Journal of Management Science Research Review
https://jmsrr.com/index.php/Journal/about

Volume 5 Issue No 1 (2026)

Online ISSN: 3006-2047
Print ISSN: 3006-2039

Impact of data privacy practices on mobile app adoption

Asif Niaz
MS Scholar at Information Technology University of the Punjab Lahore, Pakistan

Yasir Karim
Faculty Member at Faculty of Business and Management Science, Information Technology University of The Punjab Lahore Email: yasirkarim310@gmail.com

Abstract
Rapid growth in mobile applications has changed people's ideas about accessing services, communicating, and performing daily activities. It has also posed a barrier in using these applications because of increasing data privacy-related issues. The present study investigates the impact of data privacy practices on mobile app adoption, considering perceptions, trust, transparency, security measures, and data-sharing behaviors. Following a qualitative research design, the study was done by conducting seven semi-structured interviews with mobile app users in Lahore, Pakistan, from different professional and educational backgrounds. Thematic analysis was employed to derive major patterns and insights regarding privacy-driven adoption behavior. Findings reveal that users become much discomforted towards applications that require excessive and unnecessary personal information, significantly deterring their adoption intention. Transparencies within the privacy policies, particularly full and clear disclosure of data usage, appeared to be significant determinants creating trust among users. Trust was conceptualized as a mediating variable to use in linking privacy practices to the adoption decisions, especially for applications handling sensitive financial or personal data. Visible security features, such as encryption, two-factor authentication, and login alert, among others, positively influenced the hastening tendencies of users towards the adoption of mobile applications. The authors have also categorized users based on their selective data-sharing approaches whereby sensitive information would be withheld unless absolutely required for the core app functionality. It contributes to the literature by providing a round perspective on how privacy practices influence mobile app adoption on the user side. Findings of this study are helpful for the app developers, marketers, and policymakers with the need for privacy-centric design, transparent communication, and sound security measures to build up trust, adoption, and continuous user engagement.

Keywords: Data Privacy, Mobile App Adoption, User Trust

Introduction

The mobile application industry has experienced a dramatic transformation in the past years, influencing the manner in which individuals engage services, interact, and access content through their daily experiences. Mobile apps have become the most

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

commonly used platform for multiple activities, including banking, shopping, social networking, healthcare, and entertainment (Singh, Tyagi, Vasistha, Sikarwar, Malik, Singh & Verma, 2025). With millions of apps on the Google Play Store and Apple App Store, mobile applications provide personalized experiences, instant access to services, and convenience that even traditional platforms cannot match (Alrumayh, Lehman & Tan, 2021).

Such tailored mobile applications collect vast amounts of user data ranging from basic personal identifiers such as names and email addresses to behavioral data such as browsing patterns, app usage history, location, and payment information (Chang, Zaeem & Barber, 2020). This information is used by app developers to enhance the user interface, recommend personalized content, and undertake targeted promotions. Such advantages come with tremendous privacy issues. Users are increasingly aware of the risks of sharing personal information, such as identity theft, unauthorized usage of data, cyber-attacks, and unsolicited targeted marketing (Jain, Sahoo & Kaubiyal, 2021).

Data privacy practices, consequently, are becoming an essential factor in shaping users' opinions about mobile applications (Balapour, Nikkhah & Sabherwal, 2020). The practices build the technology, organizational policy, and behaviors for refraining from engaging in user information misuse. They include procedures for the storage of user data in a secure manner and anonymization of sensitive user data, obtaining user data with the user's explicit consent according to the requirements stipulated in various regulations such as GDPR and CCPA regulations (Celestin, 2024). Perceptions of users on data privacy practices consequently influence consumers' trust in app providers, their willingness to share personal data, and therefore their decision to adopt or reject mobile applications (Hudson & Liu, 2023).

Though the influence of data privacy practices on mobile adoption remains paramount, there exists scant literature in assessing the direct connection between these privacy practices and adoption behavior (Alkhalifah & Al Amro, 2017; Hasani, Rezania, Levallet, O'Reilly & Mohammadi, 2023). Such gap creates more pressing need for research probing how data privacy practices surrounding transparency, security, consent, and trust have an influence on mobile app adoption. This study strives to contribute in filling up this gap through an in-depth qualitative analysis bringing forth user experiences, expectations, and concerns toward data privacy in mobile applications.

Problem Statement

Mobile applications score high on personalized recommendations, convenience, and real-time connectivity, but at the same time run into privacy disputes that thwart users from accepting them. An app may ask for unnecessary details, may make privacy policies obscurely poor, or may not apply security considerations that users may prefer. These concerns can lead to the erosion of trust and confidence among the users (Xing, Lu, Zhao & Cao, 2024).

As far-sighted users are concerned, dedication to an app might be postponed or smashed early due to heightened consciousness of data misuse, privacy breaches, or

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

vague policies. where one app may bespeak serious facilities while the other is apprehended for having a poor reputation regarding privacy. For instance, mobile banking apps that fail to express unequivocally about encryption might drive away unknowing customers who are looking for ease in their financial conduct. Similarly, social media applications which look to acquire permission not only beyond a reasonable doubt may encounter the wrath of the consumer and lack active participant levels.

Empirical evidence regarding how privacy practices produce affirmative contributions to adoption is scarce (Anawar, Othman, Selamat, Ayop, Harum & Rahim, 2022; Kamin, 2017). It remains crucial to establish how such features as transparency of worlds, consent systems, trust-building strategies, and robust security features may affect users' willingness to adopt such mobile applications. These medleys of ingredients are much considered by app developers, marketers, and policymakers on how to socialize adoption rates, enhance engagement, and formulate sustainment in the increasingly privacy-conscious digital market. This research, intends to study these dynamics in a way that becomes privy to the design of privacy-aware mobile applications.

Research Objectives

This research seeks to examine the impact of data privacy behavior towards the adoption of the mobile application with the objectives below:

To investigate the perception of user data privacy practices in mobile apps.

