Title:Mobile Application Development, Privacy Protection, and Data Management: Analyzing the Relationship between Applications and Cultural Values

Student Name:XINYUE MA

Student ID number:15516765

Major: Communication Culture and Media

Abstract

With the development of mobile devices, the importance of mobile applications in terms of user privacy protection and data management has become increasingly evident, attracting significant attention from scholars. Currently, factors such as user privacy awareness, relevant regulations, databases, and innovations in technical methods are limiting the development of privacy security and data management in mobile applications. This study aims to address core issues in the field of mobile application privacy security. Specifically, this study seeks to uncover the essence and patterns of excessive collection of user privacy and data by mobile applications, providing new solutions and insights for existing problems. It also seeks to provide valuable references and insights for future research in related fields, thereby promoting the development of relevant disciplines. Based on privacy computing theory, this study analyses the challenges currently faced in mobile application privacy security and data management, including data leakage, unauthorised access and abuse, and limitations on users' right to know and choose. It conducts research in the field of mobile applications from the perspective of ensuring privacy security. The study investigates and analyses measures taken to protect user privacy rights for different types of mobile applications, their respective shortcomings, differences in privacy regulations for the same application across different service regions, and privacy security awareness among users from diverse cultural backgrounds in mobile applications. This paper employs a mixed qualitative and quantitative analysis method to study mobile applications. After combining case analyses and experimental data, the research results and conclusions are drawn. The research findings are expected to drive breakthroughs in the evolution and innovation of mobile application

technology, the transformation and expansion of business models, and the formulation of policies and regulations. This will enhance application performance and user trust while inspiring relevant researchers. Security and privacy are the foundation of trust; while pursuing technological possibilities, users must always be placed at the centre. Future mobile application research will increasingly focus on interdisciplinary integration and addressing emerging technologies.

Keywords: mobile applications, cross-cultural, different countries, privacy security, data management.

Table of Contents

1.Introduction

1.1Research Background

Mobile applications have evolved from simple tools into a core force shaping global social, economic, and cultural interactions. Their significance has permeated the core aspects of social life, economic development, and technological innovation. Over the past few decades, mobile applications have undergone rapid development and transformation. Mobile handheld devices have been widely adopted by a large user base, particularly in the form of smartphones. (Häkkilä, 2006) Smartphones and mobile internet have become an indispensable part of people's lives. There are over 6 billion global smartphone users, and mobile devices have become the primary gateway to the internet, far surpassing traditional PCs. In most developed countries, mobile phone penetration rates have exceeded 100% per capita (with some individuals owning multiple devices). As this trend continues, devices and operating systems are becoming increasingly complex. (Hoehle & Venkatesh, 2015) User privacy and security are being impacted by factors such as technology and the data economy (where app developers, advertisers, data analysis companies, etc., all seek to obtain more user data to gain benefits). The emergence of app stores like iOS and Android has significantly lowered the barriers for users to access apps, while also stimulating developers' innovative enthusiasm, leading to an explosive growth in the number of apps.

However, the associated issues of data breaches and misuse have become increasingly prominent and have gradually drawn the attention of the public and relevant scholars. In recent years, malicious techniques and evasion methods have proliferated in the field of

mobile application privacy security and data management, such as excessive permission requests, exploiting ‘privacy fatigue,’ or using complex interface designs to induce users to consent. Privacy involves an individual's ability to control which personal information is disclosed, when, under what circumstances, and to whom. (Blank, 2014). Although various countries have enacted a series of laws and regulations regarding mobile application user privacy security and data management, the rapid development of technological means (such as artificial intelligence, cloud computing, and big data) has made it difficult for existing laws to keep pace. (Qureshi et al., 2011) Privacy is not only a fundamental right of individuals but also the cornerstone of social stability. The consequences of privacy breaches not only impact individuals' lives but may also trigger societal trust crises. In existing research, scholars have proposed various data encryption, anonymisation, user privacy control, and data minimisation techniques, with numerous research findings emerging. These studies aim to protect the security and privacy of user data through technical means and provide abundant data sources and research tools for exploring technical approaches, application development, and related areas. (Zhang, et al. 2023) However, existing research remains insufficient in the cross-cultural domain. This study aims to conduct a systematic analysis and explore innovations in the fields of mobile application development, privacy security, and data management research, providing new insights and solutions for the theoretical development and practical application of this field. Research in this field not only concerns technological innovation but also profoundly influences the social governance structure and human experience in the digital civilisation era. It holds extremely important theoretical and practical significance for developers to create successful products, businesses to seize commercial

opportunities, policymakers to implement effective regulation, and society as a whole to maximise benefits and minimise risks.

1.2 Research Objectives

This paper aims to discuss how the success of mobile applications on a global scale increasingly depends on the integration of mobile application development and privacy and data security management in an ever-changing and complex cultural and legal context. Therefore, this study has set the following research objectives.

- First, analyse the technical measures adopted by various types of mobile application developers to protect user privacy and identify the shortcomings, as well as the main security vulnerabilities in the applications.
- Second, the study will explore the impact of differing privacy protection regulations across global service regions and countries on mobile applications, including variations in data privacy requirements among cross-border users and differences in user privacy perceptions across cultural contexts.
- Evaluate the influence of cultural contexts on user data security and privacy awareness, including differences in data sensitivity and privacy perceptions. Investigate users' understanding of privacy permissions and user satisfaction levels.

1.3 Research Questions

The following research questions are proposed and discussed in relation to the above research objectives.

- Do current mainstream applications engage in excessive permission requests or violate privacy regulations in their data collection practices? What technical measures are currently widely used to protect user privacy and security? What limitations do these technologies have when addressing complex security threats?
- What significant differences exist in privacy permission practices across different service regions for the same application?
- What specific privacy permission design improvements do users prefer to enhance trust? Do users actively manage or reject application permission requests? What factors (such as age, gender, etc.) influence their behaviour?
- How do users' sensitivities toward data privacy differ across cultural contexts? How do privacy needs and expectations change for cross-border users when using the same application, and how should developers balance legal and cultural requirements across regions?

1.4 Research Gap

Currently, although there is a significant amount of research on privacy protection, including personal information encryption, anonymisation, and user authorisation—three data privacy models—there is little research on the privacy awareness and practices of users from different cultural backgrounds in areas such as technology integration and economics. Against this backdrop, this paper will discuss the impact of different cultural backgrounds on privacy awareness and identify appropriate and universal privacy protection technologies and practices. This study will employ a combination of cross-national questionnaire surveys and

in-depth interviews to collect data on users' attitudes and behaviours toward privacy protection across different cultural backgrounds. Based on this data, the study will analyse the differences in privacy awareness across cultural contexts and discuss the extent to which privacy protection technologies are accepted and the impacts they generate in different cultural environments.

