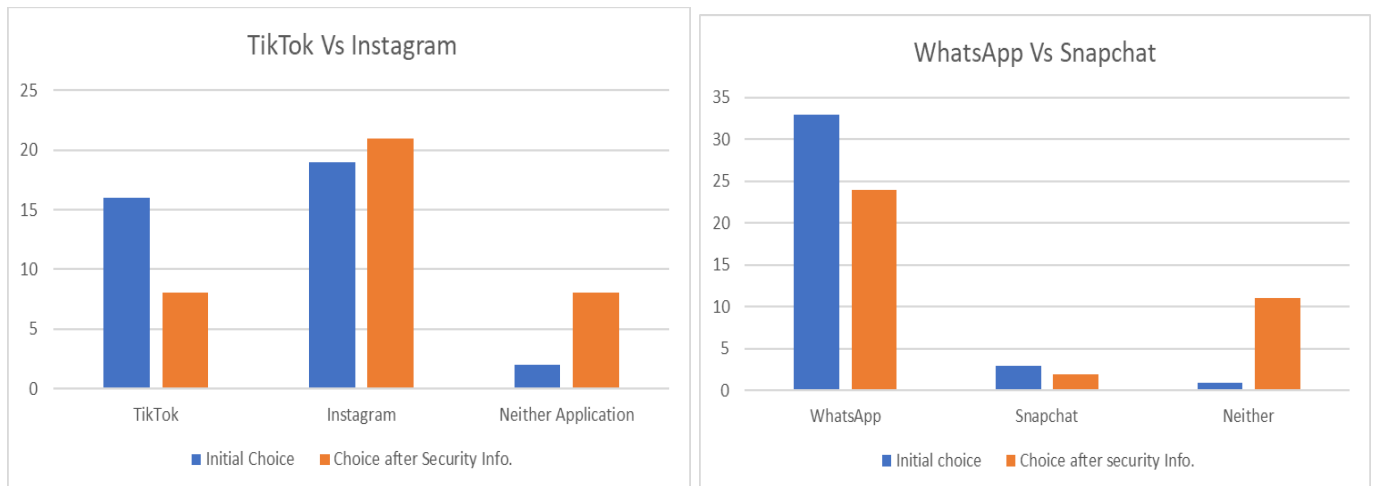
While efforts were made to attain global representation, these limitations underscore the need for caution when interpreting and applying the survey's findings. Future studies with larger, more diverse samples could contribute to a more comprehensive understanding of user perceptions of social media mobile application.

## **Results**

The analysis of results was conducted based on the survey questions aligned with our hypotheses. Utilizing the Qualtrics survey platform, data was extracted, including the information about participants and their choices, as well as responses to open-ended questions. In addition to quantitative assessments, qualitative insights were gathered through the examination of open-ended responses. These open-ended responses provided valuable context, revealing reasons why individuals refrain from downloading or discontinuing using mobile applications, often citing specific mobile application brands as examples. This dual approach allowed for a comprehensive understanding of participant perspectives and enriched the interpretation of quantitative findings.