To explore the mediating influence of trust with regard to the adoption of the mobile app and the practices of privacy.

To investigate the impact of transparency in the communication of privacy issues on user adoption.

To assess the impact of security systems such as encryption and anonymization on user decision-making in adopting apps.

To interpret user expectations and concerns about data privacy in mobile applications.

Research Questions

From the research objectives, the study is guided by the following questions:

How do users rate the treatment of personal data in mobile applications?

What is the influence of trust upon the choices of users in adopting applications on the phone?

What is the relationship between transparency/communication about privacy policies and adoption behaviors?

What is the effect of security aspects such as encryption and anonymization on user willingness regarding applications?

What are some of the most important issues for the end-users in terms of data privacy in mobile applications?

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

Literature Review

Users' Perception of Data Privacy Practices

User perception of data privacy indicates how a person understands, interprets, and judges how a mobile application collects, processes, stores, and protects one's private information (Alnajrani & Norman, 2020). Thus, a person evaluates the cognitive, emotional responses, and behavioral predisposition to privacy measures. Users' perception is influenced by both technical and social organizational factors. For example, the visibility of privacy mechanisms, usage of similar sets of applications, and their reputation (Nellore, Mishra & Zimmer, 2024).

This can enable greater adoption by users. So, people are likely to adopt applications which they trust and think ethical with regard to privacy consideration (Al-Kfairy, Alomari, Al-Bashayreh, Alfandi & Tubishat, 2024). Thus, applications that provide open privacy with minimum required personal information will definitely gain more acceptances by users. A case in point is the mobile banking applications that clarify encryption policies, while the e-commerce applications that emphasize secure payment methods tend to be adopted at a higher rate (Zhang & Xu, 2024). Meanwhile, the apps that are collecting a lot of unnecessary data, as well as permissions that cannot be justified, are usually considered intrusive and create suspicion that leads to abandonment.

However, the perceived intrusiveness of data collection considerably influences adoption behavior (Pal, Babakerkhell & Roy, 2022). In particular, users are very sensitive to permissions that are indeed unnecessary to operate the core function of the app. An example of this kind of behavioral effect is an app simply used for calculating that requests access to contacts or location data. These create negative perceptions, which will also reduce intent toward adoption. This rule fits with the observations made by Dinev et al. (2013) because privacy concerns regard more than technical measures but also perceived intentions of app providers (Wang & Lin, 2017). They interpret privacy practices in terms of ethics, reputation, and prior behavior. A company that has offended in privacy-related matters in the past or has vague policies will even have more negative perceptions by users who will not adopt even if such an app is full of functionality (Acquisti, Brandimarte & Loewenstein, 2020).

Knowing user perception is important for the construction of effective yet trusted mobile applications. User perception defines behavior, loyalty, and engagement as well as provides competitive advantage to apps that meet definitions of how users expect privacy measures to be adopted in a digital environment Yadav et al. (2024). Considering cognitive-emotional-social factors for the perception of measures will lead to implementation of privacy measures that would address legal requirements and adherence to users' values and increase adoption chances.

Trust as Mediator Amongst Privacy Practices and Adoption of Mobile Apps

Trust has been recognized as one of the key mediators across privacy practices and adoption behavior in mobile applications (Ashrafi, Ahmed, & Shahid, 2025): Confidence that customers put in providers of apps about responsible, safe, and ethical management of their personal information (Mohd Ramsi, Idris & Nordin,

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

2024). Mobile applications trust expectations include an assurance of safety for data, nonmisuse, and compliance to stated policies from the app (Mantovani, Antokol, Hoekstra, Nouwt, Schutte, Zilgalvis, Castro Gómez-Valadés & Prettner, 2017).

Studies have shown that trust leads to better intention for adoption and also moderates privacy concerns. Users may realize the risk, but high trust can reduce their concerns, which can lead to user confidence in using such apps (Wang & Lin, 2017). Reliance is a crucial aspect of apps that ask for sensitive information, including banking-related mobile apps, health management, or location-based services (Sharma et al., 2020). A healthcare app may not be welcomed even if advanced features are being offered when users do not trust the organization associated with that app with the storage of their medical records.

Trust-forming mechanisms in mobile apps include options for consent, notices on the use of data, privacy dashboards, and control over personal data. According to the study of Ashrafi, Ahmed and Shahid (2025), trust is a psychological construct that links privacy practices to adoption behavior. One will not use anything, including applications presenting great utility and usability, without such trust. Contrarily, such applications can convert all these into a positive perception of trust from use and engage consumers over time.

Apart from those, however, organizational reputation is prominently mentioned against such measures. Most of such brands were well-known with an ethical history followed by strict compliance to privacy regulations with well-publicized privacy measures-all of which are expected to bring users' trust. Trust can also serve as effects regarding word of mouth. Users are more likely to tell others about an application perceived as trustworthy compared to one deemed otherwise, which gets converted into further adoption and retention (Lee & Hong, 2019; Zalloum, Alghadeer & Nusairat, 2019).

Transparency and Communication of Privacy Policies

Transparency is one of the basic elements of the data privacy field, since this provides details about how the data of the users is collected, stored, and then used afterward in a clear, easily understandable manner (Kalliokoski, 2024). Reduced uncertainty and perceived risk through transparent communication leads to a positive impact on adoption behavior (Oldeweme, Märtins, Westmattelmann & Schewe, 2021). The clearer and more concise privacy policies tend to sway users to adopt the app rather than long-winded legal jargon or ambiguous statements that will misinterpret the ideas behind them and create a lack of trust. According to Murmann and Karegar (2021), users are more responsive to privacy notifications that explain data usage as well as consent mechanisms. Pop-up notices, opt-in or opt-out options, and real-time notices regarding data collection and usage help in transparency through which users can take their own decisions.