1.5 Significance of the study

The theoretical significance of this study lies in filling the gap in the field of cross-cultural privacy protection, enriching the theoretical framework of privacy protection, particularly the mechanisms underlying the formation of privacy awareness under the influence of cultural differences. Additionally, through a systematic analysis of privacy protection behaviours across different cultural contexts, this study offers new perspectives and research frameworks for the academic community. This research has the potential to bridge the gap between theory and practice in this research area. By measuring users' privacy awareness across different cultural contexts, this study identifies the factors influencing user satisfaction. Furthermore, by integrating existing privacy legal requirements and security technologies, it holds promise for advancing policymakers in developing new strategies.

The practical significance lies in providing feasible solutions for privacy protection practices in the global application of information technology, thereby promoting the effective protection of user privacy rights across different cultural contexts. Through this research, it can help technology developers, policymakers, and businesses better understand and respect user privacy needs, thereby enhancing user trust and experience in cross-cultural applications.

Barbosa observed that being able to declare a company or application as “privacy-friendly” may be a competitive advantage.

1.6 Dissertations’ Structure

To better present the research, this paper is divided into five sections:

- Introduction: A detailed discussion of the research objectives, background, questions, gaps, and significance.
- Literature Review: An analysis of the measures taken by different platforms to protect user privacy rights and their respective shortcomings. An examination of user satisfaction and awareness of privacy rights across different countries and cultural backgrounds. A comparison of privacy regulations for the same application across different service regions, etc.
- Research Methods: Collect specific data through data analysis, case studies, and survey questionnaires, and analyse the results to draw conclusions.
- Analysis of Research Results: Clearly state the conclusions drawn from the data and analyse the achievement of research objectives.
- Conclusion: Discuss future trends in privacy protection technology.

2.literature review

2.1.Introduction

Currently, mobile internet and technology are developing at an unprecedented pace, with many mobile applications now boasting billions of users worldwide. (Nikkhah et al., 2025) As technology advances, numerous smartphone applications collect user data that exceeds the scope of their functional requirements. (Miltgen & Peyrat-Guillard, 2014) Privacy, security, and data management issues are increasingly intertwined with how people use the internet and smartphones, paralleling the progress of mobile devices and location-based technologies. (Zhao, 2018) To provide high-quality services, mobile applications need to collect user location, personal preferences, gender, age, interests, and other data information (Pentina et al., 2016). Additionally, they can track users with very high accuracy while supporting efficient storage of mobile data in data warehouses. (Gkoulalas-Divanis, 2018) In recent years, privacy leaks and misuse issues have become increasingly prominent in the collection and processing of user privacy data by mobile applications. This chapter aims to analyse the theoretical foundations related to mobile application privacy security and data management. It is divided into several themes, systematically analysing and researching mobile application privacy security, relevant legal provisions, different application regulations, and combining existing literature to propose solutions and ideas. The current main challenge is how to balance user experience with protecting user privacy, which has become a critical issue. Users' privacy expectations are not uniform; for example, users are more sensitive about privacy data related to banking, healthcare, and contact lists, but they prefer more accurate and personalised data collection for navigation and weather-related services. All types of

software fundamentally rely on a large amount of user data to function. A scholar has proposed adopting the principle of data minimisation as an operational guideline. ‘Minimise the amount of personal information collected by service providers, such as reducing the risks associated with analysing and tracking users.’ (Kaaniche, 2020) While existing literature contains extensive research on mobile application technology and comparative studies of applications, there is limited research on the integration of application privacy regulations and related policies across different countries and cultural contexts. This chapter will conduct extensive literature reviews on the aforementioned topics.

2.2. Mobile application development

After analyzing relevant literature, it was found that mobile applications are a relatively new topic in information research, primarily divided into two main research areas: application development, and mobile application security and privacy. Currently, existing literature in the mobile development field primarily focuses on Apple and Android systems. This chapter primarily analyses the current status of two mainstream application development and privacy control methods and permission management. As of May 2021, the Android system accounted for over 75% of the market share, with the iOS system occupying the second-largest market share. (Yadav, 2022) However, Yang argues that these big data applications pose significant privacy issues. Neither Android nor iOS applications fully comply with their privacy policies in terms of data processing methods. (Kununka et al., 2017) First, both iOS and Android provide a public marketplace—the App Store and the Android Market, respectively—but they adopt fundamentally different approaches to restricting malware on devices. (Miller, 2011) iOS provides sandbox protection for applications.

However, this design decision violates the principle of least privilege, potentially leading to critical privacy and security vulnerabilities, allowing applications (whether benign or malicious) to access contacts and photos. In recent times, several (legitimate) applications have been found to abuse these permissions, such as uploading the entire contact list to the application developer without user consent. (Werthmann, 2013) This could lead to the exposure of personal privacy, triggering a series of chain reactions such as identity theft and financial loss.

The Android system is open source, and its app store offers multiple distribution channels. An increasing number of smartphones are based on the Android platform. Thanks to Android's open source kernel policy, malware developers can gain a deeper understanding of the mobile platform. (D et al., 2015) 28% of mobile web applications had at least one security vulnerability. The Android system allows users to install third-party applications, but some of these applications contain a large amount of advertising. While advertising typically enables users to use software for free, the data collection and tracking associated with it are also considered a threat to personal privacy and may infringe upon users' data protection rights. (Kollnig et al. 2021). Sales statistics from 2017 show that 86.1% of mobile phone users are using the Android operating system. There are ten different versions of the Android operating system, and each version's Android operating system API differs in terms of functionality and security. (Haq & Khan, 2021) Khatoon also noted that many ‘free’ applications often request unnecessary or redundant permissions, typically for the purpose of collecting valuable user data. A recent survey report revealed that 267,259 applications infected with malware have been identified, with 254,158 of them on the Android platform. It also indicated that the

number of malware in applications has increased by 614% since 2012. (He et al., 2015). Stevens found that some ad libraries check and exploit permissions beyond their privacy policies. The privacy threats posed by libraries automatically extracting and sending new information are significant. The openness of the Android system allows for a variety of novel and interesting tools in app stores, but devices running Android 7.0 or earlier are easily vulnerable to phishing software or malicious programs. Sierra noted that, during the development of mobile apps, hackers have employed numerous techniques to analyse and modify Android developers' apps. Attackers are modifying app content to exploit unsuspecting users. These attacks severely compromise system security. Additionally, Tsavli argues that in the Android system, when an app is installed, users are prompted to approve the permissions requested by the app. Users cannot “negotiate” or customize access and usage options. The requirement that app users must accept the app's terms and conditions in order to use the app may be viewed as intrusive behavior. (Wottrich et al., 2018)

This situation is not limited to the Android system; some applications also have similar requirements. For example, WeChat requires users to create an account to use its services. (Jia et al., 2020) When users register for a WeChat account, the ‘Tencent WeChat Software Licence and Service Agreement’ is typically presented as part of the registration process, requiring users to read and agree to the privacy agreement before continuing with the registration. Furthermore, during the account registration process or while using the service, users are required to provide certain necessary information, such as account registration services, user identity verification, mobile phone number entry, consent to use geolocation information for certain features, and authorisation to access the mobile phone contact list for

the contact list matching feature. When users register a Taobao account, they must read and agree to the privacy policy to continue with the registration process. The consent method may include checking a consent box or clicking the 'I have read and agree' button. The consent content includes the 'Taobao Platform Service Agreement,' 'Privacy Policy,' 'Alipay Registration-Related Agreements,' and other terms, but the agreement does not specify which terms are referred to as 'other.' Terms that exempt or limit liability will be highlighted in bold underlined text, and users should pay close attention to these terms.

