School: School Of Sciences



Assessment Title: Critical Analysis Assignment

Course Title: MSc. In Data Analytics

Module Title: Critical Analysis

Module Code: CO4820

 Year: 2024-2025

**A study to investigate the relationship between mobile social media app usage and concerns about personal data privacy**

Alamgir Hossain  
 MSc. In Data Analytics  
 University of Central Lancashire, Cyprus  
 Pyla, Cyprus  
 ahossain2@uclan.ac.uk

ABSTRACT

The contribution of this study is to investigate the relationship between mobile social media app usage and personal data privacy concerns. It looks at user awareness, settings for privacy and perceptions of data collection and targeted advertising. The findings raise concerns about privacy of data, mental health effects and tighter regulations. It also illustrates a strong positive correlation between privacy concerns, app permissions and government regulations. The recommended measures to curb personal data abuse include better user privacy control policies against personal data collection. There are effective measures to improve user trust and digital security.

INTRODUCTION

Mobile social media apps have become an indispensable part of daily communication and interaction worldwide. These platforms are used by users for social networking, entertainment, and information sharing in various digital spaces. However, increased mobile app usage contributes to personal data privacy risks (Hassandoust *et al.* 2021). A lot of people are unaware of how their personal information gets collected and sharaaed by the hackers. There are privacy concerns that affect users’ trust, behaviour, and decisions on the usage of mobile app in digital platforms. This study explores the association between data privacy concerns and mobile social media app usage. These factors help understand users’ awareness, and perception of privacy threats and protective measures against them online.

***Aim***

The research aims to investigate the relationship between mobile social media app usage and concerns about personal data privacy.

***Objectives***

* To evaluate how different social media apps, collect personal data through digital media.
* To identify the data privacy problems that occur due to the extremely mobile app usage.
* To recommend strategies for overcoming problems regarding personal data privacy for mobile social media app usage.

LITERATURE REVIEW

Personal Data Collection of Mobile Social Media Apps and Privacy Policy

Mobile social media app usage has surely seen a rise in worries about personal data privacy and security. Most people share personal information without knowing fully about how their data are collected, stored, and accessible by third parties. Facebook, TikTok and other companies collect a bunch of user data to personalise content and target customers (Somosi *et al.* 2023). Data breaches like the Cambridge Analytica scandal reveal the danger of inadequate privacy protection measures. User trust is influenced by privacy concerns of users that ultimately result in some users stopping the use of the app or closing their accounts. Regulations like GDPR have been implemented by governments to ensure data protection and transparency of data captured in digital platforms (Matheus *et al.* 2021). However, regardless of the regulation some of these social media app companies continue to exploit user data for commercial purposes. Users protect themselves by placing private settings and limiting shares of personal information. Younger users are more willing to trade privacy for digital engagement, according to the findings of the research (Hasal *et al.* 2021). Older users have more privacy concerns and stricter data protection practices. Therefore, the relationship between social media app usage and the feeling of privacy remains complex and evolving. These concerns help policymakers, companies, and users for developing more effective privacy protection strategies.

Data Privacy Problems Due to Extremely Mobile App Usage

Mobile apps generate excessive data and create data privacy challenges which impose user security and personal information risks. According to a 2022 survey, 55.7% of global consumers are worried about fraud on mobile apps, indicating wide concerns (Statista.com, 2022). Widely, 67% of smartphone users are worried about data security and privacy on their devices (Arbanas, 2023). These statistics highlight the seriousness of the lack of privacy measures in the contemporary market of mobile applications. Moreover, the lack of robust security measures in mobile apps exacerbates data privacy issues. One in four mobile apps has at least one high-risk security flaw that leaves it vulnerable to breach. In particular, this vulnerability poses a threat to health and wellness applications, as this type of app can result in unauthorised access to sensitive medical data if privacy protection measures are removed. This potential for breaches underscores the importance of alluding to developing such rigorous security protocols that protect user information. Thus, mobile application becomes an amplifier of data privacy issues as pervasively used by the public, evidenced by serious users’ concerns and security vulnerabilities.