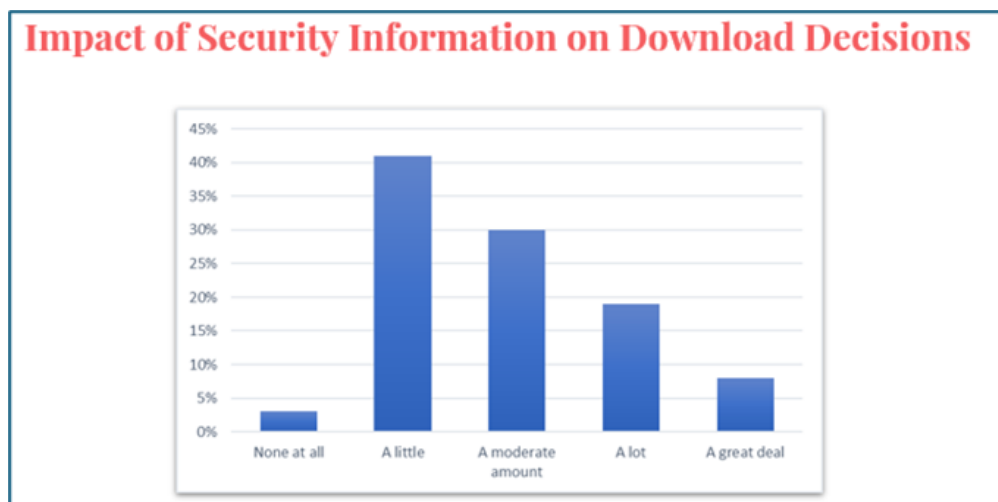
1. Among the 10 popular mobile applications examined which included Facebook, Youtube, WhatsApp, Instagram, Twitter, Snapchat, TikTok, Telegram, Imessage and WeChat. YouTube, WhatsApp, followed by Instagram emerged as the top three preferred apps, while iMessage and WeChat were noted as the least popular choices.
2. In assessing participants' awareness of security and privacy issues, the findings showcased an encouraging trend. A significant majority, approximately 87%, considered themselves to be at least "slightly well-informed." Notably, the absence of any participants claiming to be "not at all informed" suggests a favorable perception of security awareness within the surveyed group.
3. A notable 43% of participants refrained from downloading specific mobile apps, with Temu, Telegram, and TikTok being the most commonly avoided applications. The primary source of awareness regarding these concerns was derived from online sources or through discussions with friends and family. Additionally, 38% of participants discontinued the use of certain mobile applications, including myFitnessPal, Reddit, Temu, and Facebook. Common reasons for discontinuation included the persistent intrusion of targeted ads and instances where apps requested sensitive information like bank details. These findings underscore the significant consideration participants give to security and privacy when engaging with applications.
4. Participants were asked to rank factors influencing their choice of a mobile application both before and after receiving security information. Focusing on two key factors, 'security' and 'popularity,' significant shifts were observed. Regarding security, 40% of participants altered their initial ranking, with 67% increasing the importance of security after being informed about security aspects. Conversely, for the popularity factor, 45% of participants adjusted their ranking, with 59% decreasing its importance. These findings emphasize the dynamic nature of respondent preferences and decision-making processes, shaped by the availability of information.
5. Participants were presented with two sets of applications, Instagram versus TikTok in the first set, and WhatsApp versus Snapchat in the second. Initially, Instagram and WhatsApp were the most chosen applications. Security information exerted a considerable influence on participants' application preferences.

In both sets, 62% and 70% changed their initial choices, with 55% expressing decreased confidence but staying within the same brand. Notably, 24% opted for a different brand, and some remained uncertain. In the WhatsApp versus Snapchat comparison, 70% changed initial choices, with 54% staying within the same brand, 30% choosing neither, and the rest selecting a different brand.



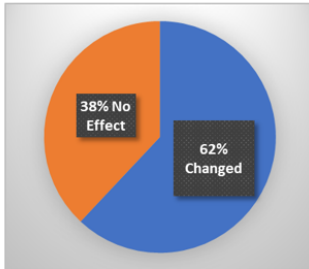
E.g- In the above graph, among the initial Instagram users (19), 13 participants remained with Instagram, 1 switched to TikTok (5%), and 5 opted for neither. In contrast, among the initial TikTok users (16), 7 stayed with TikTok, 8 switched to Instagram (50%), and 1 chose neither, showcasing the dynamic shifts in user preferences following the presentation of security information.

The study revealed a noteworthy impact of security information on participants' application preferences. A substantial majority altered their initial choices in both sets of applications, indicating the significant role of security-related factors in shaping user decisions. While a considerable proportion maintained brand loyalty despite decreased confidence, a noteworthy percentage switched to different brands or chose neither application, emphasizing the crucial influence of security information on user perceptions and choices within the realm of popular applications.