Degirmenci conducted a study to understand the varying access permissions of different types of mobile applications, analysing 12 distinct mobile applications across categories such as social media, mapping, communication, and gaming. After analysing data from four dimensions of privacy information collection (personal identity, location, and system and network settings), he concluded that the extent of personal information collection significantly influences users' concerns about privacy. Additionally, users' gender and age also have a significant impact on their privacy concerns. For example, younger users exhibit a more proactive attitude toward data management, feel more responsible, and have greater confidence in their ability to prevent potential data misuse. (Miltgen & Peyrat-Guillard, 2014). With the rapid development of technology, an increasing number of people are willing to accept data sharing and privacy compromises, prioritising convenience and efficiency as more important considerations. Wottrich concluded from experimental results that the perceived value of an application outweighs concerns about privacy issues.

2.3. Mobile Application Privacy Security and Data Management

Regarding security and privacy issues in mobile applications, research typically focuses on the calculus theory of location service information/privacy and privacy computing theory. Privacy computing theory refers to a computational approach that analyses and processes data using algorithms and technical means while simultaneously protecting data privacy. It is the core classical theory in the study of privacy behaviour. (Zhu et al.2022). Its scope encompasses multiple aspects such as information collection, storage, processing, distribution, and destruction, and it provides various privacy protection solutions for typical scenarios such as social networks, location-based services, and cloud computing. (Li et al. 2019) The ultimate goal of privacy computing is to achieve automated execution of privacy protection, establish system design theories and architectures that support a large number of users, high concurrency, and efficient privacy protection, and enable effective combinations of different algorithms. (Li et al., 2024). Based on privacy computing theory, MUIPC analysed users' concerns about privacy in mobile applications from three dimensions (perceived monitoring, perceived intrusion, and secondary use of personal information) (Degirmenci et al., 2013) and drew conclusions. The level of concern regarding privacy security and data leakage in mobile applications varies significantly across different user groups, particularly between those with strong privacy awareness and those with relaxed privacy awareness. Users' concerns about privacy in these mobile applications extend beyond data collection itself to how data is stored, shared, and utilised throughout the entire process. These concerns have become increasingly pressing in today's rapidly advancing mobile technology landscape. In recent years, as the academic community has increasingly prioritised privacy issues, privacy calculus theory—a calculus-based theory for measuring users' psychological perceptions of privacy—has gained

widespread application, becoming the most core and classic theory in privacy behaviour research. It is grounded in economic utility maximisation theory, social psychology's social contract theory, and social exchange theory. It emphasises that individuals differ in their willingness to disclose personal information to gain benefits. (Zhu et al., 2022).

2.4.Differences in privacy and security across service regions

To propose a concept and method for addressing user privacy and security in mobile applications, this study analysed and discussed mobile applications across different countries, types, and cultural contexts. After reviewing existing literature, Jia found that the same mobile application has differences in its privacy service terms for domestic and international users. Tiara, after carefully examining and evaluating Douyin's data privacy policy and application privacy settings from a data subject-centric perspective, found that Douyin has not fully implemented the content of its privacy policy and application settings. Although Douyin (well-known to Chinese users, available globally since its acquisition in 2018) and TikTok are both part of the ByteDance brand, they exhibit significant differences in terms of audience service and cultural context (Sandoval et al., 2023). Douyin primarily serves the Chinese market, while TikTok targets global users, particularly in Europe and the Americas. As an international company, its privacy protection policies vary across different countries and regions. Unlike TikTok, Douyin's terms of service include provisions prohibiting activities such as subverting the government, overthrowing the socialist system, inciting separatism, or undermining national unity, which are not present in TikTok's regulations. This has, to some extent, exacerbated the uncertainty surrounding user privacy protection. In terms of privacy security and data management, while TikTok's privacy agreement clearly

outlines the data access and utilisation methods of TikTok partners, third-party service providers, and their users, studies have identified specific issues related to data analysis on Douyin, which have raised additional privacy risks. (Syamsuar et al., 2024) However, in actual implementation, data abuse remains severe. TikTok was fined $5.7 million in February 2019 for violating the Children's Online Privacy Protection Act. (Jia, 2020) Additionally, TikTok may excessively share user data with third parties for purposes such as advertising and market research. Such behaviour infringes upon users' privacy rights.

2.5 The Relevance of Applications and Cultural Values

This chapter examines whether the concept of ‘privacy’ varies across different cultures. These differences include packaging requirements, functional space, quality expectations, app store dependency, price sensitivity, and so on (Lim et al., 2014). The concept and importance of privacy vary significantly across different cultures. Li found that the context and focus of privacy issues differ between individualistic and collectivist countries in our sample. Cultural factors at the national level highlight the importance of advocacy culture in influencing the relationship between usability structure and continued usage intent. (Hoehle et al., 2015). Some collectivist cultures may view privacy as individualistic, while others may place greater emphasis on personal freedom and privacy as an inviolable fundamental right of the individual. Different social structures, histories, or values can greatly influence the concept and practice of privacy. Through cross-cultural research, we can discover how privacy varies and conflicts globally, as well as the differing expectations of individuals and societies across cultures. There are significant differences in privacy management between cultures, such as

packaging requirements, functional needs, quality standards, app store independence, and price sensitivity. Different cultures lead to varying attitudes and behaviours toward privacy. For example, people in some regions may be more inclined to openly share their personal information, while others may be highly sensitive about sharing such information. Therefore, global privacy protection policies in a globalised context cannot be a one-size-fits-all solution but must be culturally adaptive. Additionally, the digital context blurs the boundaries of privacy, presenting a challenge in how to effectively protect personal privacy while respecting cultural differences. Li found that the cultural context and focus of privacy issues vary between individualistic and collectivist countries in our sample, with national-level culture emphasising the importance of cultural endorsement in influencing the relationship between usability structure and continued usage intent. EU users view privacy as a fundamental human right and are protected by relatively robust privacy regulations, such as the EU's General Data Protection Regulation (GDPR), which aims to protect users' online information privacy. (Hudson & Liu, 2023) It sets a benchmark for global privacy laws, prompting many multinational companies to elevate their global standards. At the federal level, there is no unified and comprehensive privacy law system, with states enacting related regulations in their respective domains.Users from the UK and Canada are more likely to be influenced by price. Users in Europe and the US (highly individualistic users) have high expectations regarding their rights to manage their own data and make independent decisions. Users are more likely to question the purpose of data collection and actively exercise their rights to delete or object. Users from the US are more likely to download medical applications and prefer self-regulation, free markets, and consumer rights protection in the