Strategies for Overcoming Problems Regarding Personal Data Privacy for Mobile App Usage

In order to enhance personal data privacy in mobile app usage, it is necessary to implement robust security and also transparency in the security. When it comes to securing both user communications and sensitive information from unauthorised access, businesses have to make sure of finalising end-to-end encryption. Multi-factor authentication (MFA) is a way of enhancing account security, which involves requiring more than one identity verification step when logging in (Mohammed *et al.* 2023). The privacy policy should be transparent, describing the data collection, storage and sharing practices with users. GDPR and others like CCPA help to maintain stringent data protection compliance frameworks (Fakeyede *et al.* 2023). In order to do this, businesses adopt privacy-by-design principles where security features are built into the app’s development so that vulnerabilities are minimised. Users should also always update apps to protect their devices from cyber threats and security flaws. It educates users on the sense of privacy settings that they can use to adjust and avoid the sharing of useless data to a greater extent. By using such anonymous data processing techniques as differential privacy, companies do not get the ability to link data with specific persons. In Apple’s App Tracking Transparency framework, users can opt out of third-party data tracking (Cheyre *et al.* 2023). All these companies provide end-to-end encryption for messages as well as calls. Together these proactive strategies from companies and users help to strengthen data privacy in mobile app usage. This helps to boost trust and security in online environments, given that addressing privacy concerns.

Theoretical Underpinnings

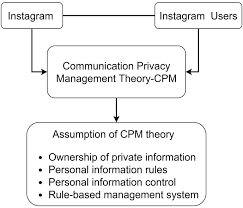


Figure 1: Communication Privacy Management (CPM) Theory (Source: Meng, 2024)

The ***Communication Privacy Management (CPM) Theory*** defines how people manage personal information disclosure online. It draws attention to the tension between disclosing information and keeping within privacy bounds on digital platforms (Meng, 2024). Mobile app users negotiate for information visibility and the security of personal data. Violations of privacy expectations can result in low levels of trust and engagement with mobile applications. Understanding the aspects of CPM theory is beneficial for developing privacy protection strategies for social media app usage.

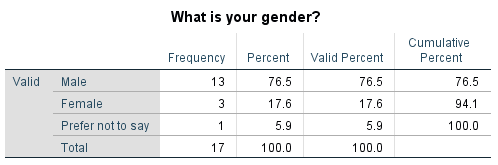
Literature Gap

Existing studies have covered mobile app usage and data privacy, but lack in user behaviour analysis. Demographic factors are not taken into consideration in how privacy concerns and security practices are analysed in mobile applications. There are very few studies that examine how regulatory policies can control mobile app data privacy risks. Filling these gaps improves understanding of current and future privacy challenges and solutions.

**METHODOLOGY**

The researcher has selected the primary quantitative research design for completing the study. Survey method has been used to collect quantitative data from 17 participants whose age lies between 18 to 54 years. 12 questions have been asked to them regarding the usage of social media. The selection of the primary data collection method is appropriate for the study as it helps the researcher to obtain the experiences directly from the participants. In addition, the quantitative data helps to perform statistical analysis by answering the “what” and “which” types of questions (Ghanad, 2023). Since the purpose of the study is to identify the relationship between mobile social media app usage and concerns for personal data, the collection of quantitative data is appropriate for completing the study effectively. After collecting the data, different statistical analyses have been performed in SPSS to meet the research objectives of the study. For example, frequency statistics and descriptive statistics have been performed to analyse the demographic information. In addition, correlation analysis and T-Test analysis have also been performed to identify the relationship between mobile app usage and concerns for personal data.

**RESULTS**



**Table 1: Frequency analysis of gender**

The sample of the study consists of 17 respondents and the majority of the participants are male (76.5%). Also, a smaller proportion of respondents are female (17.6%) and 5.9% of them choose not to disclose their gender.

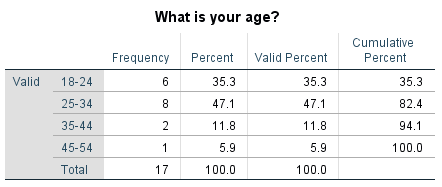


Table 2: Frequency analysis of age

Almost half (47.1%) are aged 25 to 34 years and the next most represented age group is 18 to 24 years (35.3%). However, 5.9% of respondents are the least represented age group which is from 45-54 years.