**Instagram : 51% Vs TikTok: 43%**

*After security information was provided*

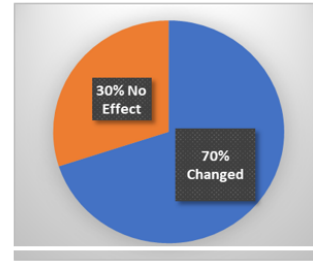


Among those who switched:

- 55% stayed within the same brand.
- 24% switched to different brand.
- 21% chose neither of the Apps.

**WhatsApp: 89% Vs Snapchat: 8%**

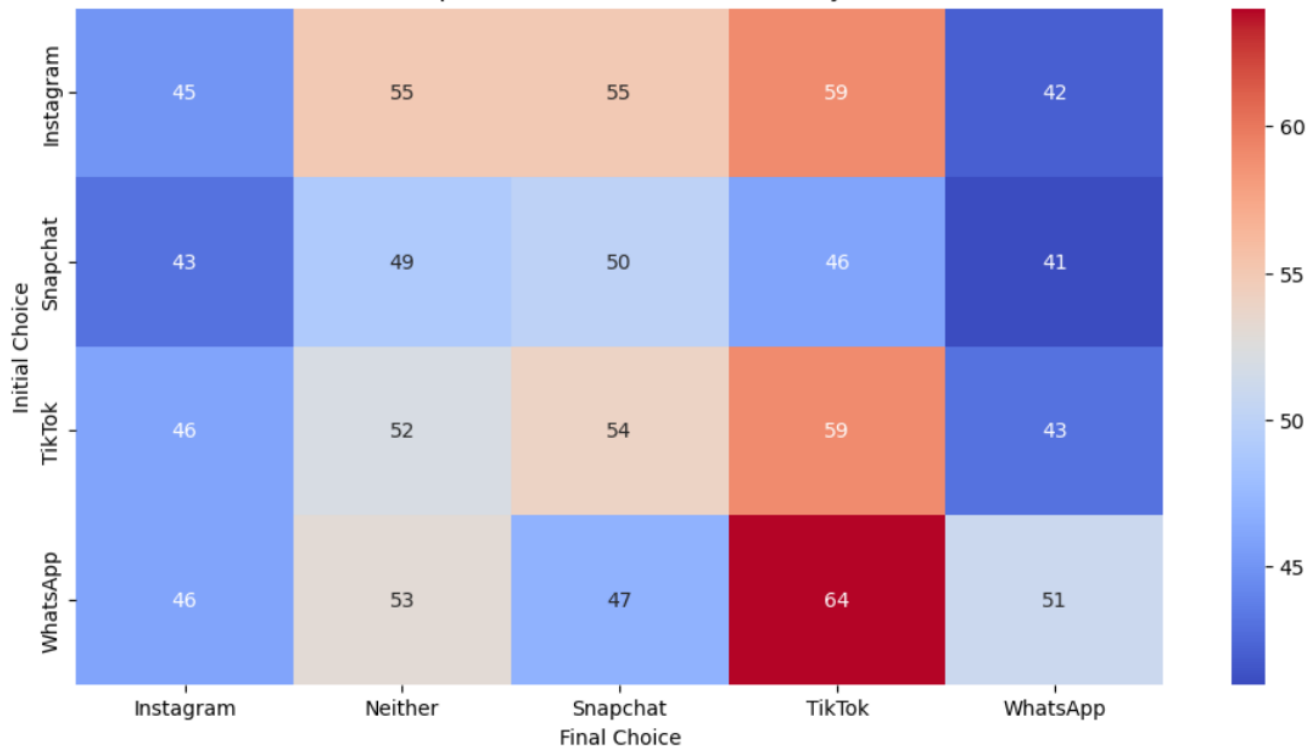
*After security information was provided*



Among those who switched:

- 54% stayed within the same brand.
- 13% switched to different brand.
- 30% chose neither of the Apps.