Moreover, transparency extends beyond policy documents to all interactions that a user has with the app (Lie, Austin, Ping Sun & Qiu, 2022). Apps with immediate feedback about data collection permissions, which explain why some permission are needed, and relevant updates about changes made to privacy settings encourage their

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

use and higher levels of trust (Brandtzaeg, Pultier & Moen, 2019). Transparent communication is what separates apps in a competitive mobile application market. Studies show that users are usually seen to perceive applications that display clear privacy policies as ethical and caring towards users, and this is set to improve adoption intentions for the application themselves (Kununka, 2019; SIYADRI & DEEPAK AKELLA, 2024). That is, being transparent is not only an effective approach to adoption but is equally effective in boosting levels of satisfaction and loyalty. This is due to the ability to discuss data processing routines for the application to be used by the users themselves. All in all, transparent communication is a critical enabling condition for adoption, trust, and continuous engagement.

Security Features and Their Impact on Adoption

Security often constitutes the major part of mobile app privacy. It includes technical safeguards such as encryption, anonymization, secure storage, and two-factor authentication, among others (Gautam & Guptar, 2024). Such mechanisms guard user information from unauthorized access and/or breaches and possible misuse. Most importantly, security becomes highly relevant in apps that deal with any financial, health, or location-sensitive data, as breaches could lead to serious ramifications (Al-Harrasi, 2021). Studies have reported that most users associate strong security characteristics with reliability and ethical behavior of the app provider, as well as professionalism (Shneiderman, 2020; Tsohou & Holtkamp, 2018). Jain (2024) talks of privacy-by-design, meaning that security is inherent at all levels of development and operational processes for the app. Users will be more inclined to see strong security practices as reliable and thus will consider the perceived risk lower and more adoption-friendly by using them.

Moreover, visible security features serve as psychological assurance indicators of trustworthiness. When users are aware that encryption, anonymization, and secure storage exist, they will be more inclined to share personal data and adopt the app (Distler, Lallemand & Koenig, 2020). Thus, security features serve as mitigators of technical risks as well as trust-building signals that boost adoption behavior. Applications that fail any of these two requirements- either visible security measures or proper communication of strategies regarding their security- will deter many prospective users, thus showing how joined-up security, trust, and adoption are (Obaidat, Obeidat, Holst, Al Hayajneh & Brown, 2020).

Users' Expectation and Concern Regarding Data Privacy

User expectation, concerning mobile applications with respect to privacy, has become very complex (Hudson & Liu, 2023). Users have minimum expectations for data collection; they should control their personal information, ensure secure storage, and expect communication in transparency (Bonatti, Kirrane, Polleres & Wenning, 2017). However, on the other side, users complain about excessive permissions, sharing their information without consent, data breaches, and marketing intrusion (Mills & Harclerode, 2017). Research has revealed that regression in adoption, engagement, and churn can be brought about if there is no fulfillment of any of those expectations

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

(Adekunle, Chukwuma-Eke, Balogun & Ogunsola, 2023). Users are more likely to withhold their sensitive information if the demand, which comes from the "application," does not aptly clarify the purposes of such demands, as well as if the privacy practice information was not communicated. The opposite is true with proactive addressing of privacy issues, user-centered control mechanisms, and clear policy statements regarding privacy: these will attract and retain users.

Such understanding of expectations and concerns is important for developers in order to balance personalization with functionality and, at the same time, privacy protection. Increasingly, users are comparing apps based on privacy, and privacy has become a point of competitive advantage with research indicating that increasing privacy expectations may bolster satisfaction, engagement, and long-term loyalty because users view the app provider as responsible and trustworthy (Bahar, Prananta, Afifudin & Rahman, 2024; Dehghanpouri, Soltani & Rostamzadeh, 2020). Lastly, privacy expectations outlined against concerns will join in the process of adoption and help to ensure that an app can be used within sensitive privacy markets over the long term.

Methodology

Research Methodology

A qualitative approach was adopted in this study so that participants' subjective experiences, feelings, and decisions regarding mobile application privacy practices could be explored in-depth (Mushtaq, Suleman & Qayyum, 2023). Qualitative methods were therefore best suited since they potentially capture constructs such as perceptions, trust formation, and behavioral intention, which are extremely hard to measure through quantitative means.

Semi-structured interviewing recorded the narratives in detail, thereby allowing the researcher to probe and obtain in-depth insights into users' attitudes toward privacy policies, security mechanisms, trust, and actual adoption behavior (Alsayed, Ismail & Hasan, 2024). The qualitative paradigm opened up ways to observe patterns, contradictions, and granular insights across different user profiles.

Data Collection

Participants: Participants for the study included seven respondents from Lahore with varying professional and educational backgrounds such as CEOs, managers, engineers, students, interns, and software developers. Diversity in criteria could give a very wide lens onto mobile application usage and privacy issues.

Procedure: The purposive sampling technique was applied to select participants with mobile app usage and privacy concerns as their main focus (Brannon, Mitchell & Liao, 2022). Each of the interviews lasted 30-45 minutes and was conducted in person. Interviews were recorded on audio, transcribed verbatim, and anonymized. Informed consent forms were distributed to the participants through whom they acknowledged that their anonymity was guaranteed and they knew their rights to withdraw from the study.

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

Effect of Methodology

This methodology allowed for an in-depth understanding of how privacy practices shaped mobile app adoption from the user perspective. Such qualitative insights merged with existing theories on privacy and adoption, giving rise to a framework that depicts interplay between trust, transparency, security, and user expectations while providing clear and actionable recommendations to app developers and policymakers for the development of privacy-aware applications that would aid in user adoption.

Data Analysis

This study explored the impact of data privacy practices on mobile app adoption in Lahore, Pakistan. The seven semi-structured interviews conducted involved people coming from diverse professional and academic backgrounds, including CEOs, general managers, engineers, software developers, interns, and students. Looking at the patterns, perceptions, and experiences related to privacy policies, trust, security measures, user control, data-sharing issues, and adoption behavior formed the crux of the analysis.