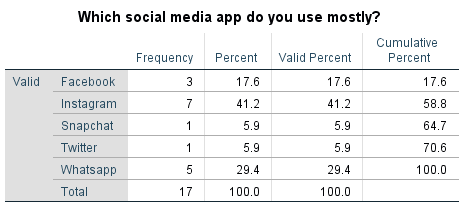


Table 3: Frequency analysis of mostly used social media app

The most used social media app is consistently Instagram which is used by 41.2% of the respondents. 28.5% of participants use Facebook, followed by 29.4% on WhatsApp.

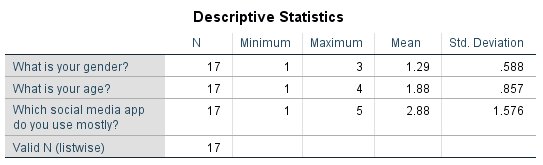


Table 4: Descriptive statistics

Variations in demographic distribution and social media preferences amongst respondents are indicated by the mean values.

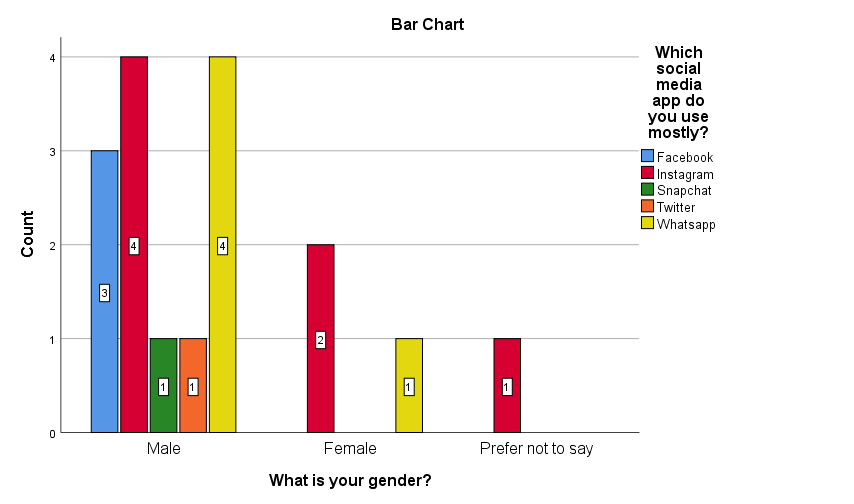


Figure 2: Visualization between gender and mostly used social media app

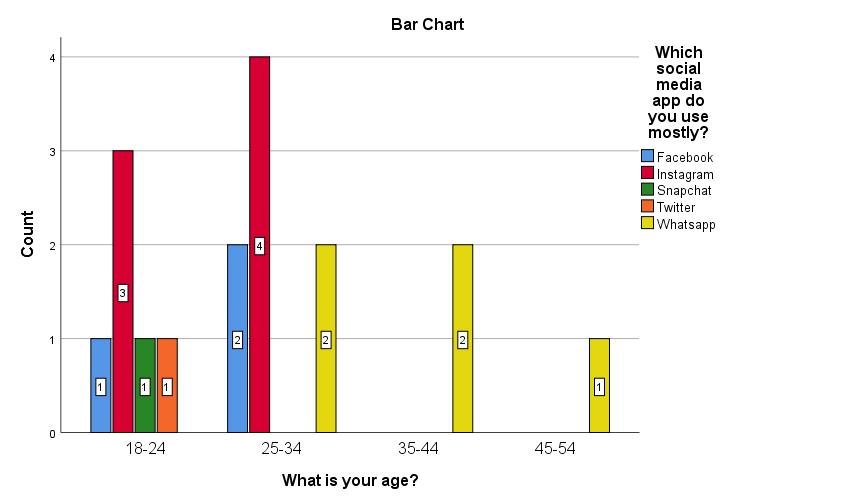


Figure 3: Visualization between age and mostly used social media app

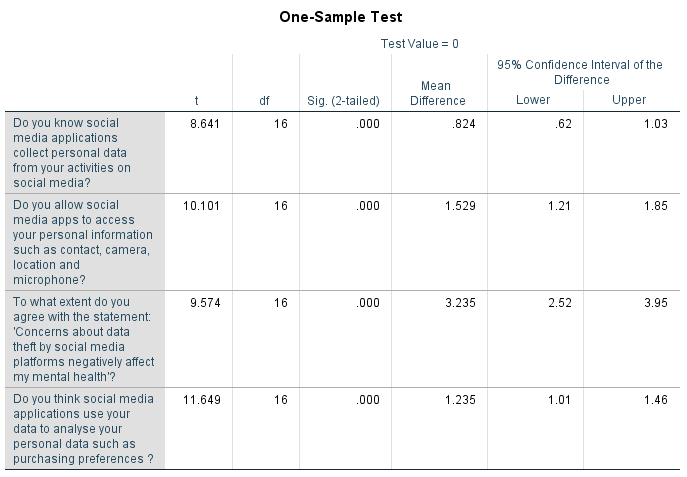


Table 5: Result of T-Test

According to the results of the sample tests, all measured privacy-related issues have very strong statistical significance. Respondents agree that social media apps collect personal data and have a mean difference of 0.824 (p = 0.000). Thus, with a mean difference of 1.529 (p = 0.000), most participants allow apps to access sensitive information. The effect on mental health of