mobile industry. Users in East Asia/certain Asian countries (highly collectivist) may be more concerned with the convenience of mobile app services, social harmony, or the interests of the state/organisation. Acceptance of data collection by governments or large platforms may be relatively high, especially in countries with strong government influence. Understanding mobile app users' attitudes toward information privacy issues in different cultural contexts will help mobile commerce businesses better serve global consumers. (Chen et al., 2013) Peltonen demonstrated that app usage is related to cultural values. (Cho et al., 2018) Attitudes toward software vary across cultural contexts; simultaneously, software is influenced by various social factors such as values, gender, and age, thereby altering its application methods. The impact of these cultural differences is not only reflected in users' acceptance of applications, but also in their demand for privacy protection and preference for personalised services. For example, in some Western countries, individualistic cultures emphasise personal freedom and privacy, leading users to approach data collection and usage with caution and prefer applications that prioritise data security. In contrast, collectivist cultures in some Eastern countries prioritise collective interests and social harmony, meaning users may be more willing to sacrifice some privacy in exchange for more convenient services or more efficient allocation of social resources. These cultural differences not only influence users' choices when using technology products but also profoundly impact companies' strategies in global markets. For instance, international companies often need to adjust their privacy policies and data management practices based on the cultural context of different regions when designing cross-border applications to meet local users' expectations. Additionally, this has prompted technology companies to

place greater emphasis on cultural adaptability in their globalisation efforts to gain users' trust and support across multiple markets.

2.6. Conclusion

This paper examines the role and impact of rapidly advancing technology in the development of mobile applications, as well as the various phenomena related to mobile application privacy, security, and data management. The development of mobile applications is influenced by numerous factors and plays a significant role in enhancing the convenience and efficiency of users' lifestyles. This chapter conducts a detailed discussion on the occurrence of privacy leaks and abuses in mobile applications, as well as their impact on user experience, by analysing relevant privacy regulations and existing literature. The research findings in this chapter provide valuable references for the development of the mobile internet sector and offer insights and methodologies for technical research and development personnel engaged in related studies and projects. As indicated by the aforementioned research, existing literature primarily focuses on technological or theoretical advancements and comparative studies of applications.

3.Research Methodology

3.1 Introduction

This chapter investigates users' awareness of privacy security across different regions of the world. A questionnaire survey was designed to measure the familiarity and application of privacy protection measures among people in various regions, their habitual behaviours in daily life, and their concerns about data breaches. The study compares and analyses differences in cultural backgrounds, legal frameworks, theprevalence of information technologies such as the internet, and people's attitudes and behaviours toward privacy protection. It is anticipated that through the questionnaire survey and a summary of relevant domestic and international literature, this chapter will explore the current challenges faced by China and propose policy recommendations: strengthening policy guidance; enhancing legal constraints; reinforcing security education; improving information security awareness; and improving information sharing. This chapter will discuss experimental design from the perspectives of research methods, questionnaire design, data analysis, and ethical considerations.

3.2 Research methods

Common methods include qualitative, quantitative, and mixed methods (Dane, 1990). To address the issues raised in the preceding section, this study employs quantitative methods and a combination of technical, legal, and cultural approaches. Quantitative methods can utilise user surveys and behavioural analysis to understand differences in user acceptance and demand for different privacy permissions across regions and cultures. Experimental designs can simulate user behaviour under different privacy requirements, such as altering privacy

permission requests and recording whether users adjust their permissions or reject certain requests. Additionally, data analysis can assess differences in privacy security needs among users in various regions, thereby providing privacy-optimised design recommendations for mobile application developers. Finally, the study analyses and summarises findings based on existing research, theoretical foundations, and experimental data.

3.3 Questionnaire Design

To explore the above issues and obtain users' psychological expectations and preferences regarding privacy security, a questionnaire survey method (based on privacy computing theory) was adopted to collect information on users' perceptions of privacy permission requirements, behaviours, and attitudes towards cultural differences, ensuring that the sample covered different regions, ages, genders, educational backgrounds, usage frequencies, and usage times. This approach allows us to observe the distribution of the sample, ensuring data generalisability and representativeness, while also facilitating an understanding of the basic characteristics of the sample and user usage patterns. A stratified multi-stage sampling method was employed: First stage: divided by region (e.g., EU, UK, China, and Singapore). Second layer: Within each jurisdiction, samples are stratified by age (18-25, 26-40, 41-60) and gender using proportional sampling. The questionnaire collects comprehensive data from multiple angles, including user permission management behaviour, privacy expectations, and cultural values. The questionnaire aims to break through the limitations of single-dimensional research by integrating technology, culture, and law for comprehensive analysis.

3.4. Data analysis

Data collection is essentially a source of information required for research questions after appropriate design. When research is necessary, data collection is crucial. The purpose of data collection is that, without gathering certain information, privacy issues in research will increasingly become a globally significant concern as digitalisation advances. (Mazhar, 2021) Users' sensitivity and awareness of privacy vary depending on regional cultural influences. In Europe and the Americas, users tend to be more sensitive about privacy. Due to stringent data protection regulations such as the European Union's General Data Protection Regulation (GDPR), users' rights regarding data privacy are more comprehensively protected. However, due to differences in national conditions, social cultures, and other factors, there may be variations in the level of privacy sensitivity across regions, as well as differences in awareness and standards of data protection between regions.

3.5 Research Philosophy

In the field of academic research, research philosophy, design, and methodology occupy a crucial position. They constitute the core beliefs that guide research design and implementation, and the differences between research philosophies provide us with multiple possible paths for understanding scientific research. This paper aims to reveal a research philosophy centred on ‘human beings’ and emphasising the subjectivity of human beings. This research follows the principles of humanism. It combines empirical analysis and historical examination to reveal the significance of positivist methodology for scientific practice and social science research. Positivism involves the question of the rationality of the views put forward. It can study this phenomenon through actual experience, experiments, or

observations in specific contexts, but to accurately describe the essence of this phenomenon, it still relies on the scientific concepts or theories proposed by researchers for objective processing. Without these scientific concepts or theories, it is impossible to obtain research results that correctly reveal the true causes behind this phenomenon. Therefore, scientifically designing experiments or observations is crucial, as this will determine which specific data the research will cover. This paper will introduce some basic concepts regarding scientific hypotheses and how to use these concepts and theories to describe scientific facts. Positivism is employed to explain a scientific method based on experiments and statistics, which aims to study specific aspects of society through social experiments and measurements. This paper discusses the distinction between positivism and statistics and how statistical tools can be used to explain these differences. (Mbanaso, 2023)