Demographic Information of Respondents

The diversity captured multiple perspectives on mobile app usage and privacy from technical knowledge of app usage, awareness of privacy, formation of trust, and emotional responses and behavioral outcomes. This helped the study in gauging functional aspects as well as psychological ones concerning privacy and the effects of perception on adoption behavior.

Respondent	Background/Role
R1	CEO, Tech Company
R2	General Manager, IT Firm
R3	Intern, Systems Company
R4	Mechanical Engineer, Public Sector
R5	MS Student, IT University
R6	Senior Account Manager, Marketing Firm
R7	Software Developer, IT Lab

Phases of Thematic Analysis

Thematic analysis followed the six phases suggested by Nowell et al. (2017), "familiarization," "coding," "developing themes," "reviewing themes," "defining themes," and "reporting." “It enabled inductive and deductive reasoning to occur, combining their experiences with the constructs that theory had developed for privacy, trust, and adoption behavior”.

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

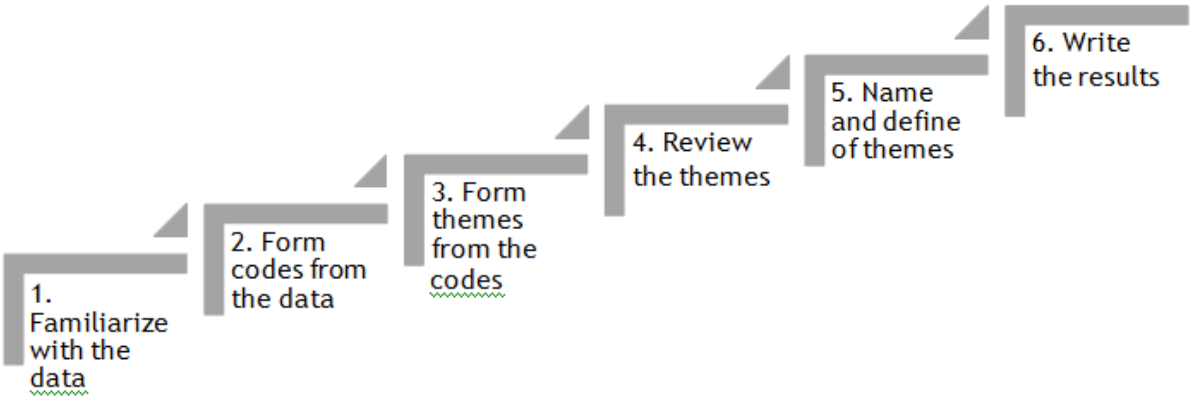

Figure 4.1: Phases of thematic analysis (Nowell et al. 2017)

Thematic Analysis Based on Interview Questions

Question 1: What do you feel when a mobile app requires your personal information?

Theme 1: User Discomfort

Respondents	Initial Code	Authentic Data Extract	Re-Coded As	Theme
R1, R2, R3, R4, R5, R6, R7	Annoyance at unnecessary requests	"I feel annoyed when an app requests information not essential to its functionality."	Discomfort	User Discomfort
R1, R2, R4, R5, R6, R7	Concern about misuse	"Unnecessary permissions raise concerns about fraud or data sharing."	Risk perception	
R1, R3, R5	Comfortable with essential info	"I am comfortable sharing data if it is needed for proper functionality."	Acceptance of core data requests	

Results

Respondents resented and felt insecure whenever apps required their personal information that seemed unrelated to the core functionality. Such excessive requests, including requests for access to contacts, location, camera, or microphone, further aroused fear of data misuse or identity theft. On the contrary, requests for essential data strictly related to app functions were usually accepted, reflecting conditional trust based on perceived necessity. This theme illustrates how user discomfort with the level of privacy has become a significant barrier toward adoption. The developer, then, must strategically design permission requests to blend minimally with user intrusive

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

demands, highly justify the reasons for data collection, and stress that such information will be handled properly. The balance between functionality and privacy enhances trust will support long interaction and, this is where ethical and transparent practices for data handling will matter.

Question 2: How do privacy policies affect your decision to install an app?
Theme 2: Trust and Clarity

Respondents	Initial Code	Authentic Data Extract	Re-Coded As	Theme
R1, R2, R4, R5, R6	Clear policies encourage adoption	"Clear, concise policies make me feel confident to install an app."	Policy clarity	Trust & Clarity
R1, R2, R4, R5, R7	Vague or long policies reduce trust	"Long or vague policies reduce my trust in the app."	Policy complexity	
R3, R7	Rarely read policies	"I usually skip reading the privacy policy if I trust the app or brand."	Brand reliance	

Results

Privacy policies emerged as primary mechanisms for building trust. Respondents felt that short, lucid policies encouraged installation, while long-winded or ambiguous policies deterred confidence. Some admitted rarely to reading the policies, with much of their trust dependent on brand reputation or past experience. Thus, one could say that adoption rests for those policies being existent and largely non-ambiguous and non-technical. Transparency speaks of ethical behavior and builds confidence that privacy protection exists. Essentially, by reducing uncertainty and perceived risk, at the end, these clear privacy policies foster user trust such that any adoption is beneficial in creating continued engagement. In trying to keep policies effective, then detail and access cannot be sacrificed; otherwise, maximum comprehension will elude users.

