PROTOCOL TITLE:
Mobile Application Selection Behavior: Popularity vs. Security

PRINCIPAL INVESTIGATOR (PI):
Name: Priyanka Pradhan , Shaohua Lu , Vishnusai Ramesh
Department: Computer Science
Are you a student? Yes☒ No ☐
If Yes, you must designate a Faculty Advisor below.

FACULTY ADVISOR (required for Student PIs):
Name: Dan Votipka
Department: Computer Science

VERSION NUMBER/DATE
V001.20231026

1.0 Purpose of the study:

The purpose of this research is to investigate whether users go by the ‘popularity’ rather than the 'security' of Social media and communication application. We seek to understand whether users' choices are primarily influenced by the widespread popularity of a mobile app rather than concerns about its security features and data privacy.

2.0 Background / Literature Review / Rationale for the study:

Smartphones are arguably one of the most important innovations to come up in recent history. And one of the best features is the ability to use mobile applications. Mobile applications like Facebook, TikTok, Google is practically impossible to avoid from a person’s day-to-day life. When a user lands their hands on a smart phone, they are given a plethora of pre-download applications and given a place like the App Store or Play Store to download other applications according to their wishes. In mobile applications, user’s security and data privacy are major issues that affect many people and organizations.

The numerous incidents of data breaches and privacy violations that have impacted various companies amplify this. Data breaches can happen for different reasons, such as cyberattacks, insider threats, insufficient security practices, or unintentional. When confidential user data is compromised, it can result in identity theft, financial fraud, privacy invasion, and other harmful outcomes for individuals. Google and Apple are among the companies that have faced criticism and legal actions related to data privacy and security. They are often required to meet the highest standards by regulators and the public to ensure they protect user data properly and securely.

3.0 Participant Population:

We plan to recruit individuals on the Prolific platform (https://www.prolific.co/) that are 18+ and living in the United States. We provide more details on Prolific in 9.0.

4.0 Special Populations:

- ☐ Children
- ☐ Fetuses/Neonates
- ☐ Prisoners
- ☐ Members of the military
- ☐ Non-English speakers
- ☐ Those unable to read (illiterate)
- ☐ Employees of the researcher
- ☐ Students of the researcher
- ☐ Adults lacking capacity to consent and/or adults with diminished capacity to consent, including, but not limited to, those with acute medical conditions, psychiatric disorders, neurologic disorders, developmental disorders, and behavioral disorders
- ☐ Disadvantaged in the distribution of social goods and services such as income, housing, or healthcare

☐ Fear of negative consequences for not participating in the research (e.g. institutionalization, deportation, disclosure of stigmatizing behavior)
☐ Approached for participation in research during a stressful situation such as emergency room setting, childbirth (labor), etc.

5.0 Research Locations and Sample Size:

5.1 Research Locations

All research will be conducted remotely via the Prolific platform and Qualtrics.

5.2 Sample Size

We plan to have at most 50 participants. We need 40 participants to complete the study. We include 10 additional participants to account for potential drop-outs and other responses that have to be thrown out for data quality issues.

6.0 Procedures Involved:

Participants will access our study through the Prolific platform using the study advertisement provided in the "Prolific Description.docx." Once they access the study, they will be directed to our Qualtrics survey, as detailed in the "Survey.docx."

The survey begins by assessing participant's frequency of using social media and communication mobile applications. Participants will be presented with a list of applications and asked to select up to three that they use the most. Additionally, participants will be presented with two sets, each containing two applications along with the number of users each application has. They will be prompted to choose one from each set and provide reasons for their choice, as well as whether they would recommend the selected application to others.

Subsequent questions will explore the factors influencing participant's decisions when downloading a mobile application. We will assess their knowledge about security and privacy considerations in this context. Participants will be queried about instances in which they refrained from downloading or uninstalled applications due to security concerns. Additionally, we will inquire about their thoughts regarding overreaching permissions granted to apps.

Following this, participants will receive false information about the given applications. They will then be presented with two sets, each containing two similar applications, and asked to make a choice. This segment aims to determine whether participants alter their views and choose a different application based on the false information provided.