Preference Comparison Before and After Security Information



```

import pandas as pd
import numpy as np
from scipy import stats

# Total number of participants
total_participants = 100

# Data: Percentage of participants shifting their preferences
# 67% increased the importance of security
# 59% decreased the importance of popularity
increase_security = 0.67
decrease_popularity = 0.59

# Number of participants who changed their preference
changed_security = int(total_participants * increase_security)
changed_popularity = int(total_participants * decrease_popularity)

# Number of participants who did not change their preference
no_change_security = total_participants - changed_security
no_change_popularity = total_participants - changed_popularity

# Observed values
observed_counts = np.array([[changed_security, no_change_security],
                             [changed_popularity, no_change_popularity]])

# Chi-square test
chi2_stat, p_value, dof, ex = stats.chi2_contingency(observed_counts)

print(f"Chi2 Stat: {chi2_stat:.4f}")
print(f"P-value: {p_value:.4f}")

# Interpretation
alpha = 0.05
if p_value < alpha:
    print("Reject the null hypothesis. There is a significant difference in the importance of security vs. popularity.")
else:
    print("Fail to reject the null hypothesis. No significant difference in the importance of security vs. popularity.")

```

Chi2 Stat: 1.0511  
P-value: 0.3053  
Fail to reject the null hypothesis. No significant difference in the importance of security vs. popularity.

## Discussion

This study is centered around the concept of the privacy paradox, a psychological phenomenon coined in 2001. The privacy paradox refers to the discrepancy between users' expressed concerns and their actual behavior regarding privacy in an online environment.

The primary objective of this study is to investigate whether users prioritize privacy over the popularity of the apps they typically use. To achieve this, we conducted a survey to gather insights into people's decision-making processes when selecting an app for use.

Our findings challenge the initial hypothesis and highlight the complexity of user preferences. The fact that a significant portion (30%) of participants prioritize security over popularity contradicts the assumption that people generally prioritize popularity in apps.

Even though 70% of participants chose to stay within the same app after educational interference suggests most users have a strong attachment to certain applications. We still got the subsequent shift



in priority rankings indicates that users are open to reconsidering their preferences. For example, the enhancement in security ranking, possibly as they become more informed about security aspects.

It's crucial to recognize the nuanced nature of user preferences, and our research has provided valuable insights into the diversity of priorities among users. This information can be instrumental in refining app development and marketing strategies to better align with user values.

Now that we have uncovered the nuances of user preferences and decision-making regarding popular mobile applications, our findings shed light on the intricate interplay between privacy concerns, app popularity, and the influence of security information. This exploration contributes to a deeper understanding of the privacy paradox in the digital realm, where expressed concerns often diverge from actual behaviors.

Understanding the factors influencing app choice, particularly the pivotal role of security information, has practical implications. App developers, policymakers, and digital platforms can leverage these insights to enhance user experience by prioritizing security features and transparent communication about privacy. Additionally, businesses can refine marketing strategies based on the identified preferences and concerns of users.

Further exploration into the specific factors that contribute to users' changing priorities could offer deeper insights. Understanding why certain individuals prioritize security over popularity and vice versa could guide the development of features that resonate with different segments of the user base. Investigating how different demographics respond to security disclosures and exploring evolving trends in app preferences over time could provide a more nuanced understanding. Moreover, examining the effectiveness of various strategies to communicate security information to users could guide the development of more user-friendly privacy practices.

We suggest increasing the number of participants to get a better mix for future studies. Having more people with different backgrounds can give us a wider view of how users behave and what they prefer. It's important to actively include people from different places, ages, ethnicities, and economic backgrounds. This mix can reduce biases linked to specific regions and make the results more applicable overall

## **Conclusion**

In conclusion, our findings suggest a dynamic and evolving landscape of user preferences, emphasizing the importance of considering both popularity and security in app design and marketing strategies.

We've observed the influential role of educational intervention and recognized its potential as a formidable tool for individuals in the selection of apps for download or usage.

Our findings suggest that the responsibility lies with the application platform to notify users and offer fundamental educational guidance on app security, should users opt for such assistance. The platform should independently detect all downloaded apps for each user, consistently assess potential risks, and promptly inform users in case of privacy or security violations. Users will receive relevant background information, enabling them to make informed decisions about whether to proceed or not.

Ultimately, our study envisions a future where users, armed with informed choices, navigate the app landscape with confidence, ushering in a new era of privacy-conscious digital experiences.