Question 3: Which privacy practices make you feel safer while using the app?
Theme 3: Privacy Control

Respondents	Initial Code	Authentic Data Extract	Re-Coded As	Theme
R1, R2, R3, R4, R5, R6, R7	Control over permissions	"I feel safe when I can choose what data the app can access."	User autonomy	Privacy Control
R1, R3, R4, R5	Notifications about account	"Login alerts from new devices make me	Activity monitoring	

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

Respondents	Initial Code	Authentic Data Extract	Re-Coded As	Theme
	activity	confident the app is secure."		
R2, R6, R7	Transparency on third-party sharing	"Clear statements against selling data to third parties increase trust."	Third-party transparency	

Results

This study's data indicated that user empowerment and transparency were at the center of safety perception. Participants identified granular permission control, notifications for new logins, and explicit sharing with third parties as features that could inspire confidence. Such matters of privacy empower users to take charge of their private information and instill confidence in the integrity of the app provider. By permitting informed consent and control, the apps reduce perceived risk and enhance their adoption and sustained use. The findings highlight that privacy control and transparency must be integrated when constructing applications for meeting user expectations for safety and trustworthiness, along with ethical management of data.

Question 4: How do security measures affect your continuance of app use?
Theme 4: Security Features

Respondents	Initial Code	Authentic Data Extract	Re-Coded As	Theme
R1, R2, R5, R7	Encryption and 2FA	"Strong encryption and two-factor authentication make me feel safe."	Technical security	Security Features
R3, R4, R6	Login alerts and monitoring	"Login alerts increase my confidence in continued use."	Activity alerts	
R1, R2, R4	Absence of security reduces usage	"Apps that seem unsafe are quickly deleted."	Low trust	

Results

Security features heavily influenced further use and trust. Specifically, participants trusted applications that featured strong encryption, two-factor authentication, and activity monitoring. Conversely, this risk-averse attitude made them promptly remove apps with no obvious indications of security measures. Security seemed particularly important for applications handling sensitive data, such as finances, identity, or location. These features provide some signal of provider reliability and thus permit a

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

reduction in perceived risk and stimulate adoption accordingly. Thus, ensuring user confidence and engagement will demand clear communication and reflective embedding of advanced, easy-to-operate security features by the developers. Therefore, strong security implementation is directly linked to sustainability of adoption.

Question 5: What information do you withhold from sharing with mobile apps?
Theme 5: Selective Data Sharing

Respondents	Initial Code	Authentic Data Extract	Re-Coded As	Theme
R1, R2, R4, R5, R6	Withhold sensitive info	"I avoid sharing CNIC, financial details, or unnecessary access to contacts and camera."	Sensitive data avoidance	Selective Data Sharing
R3, R5, R7	Limit location and microphone access	"I disable location or microphone unless required for core functionality."	Permission restriction	
R1, R3, R4, R6	Only share necessary info	"I provide data only if the app requires it for essential tasks."	Minimal data sharing	

Results

Users actively held back sensitive information unless it was necessary for the core functionality. Generally restricted data included CNIC, financial details, camera, microphone, and location. This demonstrates a cautious and risk-aware approach to app usage. Apps requesting unnecessary sensitive data were negatively viewed, diminishing their chances for adoption. Findings stress that selective data sharing reflects user protective behavior and the need for privacy-respecting design. Developers prioritizing minimalistic data collection, explicit consent, and transparent handling will enhance options for adoption, trust, and retention. Users' selective behavior signifies the importance of ethical, privacy-driven design of apps.

Discussion and Conclusion

Discussion

The study had a principal objective of investigating how practices regarding data privacy affect mobile application adoption in Lahore, Pakistan, mainly focusing on users' perception, trust, transparency, the presence of security measures, and selective data sharing. The qualitative findings from seven semi-structured interviews gave rich insight into the mechanisms through which privacy practices act to shape user adoption behavior and continued usage of mobile applications.

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

The findings indicate that perceptions of privacy practice significantly influence adoption decisions. Participants showed reluctance and lack of comfort when the apps require unnecessary personal information such as location, contact, camera, or microphone, consistent with the finding of the previous research of Akter, Dosono, Ahmed, Kapadia, and Semaan (2020). This becomes a hindrance to adoption since users are very sensitive to potential misuse of data, identity theft, and other forms of information disclosure. Nevertheless, users became receptive if the collection of data was considered necessary for the function of the app. This shows that the users adopted through a trust of necessity, where the users see what the app requires in terms of data. The next finding showed the importance of app ethics to the level of users' perception. Apps with established brands or clear evidence for responsible handling of data were more likely to be adopted, suggesting that the perception extends beyond technical practice to considerations of organizational trustworthiness and credibility. This corroborates Wang, Lin, and Shao's (2025) assertion that users investigate privacy practices not only through policies but also through an assessment of perceived ethical behavior.

This highlights that app uptake, as far as privacy and security standards, goes beyond protection but also depends on the users' sense of control regarding information. "Those applications that provide a finer level of control, opt-in and out, and a clearer understanding about how their consent will be handled, stand a much better chance of achieving better uptake and use."Trust, therefore, became a significant mediating factor linking privacy practices to mobile app adoption. In this regard, the participants reaffirmed that good privacy practices, transparent communications, and clear security measures enhance trust in users and facilitate an installation decision and further use of the app. On the contrary, vague or long privacy policies, unsolicited permissions, and poor security measures have low trust; thus, some users refrain from downloading or uninstall applications. This builds on previous studies (Apau, Titis & Lallie, 2025; Stewart & Jürjens, 2018) which emphasize that trust is a vital ingredient for adoption, particularly in those situations where an app demands sensitive personal or financial information. The present study further expands by elaborating on two facets of trust: as a cognitive and emotional construct; cognitive, in that appraisal of privacy and security measures in an app are involved, and emotional in that there is confidence in the general sense that personal data will not be misused. Participants highlighted that trust was further reinforced wherever the app provided control to the users over permissions, notifications about account activity, and assurance that third-party selling of their data will not be done.