data theft is significant enough to affect the concern in the mean difference of 3.235 (p = 0.000). Respondents are highly certain that social media apps process personal data, with a mean difference of 1.235 (p = 0.000). The findings reveal the importance of privacy concerns and the psychological consequences for users.

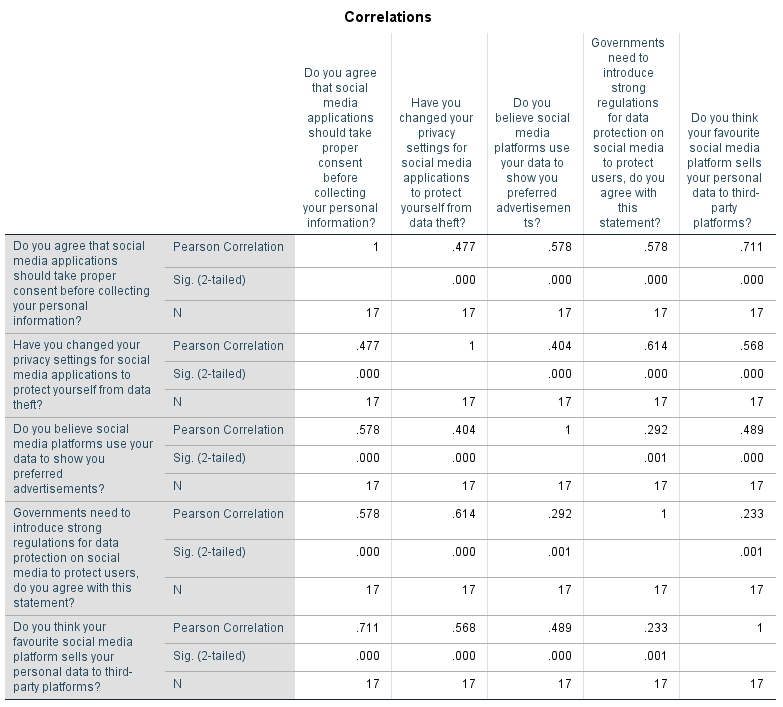


Table 6: Result of correlation analysis

The relationship results showed a high relationship between privacy concerns and social media practice perceptions. Users believe platforms use personal data and this correlation was very strong and positive (r = 0.711, p = 0.000). Changing privacy settings correlates with consent before data collection (r = 0.477, p = 0.000), indicating the presence of awareness of the security measures. The stronger government regulation (r = 0.578, p = 0.000) supported by the users indicates the demand for more strict policies. Targeted marketing concerns, such as social media’s influence on advertisements, show a moderate correlation (r = 0.489, p = 0.000). Overall, findings show concerns for users’ privacy and expectations in terms of regulation.