To conclude, we will gather demographic information from participants, including their age, gender, and educational background. A disclaimer will be provided at the end of this section, clarifying that the information they received was not accurate.

6.0 Additional Safeguards for Special Populations:

N/A

7.0 Investigational Medical Devices:

N/A

8.0 Incomplete Disclosure or Deception:

We initially do not provide any background information about the mobile applications. This is necessary because we do not want the participants to alter their views and answer according to the given information.
However, towards the end of the survey we will be providing some information about the applications based on true or false information and see whether their answers changes accordingly.
In order to make it clear that this has occurred at the end of the survey we explain this to participants and tell them which information were true and which were fabricated.

9.0 Recruitment Methods:

We will post the study on Prolific (https://www.prolific.co/) and limit it to participants in the United States that are 18+. Prolific is an online crowdsourcing platform designed to support research study recruitment, similar to Amazon MechanicalTurk. Prolific allows us to pay participants through their platform while anonymizing them to us. We only receive a Prolific ID from participants. Because we do not know the mapping of Prolific IDs to actual users, we are not able to connect survey responses back to any individual, allowing the response to be anonymous.

10.0 Consent Process:

We will obtain consent at the beginning of the survey by having the consent document at the beginning of the survey (Consent.docx). Respondents will be informed of the goals and procedures of the study, any relevant risks (there are

none beyond those faced in daily life), and steps taken by the research team to protect their confidentiality and anonymity. Respondents will have to mark in the affirmative that they understand the consent document, that they are 18+, and consent to the study. Respondents will also be informed that they may withdraw from the study at any time without any loss of compensation. Participants will not be asked to provide their name, contact information, or signature during the consent process as this would be the only data that would deanonymize their response.

11.0 Compensation:

Payment will be through the Prolific platform. We will pay participants at a rate of $12/hour, which will be equivalent to $2 as the study takes 10 minutes.

12.0 Economic Burden:

N/A

13.0 Recording with Audio, Video, or Photographs

N/A

14.0 Potential Benefits to Participants:

There are no direct benefits from participating in this research.

15.0 Risks to Participants:

There is no risk to this study greater than encountered in daily life.

16.0 Withdrawal of Participants:

If a participant wishes to withdraw from the study they are able to stop the survey at any point. Their data will automatically be removed.

17.0 Data Management and Confidentiality:

Information about the participants will be available to the entire research team. Information about the participants will be available on Qualtrics (through the survey; only accessible to the research team), and on Box in a password-protected, encrypted container.

Participants will not be recontacted. Data in this study will include all information collected via Qualtrics for the survey and any derived data from the responses.

All of the data will be stored on the Box and uploaded directly there. The data will be secured using end-to-end encryption for data transmission and access control tools employed by Box. It will also be uploaded in the form of an encrypted container, requiring a shared password maintained by the research team.

18.0 Provisions to Protect the Privacy and Confidentiality of Participants and the Research Data:

All data will be provided anonymously and the research team will only have access to the participants' Prolific ID number. There should be limited contact with the research team unless a participant has a concern and reaches out to the research team.

19.0 Provisions to Monitor the Data to Ensure the Safety of Subjects:

N/A, research does not involve more than Minimal Risk.

20.0 Compensation for Research-Related Injury:

N/A, research does not involve more than Minimal Risk.

21.0 Data Sharing and Specimen Banking:

Data that is identifiable will not be shared outside of the research team. Some of the derived data may be shared as part of the research findings, as well as to help inform potential future studies.

22.0 International Research:

N/A

23.0 Multiple sites:

N/A

24.0 Reliance Agreements/Single IRB:

N/A

25.0 Qualifications to Conduct Research and Resources Available:

Priyanka Pradhan – Student, Graduate Data Science . She is certified through CITI in social and behavioral Research.

Shaohua Lu – Student, Graduate Data Science . He is certified through CITI in social and behavioral Research.

Vishnusai Ramesh – Student, Graduate Software Systems Development. He is certified through CITI in social and behavioral Research.

Faculty Advisor -

Dan Votipka – Professor, PhD Computer Science, and has conducted a number of related research projects. He also is certified through CITI.