Transparency in privacy communication was again a recurring theme affecting adoption behavior. The participants have preferred a privacy policy that explains the basics of privacy clearly, concisely, and in user-friendly fashion, rather than long technical statements or legal documents. Clear policies limit uncertainty, improve confidence, and favor the decisions to install. The foregoing findings support the assertion made by Kovari (2024) and Patil (2024), which claims that transparency improves informed decision-making and cultivates trust. It is important to note that the study found that transparency goes beyond written policies. Users highly valued

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

contextual expects and just-in-time prompts-such as permission requests closely tied to specific actions (for example, camera access only when taking a photo) providing an additional mechanism to enhance understanding with an ethical signal about responsible app behavior that promotes adoption and sustained engagement.

With respect to participants, high-level security measures such as encryption, two-factor authentication, login alerts, and anonymization were considered important predictors that determined whether users continued using an app. Secure apps raised users' confidence and willingness to engage in the long run, but lack of security led them to abandon the app. This concurs with Kraus, Wechsung, and Möller (2017), who assert that security is a necessity not just technically but psychologically for the users. They also found that visible and comprehensible security practices overall contribute to perceived reliability, trust being the closely knit factor in this regard. When asked about security, participants favored apps that enunciatively shared security measures, stating that security is not merely about keeping data safe but also about signaling incentives for the provider to act responsibility and handle personal information ethically.

Another finding was that users show a tendency toward selective data sharing. Participants stated that they usually withhold sensitive data unless asked explicitly for core app functions. This behavior included limiting access to location, financial information, CNIC, contacts, camera, or microphone. Such selective sharing shows a risk-averse attitude that users maintain to protect themselves from actions of misuse or non-consensual disclosure. This highlights that app uptake, as far as privacy and security standards, goes beyond protection but also depends on the users' sense of control regarding information. Those applications that provide a finer level of control, opt-in and out, and a clearer understanding about how their consent will be handled, stand a much better chance of achieving better uptake and use. This supports literature focused on emphasizing that user empowerment in privacy decisions is a very important factor for technology acceptance and engagement.

Implications of the Study

The results have several theoretical and practical implications:

For App Developers:

Develop applications that need less and relevant information.o Implement effective and strong security measures that should be clear to users.

Provide fine-grained permissioning options and-contextual cues for the use of sensitive features.

For Marketers:

Focus on communication that builds trust and highlights transparent policies and responsible data management.

Use concise, accessible privacy statements that mitigate cognitive load and therefore enhance adoption.

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

For Policymakers and Regulators:
Promote regulations with clear and enforceable privacy standards that are designed for local user concerns.
Promote awareness campaigns educating users on privacy rights and app security.

Theoretical Implications:
It establishes the mediating role of trust between privacy practices and adoption behavior.
Highlights the relationship between perception, security, and autonomy in adoption models for technology.
The adoption frameworks should be coupled with elements of culture and share behavior to make predictions correctly.

Limitations of the Study
The study, however, has limitations that comprise the following:

Sample Size: Only seven individuals were interviewed with the restrainting generality, and sample size allows for more appropriate and representative information.

Geography: The scope of research here is limited to the Lahore, Pakistan, environment; other geographical or cultural settings could possibly present varying concerns of privacy adoption.

Self-Reported Data: The impact of the social desirability bias might affect the underreporting or overreporting of the recklessness behavior in terms of trust to the respondents.

Focus on Perceptions: As it aims to describe perceptions and does not examine the quantity of the app use behavior in reality, the study would not be able to make any prediction about the adoption rate of the same on a larger scale.

Future Recommendations
Areas that could be used for future studies could consider the following:

Enhancing Sample Diversity: Having a diverse group of subjects participate in terms of age, geographical location, and socio-economic parameters to demonstrate a set of perceptions on privacy

Participation in Quantitative Analysis: Utilizing the results of the qualitative study to conduct further analysis of the adoption process through either survey analysis or behavior analysis in an attempt to better understand the influence of privacy policies in the adoption process.

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

Cross-Cultural: They can examine concerns about privacy in relation to the implementation of privacy norms in several countries in different regulatory regimes.
Time longitudinal studies: To establish if there exists observable trust attitude and privacy perception acceleration because of app use over time

Designing Interventions: Conduct privacy-informed intervention designs with consent procedures and educational interventions in order to investigate the effects of the interventions on the adopters as well as the retention of the latter..

Conclusion

This research is has found that personal data privacy practices significantly affect the adoption of mobile apps by users. Privacy perceptions alongside consumer trust in providers, clarity of policies, and robustness of security measures directly interact with autonomy in controlling the data by users and thus influence their installation and use of apps. Findings indicated that suspicions and discomfort created due to excessive or superfluous data requests inhibit adoption while transparency, safe practices, and control within consumers increase trust and confidence.
In the Pakistani context, this study contributes to understanding how privacy-driven adoption behavior is framed. It sports ethical, transparent, and user-centric app development. Privacy could thus be one more area to increasing the level of engagement by users, adoption, and retaining such users over time, combined with strong security and communication strategies. The study demonstrated that integrating technical measures with responsibility-creating, culturally attuned, and empowering users can elicit informed decision-making can build trust.
Consequently, mobile apps that combine function with personalized privacy are much better poised to prosper in highly competitive environments. Ethical design, transparency, and trust-building remain the most enabling factors of adoption while providing actionable insights to developers, marketers, and regulators seeking to enhance user satisfaction and involvement in mobile applications.

References

Acquisti, A., Brandimarte, L. and Loewenstein, G., 2020. Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. Journal of Consumer Psychology, 30(4), pp.736-758.

Adekunle, B.I., Chukwuma-Eke, E.C., Balogun, E.D. and Ogunsola, K.O., 2023. Improving customer retention through machine learning: A predictive approach to churn prevention and engagement strategies. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 9(4), pp.507-523.

Akter, T., Dosono, B., Ahmed, T., Kapadia, A. and Semaan, B., 2020. " I am uncomfortable sharing what I can't see": Privacy Concerns of the Visually Impaired with Camera Based Assistive Applications. In 29th USENIX Security Symposium (USENIX Security 20) (pp. 1929-1948).