DISCUSSION

The study finds that there is a strong link between mobile social media app use and data privacy concerns. The male is the majority of respondents (76.5%) with 47.1 % being above 25 and younger than 35 years. The app that users most use is Instagram, of which 41.2% actively engage with the platform. Respondents agree that apps collect and process their data, and confirm significant concern about data privacy through statistical tests. There is a mean difference of 3.235 (p = 0.000) that raised concerns about mental health impacts. There is a strong positive correlation between privacy settings and consent (r = 0.477, p = 0.000) implying awareness about security measures. The findings point to users’ need for strict government regulation (r = 0.578, p 0.000) to improve data protection and privacy policies.

CONCLUSION

From the above discussion, it can be concluded that the study shows a strong link that exists between the usage of mobile social media apps and data privacy concerns. The findings of the study indicate that most respondents acknowledge that social media platforms are collecting personal data to target the market. The need for strict regulation is very essential to address data security concerns and mental health impacts. People are aware of privacy settings, but a significant number continue to expose highly personal data. The results of the correlation indicate a strong demand for government intervention to improve data protection policies. The results show that increases in user’s trust are achievable by increasing transparency and improving more rigorously regulations. Future studies should examine broader demographics and longer-term consequences of data privacy concerns.

RECOMMENDATIONS

* Recommendation 1: Strengthening User Privacy Controls

Social media platforms should ease the ability for users to personalise the setting of data sharing. Preventing unauthorized access to sensitive information includes stronger encryption, two-factor authentication, and opt-in permissions. Regular information about privacy policies, and data used should be provided to users to allow them to make informed decisions.

* Recommendation 2: Implementing Stricter Government Regulations

Comprehensive data protection laws should be introduced by governments to initiate the regulation of where social media apps collect, store and use data. The system can be enforced by making data-sharing practices transparent and imposing penalties for breaches. Making security stronger can be done through mandatory user consent policies and periodic audits. It can also enhance the protection for misuse by educating users on digital privacy rights.

REFERENCES

Arbanas, J. (2023). *Data privacy and security worries are on the rise, while trust is down*. [online] Deloitte Insights. Available at: https://www2.deloitte.com/us/en/insights/industry/telecommunications/connectivity-mobile-trends-survey/2023/data-privacy-and-security.html [Accessed 5 Mar. 2025].

Cheyre, C., Leyden, B.T., Baviskar, S. and Acquisti, A., (2023). *The Impact of Apple's App Tracking Transparency Framework on the App Ecosystem* (No. 10456). CESifo Working Paper. <https://www.econstor.eu/bitstream/10419/279205/1/cesifo1_wp10456.pdf>

Fakeyede, O.G., Okeleke, P.A., Hassan, A.O., Iwuanyanwu, U., Adaramodu, O.R. and Oyewole, O.O., (2023). Navigating data privacy through IT audits: GDPR, CCPA, and beyond. *International Journal of Research in Engineering and Science*, *11*(11). <https://www.researchgate.net/profile/Olajumoke-Oyewole/publication/384398894_Navigating_Data_Privacy_Through_IT_Audits_GDPR_CCPA_and_Beyond/links/66f6f344f599e0392fa903fc/Navigating-Data-Privacy-Through-IT-Audits-GDPR-CCPA-and-Beyond.pdf>

Ghanad, A., (2023). An overview of quantitative research methods. *International journal of multidisciplinary research and analysis*, *6*(08), pp.3794-3803. <https://www.researchgate.net/profile/Anahita-Ghanad/publication/373370007_An_Overview_of_Quantitative_Research_Methods/links/67b28ffc645ef274a48341a1/An-Overview-of-Quantitative-Research-Methods.pdf>

Hasal, M., Nowaková, J., Ahmed Saghair, K., Abdulla, H., Snášel, V. and Ogiela, L., (2021). Chatbots: Security, privacy, data protection, and social aspects. *Concurrency and Computation: Practice and Experience*, *33*(19), p.e6426. <https://onlinelibrary.wiley.com/doi/pdf/10.1002/cpe.6426>