3.6 Ethics

Ethical Issues: In addressing ethical issues that arise during the survey, we adhere to a people-centred principle to protect the privacy and choice rights of survey participants. Any data processing involved in the survey must be transparent, while ensuring data security. The questionnaire first explains the purpose, analysis of use, and anonymisation of data after the survey, requiring participants to tick a box to indicate consent. No IP addresses, names, or other identifiably traceable records are collected; only demographic data groups are recorded. Sensitive or leading questions are avoided as much as possible. At the end of the questionnaire, participants are recommended to contact psychological counselling organisations. Additionally, the homepage explains the use of data and anonymisation

processes, and provides an option to skip sensitive questions. The study must ensure data anonymity, confidentiality, and informed consent from research participants; risks of infringing on user privacy must be avoided. Additionally, for the ethical challenges faced in cross-cultural research, the design of the survey questionnaire and interview content must be carefully considered to avoid cultural biases and misunderstandings.

3.7. Conclusion

This chapter employs quantitative research methods to analyse and explore users' acceptance levels and demand differences for various permissions of mobile applications across different regions and cultural backgrounds through questionnaire surveys. Quantitative research can utilise objective, quantifiable data to reveal patterns in user behaviour and privacy preferences. This study systematically investigates the impact of privacy permission settings on user decision-making through user surveys, behavioural experiments, and analysis, and provides recommendations for privacy-optimised design to mobile application developers. The primary objective of this study is to explore regional and cultural differences in users' acceptance of privacy permissions. Quantitative methods can quantify the relationships between different factors (such as privacy settings, user behaviour, and culture) by designing structured questionnaires, observing, and analysing large-scale data. Simulated experiments are designed to record users' behavioural responses (e.g., whether they modify permissions or refuse authorisation) when faced with different permission requests while using mobile applications, thereby understanding users' decision-making patterns. Using methods such as cluster analysis, analyse underlying patterns in user behaviour data, such as which

permissions are more likely to be accepted by users and which factors lead to users refusing authorisation. Apply Hofstede's cultural dimensions theory (such as individualism and collectivism, uncertainty avoidance, etc.) to explore how cultural differences influence users' perception of privacy risks and permission decisions. The research findings may provide data-driven optimisation recommendations for mobile app developers.

4.Research findings and discussion

4.1 Introduction

A total of 180 survey questionnaires were distributed evenly across four countries: the European Union, the United Kingdom, China, and Singapore. The survey targeted three age groups: 18 to 25 years old, 26 to 40 years old, and 41 to 60 years old. The survey focused on privacy security and data management in mobile applications. A total of 180 questionnaires were distributed, with 161 valid responses received.

4.2. Descriptive Analysis

4.2.1 Demographic Research

Demography is the study of population size, structure, distribution, and patterns of change. Through demographic analysis, governments can formulate reasonable social policies and optimise resource allocation, thereby promoting sustainable social development. Figure 1 shows statistical data on the age and gender of respondents.

Table 1

	18-25 years	26-40 years	41-60 years	
				total
man	22	23	07	52
woman	11	75	23	109
total	33	98	30	161

From the above table, we can see that there are 161 people in total, with middle-aged people accounting for the majority. There are 98 middle-aged people in total, while there are only 33 people aged 18 to 25 and 30 people aged 21 to 60. There are nearly twice as many women as men in the survey sample. There are 109 women in total and 52 men.

4.2.2. Descriptive analysis

Table 2

Please answer the following questions according to the following scoring criteria: 1-Strongly

disagree 2-Disagree 3-Neutral 4-Agree 5-Strongly agree (This questionnaire is conducted anonymously, so the privacy information of the respondents will not be disclosed)					
	1	2	3	4	5
Privacy leakage of mobile applications					
Have you encountered the following privacy security issues?	75	21	22	30	13
Have you ever encountered an application that frequently asks for permissions unrelated to functionality?	41	11	08	31	70
Have you received harassing ads/scam messages related to the use of the app?	21	19	55	32	34
Do you find most app permissions confusing and difficult to understand?	77	31	06	26	21
Do you use ios often?	101	11	20	09	20
Do you use Android?	54	22	28	24	33
Different countries and service areas					
If you have used the same app in different countries, do you feel the privacy policy is different?	11	41	33	22	54
Do you think users attitudes to privacy are different in different regions?	34	33	01	42	51
Do you think Asian users are more receptive to data exchange for convenience?	02	28	44	35	22
Do you think users in developing countries have a low awareness of privacy risks?	20	47	32	27	35
User privacy awareness					
Do you often refuse to grant non-essential permissions?	39	42	10	21	43
Do you regularly check your app permissions	56	22	33	43	7
Will you uninstall apps with vague privacy policies?	08	11	76	12	54
Did you report an app that collected excessive data to the platform?	93	06	33	20	09

If an app is free but requires you to watch ads, would you voluntarily refuse it?	43	26	43	58	34
Are you concerned about privacy leakage?	12	22	23	16	88
Do you think privacy laws are important?	41	11	09	45	55

Researchers used five different levels of the same degree to assess the psychological state of respondents. From number one to number five, there are five different levels: the first represents extreme opposition, the second represents opposition, the third represents a neutral attitude, the fourth represents agreement, and the fifth represents extreme agreement. Within the same dimension, the higher the composite score, the higher the respondent's acceptance of the issue. This table delves into users' views on privacy protection and data management, as well as their dissatisfaction, across different national cultural contexts. The first part focuses on privacy leaks in mobile applications, while the second part of the literature review delves into related literature. The second part explores differences in privacy regulations for applications across different countries and service regions, and assesses the depth of these differences through a questionnaire survey. In the second part, we primarily examine whether respondents have sufficient awareness of privacy, whether they would proactively report non-compliant data collection practices, and their sensitivity to privacy management. By combining cross-country and regional data, we analyse differences in individualism and collectivism in the context of trading personal privacy for advertising.As can be seen from the survey chart, users in Europe and the United States are most concerned about government and corporate surveillance of users, and are highly averse to being monitored and having their data used. In contrast, users in Asia have less stringent privacy requirements, and in some regions, the pursuit of convenience outweighs data exchange. From a behavioural perspective,