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

Al-Harrasi, Z.O.S., 2021. Context-Aware Data Leakage Prevention Theoretical Approach For Mobile-Cloud Computing. Sultan Qaboos University (Oman).

Al-Kfairy, M., Alomari, A., Al-Bashayreh, M., Alfandi, O. and Tubishat, M., 2024. Unveiling the Metaverse: A survey of user perceptions and the impact of usability, social influence and interoperability. Heliyon, 10(10).

Alkhalifah, A. and Al Amro, S., 2017. Understanding the Effect of Privacy Concerns on User Adoption of Identity Management Systems. J. Comput., 12(2), pp.174-182.

Alnajrani, H.M. and Norman, A.A., 2020. The effects of applying privacy by design to preserve privacy and personal data protection in mobile cloud computing: An exploratory study. Symmetry, 12(12), p.2039.

Alrumayh, A.S., Lehman, S.M. and Tan, C.C., 2021. Emerging mobile apps: Challenges and open problems. CCF Transactions on Pervasive Computing and Interaction, 3(1), pp.57-75.

Alsayed, A.O., Ismail, N.A. and Hasan, L., 2024, February. Exploring user perspectives: empowering self-management strategies through semi-structured interviews in the context of mobile app-based approaches. In Proceedings of the 2024 13th International Conference on Software and Computer Applications (pp. 38-44).

Anawar, S., Othman, N.F., Selamat, S.R., Ayop, Z., Harum, N. and Rahim, F.A., 2022. Security and Privacy Challenges of Big Data Adoption: A Qualitative Study in Telecommunication Industry. International Journal of Interactive Mobile Technologies, 16(19).

Apau, R., Titis, E. and Lallie, H.S., 2025. Towards a Better Understanding of Mobile Banking App Adoption and Use: Integrating Security, Risk, and Trust into UTAUT2. Computers, 14(4), p.144.

Ashrafi, D.M., Ahmed, S. and Shahid, T.S., 2025. Privacy or trust: understanding the privacy paradox in users intentions towards e-pharmacy adoption through the lens of privacy-calculus model. Journal of Science and Technology Policy Management, 16(7), pp.1224-1247.

Ashrafi, D.M., Ahmed, S. and Shahid, T.S., 2025. Privacy or trust: understanding the privacy paradox in users intentions towards e-pharmacy adoption through the lens of privacy-calculus model. Journal of Science and Technology Policy Management, 16(7), pp.1224-1247.

Bahar, A., Prananta, A.W., Afifudin, M. and Rahman, R.T., 2024. Mobile App Usability, Data Privacy, Brand Loyalty, and Customer Retention in Indonesia's Online Transportation Services Industry. International Journal of Business, Law, and Education, 5(2), pp.2562-2572.

Balapour, A., Nikkhah, H.R. and Sabherwal, R., 2020. Mobile application security: Role of perceived privacy as the predictor of security perceptions. International Journal of Information Management, 52, p.102063.

Bonatti, P., Kirrane, S., Polleres, A. and Wenning, R., 2017, September. Transparent personal data processing: The road ahead. In International Conference on

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

Computer Safety, Reliability, and Security (pp. 337-349). Cham: Springer International Publishing.

Brandtzaeg, P.B., Pultier, A. and Moen, G.M., 2019. Losing control to data-hungry apps: A mixed-methods approach to mobile app privacy. Social science computer review, 37(4), pp.466-488.

Brannon, G.E., Mitchell, S. and Liao, Y., 2022. Addressing privacy concerns for mobile and wearable devices sensors: Small-group interviews with healthy adults and cancer survivors. PEC innovation, 1, p.100022.

Celestin, P., 2024. How Emerging Data Protection Laws Are Reshaping Digital Marketing And Consumer Privacy Policies.

Chang, K.C., Zaeem, R.N. and Barber, K.S., 2020, October. Is your phone you? how privacy policies of mobile apps allow the use of your personally identifiable information. In 2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA) (pp. 256-262). IEEE.

Dehghanpouri, H., Soltani, Z. and Rostamzadeh, R., 2020. The impact of trust, privacy and quality of service on the success of E-CRM: the mediating role of customer satisfaction. Journal of business & industrial marketing, 35(11), pp.1831-1847.

Distler, V., Lallemand, C. and Koenig, V., 2020, September. Making encryption feel secure: Investigating how descriptions of encryption impact perceived security. In 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 220-229). IEEE.

Gautam, P.K. and Guptar, H., 2024, May. A Security Model for the Enhancement of Mobile Security. In International Conference on Intelligent Communication, Control and Devices (pp. 463-473). Singapore: Springer Nature Singapore.

Hasani, T., Rezania, D., Levallet, N., O'Reilly, N. and Mohammadi, M., 2023. Privacy enhancing technology adoption and its impact on SMEs' performance. International Journal of Engineering Business Management, 15, p.18479790231172874.

Hudson, S. and Liu, Y., 2023. Mobile app users' privacy concerns: different heuristics for privacy assurance statements in the EU and China. Information Technology & People, 36(1), pp.245-262.

Hudson, S. and Liu, Y., 2023. Mobile app users' privacy concerns: different heuristics for privacy assurance statements in the EU and China. Information Technology & People, 36(1), pp.245-262.

Jain, A.K., Sahoo, S.R. and Kaubiyal, J., 2021. Online social networks security and privacy: comprehensive review and analysis. Complex & Intelligent Systems, 7(5), pp.2157-2177.

Jain, S., 2024. Integrating Privacy by Design Enhancing Cyber Security Practices in Software Development. Journal Of Multidisciplinary, 4(11), pp.1-11.

Kalliokoski, K., 2024. Who Knows What They Know—Interplay of Digital Privacy Transparency and Consumer Data Privacy Concerns.

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

Kamin, D.A., 2017. Exploring security, privacy, and reliability strategies to enable the adoption of IoT (Doctoral dissertation, Walden University).