Hassandoust, F., Akhlaghpour, S. and Johnston, A.C., (2021). Individuals’ privacy concerns and adoption of contact tracing mobile applications in a pandemic: A situational privacy calculus perspective. *Journal of the American Medical Informatics Association*, *28*(3), pp.463-471. <https://pmc.ncbi.nlm.nih.gov/articles/PMC7936517/pdf/ocaa240.pdf>

Matheus, R., Janssen, M. and Janowski, T., (2021). Design principles for creating digital transparency in government. *Government Information Quarterly*, *38*(1), p.101550. <https://www.sciencedirect.com/science/article/pii/S0740624X20303294>

Meng, X., (2024). From Interpersonal Privacy to HumanTechnological Privacy: Communication Privacy Management Theory Revisited. *Technical Communication*, *71*(2), pp.72-88. <https://www.stc.org/techcomm/2024/05/07/from-interpersonal-privacy-to-human-technological-privacy-communication-privacy-management-theory-revisited/>

Mohammed, A.H.Y., Dziyauddin, R.A. and Latiff, L.A., (2023). Current multi-factor of authentication: Approaches, requirements, attacks and challenges. *International Journal of Advanced Computer Science and Applications*, *14*(1). <https://www.mdpi.com/2076-3417/13/19/10871>

Somosi, Z., Hajdú, N. and Molnár, L., (2023). Targeting in Online Marketing: A Retrospective Analysis with a Focus on Practices of Facebook, Google, LinkedIn and TikTok. *European Journal of Business and Management Research*, *8*(1), pp.33-39. <https://mail.ejbmr.org/index.php/ejbmr/article/download/1724/1011>

Statista.com. (2022). *Mobile app cyber security threats global 2022 | Statista*. [online] Available at: https://www.statista.com/statistics/1381432/mobile-app-usage-cyber-threats-consumers-worldwide [Accessed 5 Mar. 2025].

APPENDIX

Survey Title: A Study to investigate the relationship between mobile social media App usage and concerns about personal data privacy

**Consent:** This study explores the relationship between mobile social media app usage and personal data privacy concerns. Participation is voluntary, anonymous, and confidential. The collected primary data will be securely stored for a period of 2 months following data collection. After this period, the data will be permanently deleted or anonymized to ensure participant confidentiality, in compliance with ethical research guidelines and data protection regulations. You may withdraw anytime without consequences.

**Questionnaires:**

1. What is your gender?

* Male
* Female
* Prefer not to say

2. What is your age?

* 18 to 25
* 26 to 30
* 31 to 35
* 36 to 40
* 41 or above

3. Which social media app do you use mostly?

* Instagram
* Facebook
* LinkedIn
* WhatsApp
* Snapchat
* Others

4. Do you know social media applications collect personal data from your activities on social media?

* Yes
* No

5. Do you allow social media apps to access your personal information such as contact, camera, location and microphone?

* Yes
* No
* Allow only while using the app

6. To what extent do you agree with the statement: 'Concerns about data theft by social media platforms negatively affect my mental health'?

* Strongly disagree
* Partially disagree
* Neutral
* Partially agree
* Strongly agree

7. Do you think social media applications use your data to analyse your personal data such as purchasing preferences ?

* Yes
* No
* I don't think so

8. Do you agree that social media applications should take proper consent before collecting your personal information?

* Strongly disagree
* Partially disagree
* Neutral
* Partially agree
* Strongly agree

9. Have you changed your privacy settings for social media applications to protect yourself from data theft?

* Yes
* No

10. Do you believe social media platforms use your data to show you preferred advertisements?

* Strongly disagree
* Partially disagree
* Neutral
* Partially agree
* Strongly agree

11. Governments need to introduce strong regulations for data protection on social media to protect users, do you agree with this statement?

* Strongly disagree
* Partially disagree
* Neutral
* Partially agree
* Strongly agree

12. Do you think your favourite social media platform sells your personal data to third-party platforms?

* Strongly disagree
* Partially disagree
* Neutral
* Partially agree
* Strongly agree