users in developing countries have a very low level of respect for privacy. One reason for this is that many developing countries do not have a clear definition of privacy. An increasing number of users are becoming aware of privacy risks and are beginning to care about how to monitor and protect personal information. Survey results show that most respondents are concerned about whether mobile applications protect users' privacy and security. In particular, users in Europe and China have the highest level of concern about data breaches and the misuse of personal information. Additionally, while most people believe they should pay for higher-level privacy monitoring, a significant portion still distrust current policies due to unclear terms and a lack of security awareness. In the UK and Singapore, despite similar concerns, users are more trusting of data usage, reflecting how legal and cultural contexts influence privacy perceptions across regions. Surveys found that most mobile apps request irrelevant permissions, misuse data, and have opaque privacy terms. Chinese users have the lowest understanding of permission explanations (44.82%) and the highest rate of refusing unrelated permissions (77.58%), while European users are more concerned about government or corporate monitoring of app data. Which types of apps cause the most privacy intrusions in different regions and among different users? The most commonly used social networking and e-commerce shopping apps, as well as financial services apps, are the most intrusive in terms of privacy. Individualistic cultures (such as those in Europe and the United States) are more likely to refuse to install apps that require unnecessary permissions, while collectivist cultures (such as those in Asia) are more willing to sacrifice some privacy for convenience. 63.79% of Chinese users have encountered harassing ads or spam messages, but some users are still willing to accept a certain degree of data exchange in exchange for higher efficiency and

better services. People in developing countries have low levels of privacy education and awareness, necessitating improvements in risk awareness through education and legal regulations. Although most respondents stated that they highly value privacy, their behaviour often diverges significantly from their attitudes. Young users (18-25) have a weak understanding of privacy issues but are also the most likely to uninstall apps with unclear privacy terms. The uniqueness of young users: 18-25 users have weak privacy awareness (only 25% of users read privacy terms) and the strictest requirements. Middle-aged and elderly users have higher demands but lack basic skills, thus facing higher risks. Analysis based on the privacy calculus theory indicates that whether people disclose information is based on their assessment of benefits and risks, rather than simply determined by culture or law. Widespread abuse of permissions: 73% of users in Asia have encountered apps requesting irrelevant permissions (e.g., gaming apps requesting access to the address book). Privacy policies are opaque: 58% of users in Singapore find permission explanations obscure and difficult to understand (especially Chinese users, with only 44.8% understanding). The survey results reveal a privacy paradox: 80% of EU users are concerned about privacy leaks, but only 30% regularly check permission settings. Risks in developing countries: Low privacy awareness (63.8% of users in Asia encounter harassing ads) and insufficient legal protection. Individualist cultures view privacy as a basic human right and pursue data autonomy (52% of EU users exercise their right to delete data). Collectivist cultures prioritise service convenience (71% of users in Asia accept ad tracking for free services).

4.3 Discuss

The discussion on privacy protection must strike a balance between digital culture, legal requirements, and individual rights. Only then can privacy protection issues be resolved within the global digital ecosystem and trust be established. This survey was conducted via a questionnaire to explore how users in different regions and of different types perceive and use mobile applications, as well as their concerns and experiences regarding privacy violations. The survey results show that users are highly concerned about privacy violations, but attitudes toward such violations vary significantly across regions and user types. The survey found that many users are deeply concerned about privacy violations. Users generally believe that such violations are widespread. The level of concern about privacy violations varies by region and user type. Opinions on privacy regulations such as the GDPR are mixed. Some users believe that privacy regulations have helped businesses improve their privacy protection standards. Others believe that privacy regulations are not being properly enforced by businesses or that these regulations only apply to a small portion of businesses. Users in different regions also have differing attitudes toward privacy violations. While many users express concerns about privacy issues, they are willing to make few concessions. Few users carefully read and manage permission requests. Few users uninstall apps with vague privacy terms or those that collect large amounts of data. Few users report apps that violate user privacy or collect large amounts of data. Asians are more tolerant of free apps that require users to watch ads. Although users express concerns about privacy violations, they are willing to make few concessions for convenience. Users value privacy but are willing to sacrifice some privacy rights for convenience. The presence of harassing ads and fraudulent information suggests that user data may be shared or sold. Some apps

offer free services and then profit from ads and data. Users are angry about privacy violations but still compromise for the sake of convenience. Survey results show that some users find privacy policy terms difficult to understand, with a large number of legal or technical terms deterring users. Users agree to the collection of personal information without fully reading and understanding the terms, thereby losing control over their personal data. This survey highlights various issues related to privacy and security violations in mobile applications. These include privacy leaks, abuse of permissions, and obscure terms and services. Users' concerns about privacy and their own behaviour also vary by region, and there are some puzzling contradictions. Developers, users, regulators, and technical experts must collaborate to address privacy security violations. Through improved privacy policies, enhanced user awareness, stronger enforcement, and innovation, a safer, more open, and transparent mobile app ecosystem can be established. Privacy is not merely a technical issue but also a social one. Only when privacy is safeguarded can mobile apps truly serve users and thrive.

5. Recommendations and Conclusion

5.1 Recommendation

Based on the above research, the following are some recommendations for strengthening user privacy protection and management in mobile applications across different regions and

markets. We recommend that privacy policies of major platforms should place greater emphasis on users' right to understand and choose, with content that is simpler and clearer. We suggest that platforms should enhance transparency, clearly stating in their privacy policies what user data the app will collect and how it will be used. Ambiguous or unclear terminology should not appear in privacy policies. Strict compliance with local regulatory requirements must be maintained. Data privacy (GDPR, CCPA, PIPL, etc.), content requirements, payment, age verification, etc. Content compliance should be a top priority. Consult local legal advisors for compliance review. Conduct rigorous optimisation for mainstream devices and networks in target markets. The app should run smoothly on low-spec devices and support offline functionality for core modules in weak or disconnected network conditions, such as content caching, offline features, and offline messaging. Intelligently control data consumption. Address cultural needs in different markets by allowing users to choose their privacy settings. When promoting privacy protection, tailor promotional methods to the cultural level and background of different markets. Marketing materials and content should align with local cultural contexts to avoid cultural appropriation or offence. When using colours, images, icons, and character designs, consider their cultural meanings; they should be positive and unambiguous. At appropriate times, incorporate local festivals or events to engage users and enhance the festive atmosphere, such as Double Eleven, Diwali, and Ramadan promotions. The app’s copy, notifications, and interactions should align with local users’ communication styles and emotional expectations. From core functionality to subtle cultural experiences, every detail requires careful refinement. Avoiding cultural stereotypes requires thorough user research and continuous local testing. Users

should enhance their privacy awareness, regularly review app permissions, and read and understand privacy policies before installing apps. Governments and businesses should collaborate to help users better understand and utilise relevant regulations, enabling them to use digital services with greater confidence. Platforms and governments should advocate that ‘privacy is a fundamental right.’