Kovari, A., 2024. AI for decision support: Balancing accuracy, transparency, and trust across sectors. Information, 15(11), p.725.

Kraus, L., Wechsung, I. and Möller, S., 2017. Psychological needs as motivators for security and privacy actions on smartphones. Journal of Information Security and Applications, 34, pp.34-45.

Kununka, S., 2019. User centric privacy policy modelling. The University of Manchester (United Kingdom).

Lee, J. and Hong, I.B., 2019. Consumer's electronic word-of-mouth adoption: The trust transfer perspective. International Journal of Electronic Commerce, 23(4), pp.595-627.

Lie, D., Austin, L.M., Ping Sun, P.Y. and Qiu, W., 2022. Automating accountability? Privacy policies, data transparency, and the third party problem. University of Toronto Law Journal, 72(2), pp.155-188.

Mantovani, E., Antokol, J., Hoekstra, M., Nouwt, S., Schutte, N., Zilgalvis, P., Castro Gómez-Valadés, J.P. and Prettner, C., 2017. Towards a code of conduct on privacy for mhealth to foster trust amongst users of mobile health applications. In Data Protection and Privacy:(In) visibilities and Infrastructures (pp. 81-106). Cham: Springer International Publishing.

Mills, J.L. and Harclerode, K., 2017. Privacy, mass intrusion, and the modern data breach. Fla. L. Rev., 69, p.771.

Mohd Ramsi, M.F., Idris, S.R.A. and Nordin, S.K., 2024. Why digital trust matters to us?. APB Rembau e-Bulletin.

Murmann, P. and Karegar, F., 2021. From design requirements to effective privacy notifications: Empowering users of online services to make informed decisions. International Journal of Human–Computer Interaction, 37(19), pp.1823-1848.

Mushtaq, N., Suleman, S. and Qayyum, A., 2023. Addressing user concerns: A qualitative study on data privacy in mobile banking. Bulletin of Business and Economics (BBE), 12(4), pp.135-140.

Nellore, N., Mishra, T. and Zimmer, M., 2024. Unveiling user perspectives: Exploring themes in Femtech mobile app reviews for enhanced usability and privacy. Proceedings of the ACM on Human-Computer Interaction, 8(MHCI), pp.1-21.

Nowell, L.S., Norris, J.M., White, D.E. and Moules, N.J., 2017. Thematic analysis: Striving to meet the trustworthiness criteria. International journal of qualitative methods, 16(1), p.1609406917733847.

Obaidat, M.A., Obeidat, S., Holst, J., Al Hayajneh, A. and Brown, J., 2020. A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures. Computers, 9(2), p.44.

Oldeweme, A., Märtins, J., Westmattelmann, D. and Schewe, G., 2021. The role of transparency, trust, and social influence on uncertainty reduction in times of

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

pandemics: empirical study on the adoption of COVID-19 tracing apps. Journal of medical Internet research, 23(2), p.e25893.

Pal, D., Babakerkhell, M.D. and Roy, P., 2022. How perceptions of trust and intrusiveness affect the adoption of voice activated personal assistants. IEEE Access, 10, pp.123094-123113.

Patil, D., 2024. Explainable Artificial Intelligence (XAI) for industry applications: Enhancing transparency, trust, and informed decision-making in business operation. Trust, And Informed Decision-Making In Business Operation (December 03, 2024).

Sharma, V., You, I., Andersson, K., Palmieri, F., Rehmani, M.H. and Lim, J., 2020. Security, privacy and trust for smart mobile-Internet of Things (M-IoT): A survey. IEEE access, 8, pp.167123-167163.

Shneiderman, B., 2020. Bridging the gap between ethics and practice: guidelines for reliable, safe, and trustworthy human-centered AI systems. ACM Transactions on Interactive Intelligent Systems (TiiS), 10(4), pp.1-31.

Singh, A.P., Tyagi, M., Vasistha, G., Sikarwar, N., Malik, N., Singh, M.K. and Verma, V.K., 2025. Social media application development. In Applications of Artificial Intelligence in 5G and Internet of Things (pp. 1-6). CRC Press.

SIYADRI, Y. and DEEPAK AKELLA, S.R., 2024. ADVANCING USER-CENTRIC PRIVACY: A COMPREHENSIVE RESEARCH ROADMAP FOR ETHICAL AND SECURE TECHNOLOGY DEVELOPMENT. i-Manager's Journal on Information Technology, 13(3).

Stewart, H. and Jürjens, J., 2018. Data security and consumer trust in FinTech innovation in Germany. Information & Computer Security, 26(1), pp.109-128.

Tsohou, A. and Holtkamp, P., 2018. Are users competent to comply with information security policies? An analysis of professional competence models. Information Technology & People, 31(5), pp.1047-1068.

Wang, E.S.T. and Lin, R.L., 2017. Perceived quality factors of location-based apps on trust, perceived privacy risk, and continuous usage intention. Behaviour & Information Technology, 36(1), pp.2-10.

Wang, X., Lin, X. and Shao, B., 2025. Security and Privacy Protection in Developing Ethical AI: A Mixed-Methods Study from a Marketing Employee Perspective. Journal of Business Ethics, 200(2).

Xing, Y., Lu, H., Zhao, L. and Cao, S., 2024. Privacy and security issues in mobile medical information systems MMIS. Mobile Networks and Applications, 29(3), pp.762-773.

Yadav, O.P., Teotia, R. and Baliyan, R., 2024. Digital Transformation and Consumer Behavior: A Marketing Perspective. Digital Economy of India, 12(2), p.41.

Zalloum, L., Alghadeer, H. and Nusairat, N., 2019. The effect of using mobile banking services applications on electronic word of mouth: The mediating role of perceived trust. International Business Research, 12(9), pp.62-80.

Zhang, P. and Xu, L., 2024. Design and implementation of mobile e-commerce application built on WAP mobile payment system. Wireless Networks, 30(6), pp.6089-6104.