5.2. Conclusion

Current mainstream privacy protection technologies have certain limitations and are often used in scenarios with high security requirements. For example, the open-source nature of the Android system has led to the proliferation of malicious software, while the sandbox environment of the iOS system may also result in user privacy leaks due to design flaws. Research articles suggest that designers should adopt the principle of data minimisation, streamline permission requests, and enhance users' visibility and control over such requests. Additionally, designers should strengthen the integration of technical and legal measures, as laws and regulations in different regions significantly influence app design. The same app may have different privacy policies in various countries. For instance, there are differences in certain data management clauses between Douyin (the Chinese version) and TikTok (the international version). Research articles suggest that designers should strictly comply with local laws and regulations, utilise local legal advisors for compliance reviews, and promote the standardisation of privacy standards globally. Regarding the issue of mobile applications infringing on user privacy and users' privacy rights, we have reached a point where we have no choice but to tolerate such infringements. This is not a technical issue but a systemic, cultural, and economic issue. People in low-income regions are forced to bear the

consequences due to a lack of awareness. For instance, based on privacy calculus theory, survey results indicate that individuals may disclose their private information when the perceived benefits of disclosure are at least equivalent to the perceived risks. However, any disclosure entails the loss of personal information. Yet, as long as the risks are manageable and there is sufficient income, individuals are likely to accept such losses. Privacy protection in mobile applications is a multi-dimensional, dynamic process that relies on the joint efforts of technology, law, and culture. The study calls on developers, policymakers, and users to jointly create 'privacy-friendly' environments, balancing technological innovation with user needs, and providing sustainable solutions for privacy security in the digital age. Any disclosure of information means the loss of personal data.

5.3 Limitations of the study

The limitations of this study include the fact that the questionnaire survey was not sufficiently in-depth to reflect underlying motivations and emotions, nor could it adequately capture differences in basic privacy habits among different groups. It was unable to explore the underlying causes and motivations behind privacy violations. The observed behavioural differences may not be due to cultural values but rather other factors. User habits may be influenced by popular apps in the local market rather than cultural preferences. It could also be because the mainstream apps in the respondents' countries or regions operate in this manner, rather than due to inherent cultural factors. Additionally, quantitative research relies heavily on the availability and validity of data, which may not accurately reflect reality and instead oversimplify it. Economic development levels determine users' payment capabilities. As a result, our research findings were mistakenly interpreted as cultural rejection. Since this

questionnaire was prepared in both Chinese and English versions, and the researcher is not a native English speaker, translation quality issues led to experience problems, which were mistakenly interpreted as cultural rejection in the research findings.

‘Culture’ is often studied using national borders as cultural variables (e.g., ‘Chinese users,’ ‘American users’). This obscures the significant subcultural differences within countries: region, ethnicity, age, education level, socioeconomic status, urbanisation level, etc., can all lead to significant differences (e.g., the differences between elderly users in first-tier cities and third- or fourth-tier cities in China may be greater than those between some young people in Europe and the United States). Moreover, within the same cultural group, individuals' values, technical proficiency, and usage habits can vary greatly. The findings of this study describe tendencies rather than absolute truths. Culture is dynamic, and globalisation and the widespread adoption of technology are rapidly changing user behaviour and expectations. The findings of this study may soon become outdated. The study's greatest limitation lies in the complexity and dynamism of ‘culture,’ as well as the difficulty of effectively separating and appropriately measuring these factors. Overreliance on national labels, ignoring the diversity within a country, and confusing culture with other factors (such as regulations, markets, and the economy) can lead to one-sided, stereotypical, or even erroneous results.

5.4 Future Research Prospects

With the widespread use of smartphones and the deepening development of mobile internet, issues related to user privacy and data security have become increasingly severe. This paper analyses three key issues in mobile applications: user privacy security, cultural and

cross-cultural privacy protection, and mobile user data management. Based on this analysis, the paper proposes the following future research directions and recommendations to promote further research in these areas. The paper has demonstrated that there are significant differences in user privacy awareness across different cultural contexts. Cross-cultural privacy protection theories remain incomplete. Future research can be conducted in the following directions. Cultural dimensions and privacy behaviour. Combining Hofstede's cultural dimensions theory (e.g., individualism vs. collectivism, uncertainty avoidance, etc.), explore how different cultural values influence users' privacy sensitivity, willingness to share user data, and acceptance of privacy protection technologies. For users from different cultural backgrounds, explore how to develop more applicable privacy policies. In collectivist cultures, people place greater emphasis on convenience, while in individualist cultures, people focus more on data ownership. Future privacy policies should take these differences into account. In developing countries with lower privacy awareness, explore the feasibility of enhancing user privacy awareness through education, publicity, and legal measures, as well as pathways for integrating technology and culture.

Current privacy protection technologies such as data encryption, anonymisation, tokenisation, and permissions still have many shortcomings, and technical breakthroughs can be attempted. Design a new permission system that allows users to finely control application requests based on the scenario (e.g., allowing users to grant temporary permissions to an application rather than a blanket ‘one-size-fits-all’ permission). Building on privacy computing technologies such as federated learning and multi-party secure computation, explore the implementation of these technologies in mobile applications, enabling mobile applications to perform data

analysis tasks without accessing user data. Use artificial intelligence to monitor application behaviour, predict privacy risks in advance, and proactively notify users, thereby assisting them in making decisions. Currently, different countries and regions have varying definitions and requirements for privacy (e.g., GDPR, CCPA, PIPL), which poses challenges for cross-border applications. Future research can focus on the following areas: Coordinate privacy regulations across different countries, promote internationally recognised privacy protection principles, while also preserving regional cultural differences. Design tools to help developers automatically adapt to legal requirements in different regions, such as using algorithms to automatically generate privacy policies that comply with different regions. Evaluating whether privacy regulations in different regions achieve their intended effects, analysing gaps between specific legal provisions and user behaviour, and providing recommendations for policy formulation. Although people are concerned about their privacy, their behaviour does not always reflect their attitudes (the privacy paradox). Future research could explore the following angles: Studying how users balance privacy risks and convenience. Explore the role of nudge theory in privacy design, such as guiding users toward safer choices through default options. Use longitudinal or experimental methods to track changes in user privacy behaviour over time, and how technology, law, and culture influence behaviour over time, to understand how technology affects behaviour over time. Explore the impact of 'privacy fatigue' on users frequently prompted for permissions, and simplify the process to make it easier for users to manage their privacy and make more informed decisions. As technologies like artificial intelligence, the metaverse, and the Internet of Things evolve, new privacy issues will emerge. Research how AI-generated

content (such as deepfakes) threatens user privacy and what technical or legal measures can be taken to prevent abuse. Study how user identity in virtual environments complicates privacy protection, such as the conflict between anonymity and social interaction when users seek both. In decentralised computing environments, explore local data storage and processing to reduce privacy risks associated with cross-domain transmission. Privacy issues in mobile applications will evolve toward a multidisciplinary, technology-driven, and culturally adaptive approach. Through collaboration across fields such as computer science, law, psychology, and sociology, we can create a safer, more transparent ecosystem. Privacy is not merely a technical issue; it is a matter of the co-evolution of humans, technology, society, and law. Only by placing users at the centre can we achieve true 'privacy-friendly' solutions.

References

Barbosa, P., Brito, A., & Almeida, H. (2020). *Privacy by Evidence: A Methodology to develop privacy-friendly software applications. Information Sciences, 527*, 294-310.

Blank, G., Bolsover, G., & Dubois, E. (2014, August). *A new privacy paradox: Young people and privacy on social network sites. In Prepared for the Annual Meeting of the American Sociological Association (*Vol. 17).

Chen, J. Q., Zhang, R., & Lee, J. (2013). A cross-culture empirical study of M-commerce privacy concerns. *Journal of Internet Commerce*, *12*(4), 348-364.

Cho, H., Knijnenburg, B., Kobsa, A., & Li, Y. (2018). Collective privacy management in social media: A cross-cultural validation. *ACM Transactions on Computer-Human Interaction (TOCHI)*, *25*(3), 1-33.

Degirmenci, K., Guhr, N., & Breitner, M. (2013). Mobile applications and access to personal information: A discussion of users' privacy concerns. In *Proceedings of the 34th International Conference on Information Systems (ICIS 2013)* (pp. 1-21). Association for Information Systems (AIS).

Dane, F. C. (1990). *Research methods*. Thomson Brooks/Cole Publishing Co.

D. He, S. Chan and M. Guizani, "Mobile application security: malware threats and defenses," in *IEEE Wireless Communications*, vol. 22, no. 1, pp. 138-144, February 2015, doi: 10.1109/MWC.2015.7054729. keywords: {Smart phones;Mobile communication;Computer hacking;Spyware;Electronic mail},

Enck, W. (2011). *Defending users against smartphone apps: Techniques and future directions. In Information Systems Security: 7th International Conference, ICISS 2011,*

Henke, J., Joeckel, S., & Dogruel, L. (2018).

Gkoulalas-Divanis, A., & Bettini, C. (Eds.). (2018). *Handbook of mobile data privacy*. Springer International Publishing.

Häkkilä, J. (2006). *Usability with context-aware mobile applications: Case studies and design guidelines*. University of Oulu.

Haq, I. U., & Khan, T. A. (2021). Penetration frameworks and development issues in secure mobile application development: A systematic literature review. *IEEE Access*, *9*, 87806-87825.

He, D., Chan, S., & Guizani, M. (2015). Mobile application security: malware threats and defenses. *IEEE Wireless Communications*, *22*(1), 138-144.

Hoehle, H., & Venkatesh, V. (2015). Mobile application usability. *MIS quarterly*, *39*(2), 435-472.

Hermida, A., & Hernández-Santaolalla, V. (2020). *Horizontal surveillance, mobile communication and social networking sites. The lack of privacy in young people's daily lives*.

Hoehle, H., Zhang, X., & Venkatesh, V. (2015). An espoused cultural perspective to understand continued intention to use mobile applications: a four-country study of mobile social media application usability. *European journal of information systems*, *24*(3), 337-359.

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

Jia, L., & Ruan, L. (2020). Going global: Comparing Chinese mobile applications' data and user privacy governance at home and abroad. *Internet policy review*, *9*(3).

Kaaniche, N., Laurent, M., & Belguith, S. (2020). *Privacy enhancing technologies for solving the privacy-personalization paradox: Taxonomy and survey. Journal of Network and Computer Applications, 171*, 102807,p3.

Kolkata, India, December 15-19, 2011, Procedings 7 (pp. 49-70). Springer Berlin Heidelberg.

Khatoon, A., & Corcoran, P. (2017,September). Android permission system and user privacy—A review of concept and approaches. In *2017 IEEE 7th International Conference on Consumer Electronics-Berlin (ICCE-Berlin)* (pp. 153-158). IEEE.

Kollnig, K., Shuba, A., Binns, R., Van Kleek, M., & Shadbolt, N. (2021). Are iphones really better for privacy? comparative study of ios and android apps. *arXiv preprint arXiv:2109.13722*.

Kununka, S., Mehandjiev, N., & Sampaio, P. (2017). A comparative study of android and ios mobile applications' data handling practices versus compliance to privacy policy. In *IFIP International Summer School on Privacy and Identity Management* (pp. 301-313). Cham: Springer International Publishing.

Li, F., Li, H., Niu, B., & Chen, J. (2019). Privacy computing: Concept, computing framework, and future development trends. *Engineering*, *5*(6), 1179-1192.

Li, F., Li, H., & Niu, B. (2024). Privacy Computing Theory. In *Privacy Computing: Theory and Technology* (pp. 43-88). Singapore: Springer Nature Singapore.

Li, Y., Rho, E. H. R., & Kobsa, A. (2022). Cultural differences in the effects of contextual factors and privacy concerns on users' privacy decision on social networking sites. *Behaviour & Information Technology*, *41*(3), 655-677.

Lim, S. L., Bentley, P. J., Kanakam, N., Ishikawa, F., & Honiden, S. (2014). Investigating country differences in mobile app user behavior and challenges for software engineering. *IEEE Transactions on Software Engineering*, *41*(1), 40-64.

Martin, K., & Shilton, K. (2016). Putting mobile application privacy in context: An empirical study of user privacy expectations for mobile devices. *The Information Society*, *32*(3), 200-216.

Mbanaso, U. M., Abrahams, L., & Okafor, K. C. (2023). Research philosophy, design and methodology. In *Research Techniques for Computer Science, Information Systems and Cybersecurity* (pp. 81-113). Cham: Springer Nature Switzerland.

Methods of data collection: A fundamental tool of research. *Journal of Integrated Community Health*, *10*(1), 6-10.

Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. *European journal of information systems*, *23*(2), 103-125.

Miller, C. (2011). Mobile attacks and defense. *IEEE Security & Privacy*, *9*(4), p

Qureshi, S. S., Ahmad, T., & Rafique, K. (2011, September). Mobile cloud computing as future for mobile applications-Implementation methods and challenging issues. In *2011 IEEE International Conference on Cloud Computing and Intelligence Systems* (pp. 467-471). IEEE.

Nikkhah, H. R., Schlackl, F., & Sabherwal, R. (2025). Does Culture Affect Post-Adoption Privacy Concerns of Mobile Cloud Computing App Users? Insights from the US, the UK, and India. *Information Systems Frontiers*, 1-22.

Peltonen, E., Lagerspetz, E., Hamberg, J., Mehrotra, A., Musolesi, M., Nurmi, P., & Tarkoma, S. (2018, September). The hidden image of mobile apps: geographic, demographic, and cultural factors in mobile usage. In *Proceedings of the 20th International Confe*

rence on Human-Computer Interaction with Mobile Devices and Services (pp. 1-12).

Pentina, I., Zhang, L., Bata, H., & Chen, Y. (2016). Exploring privacy paradox in information-sensitive mob

ile app adoption: A cross-cultural comparison. *Computers in Human Behavior*, *65*, 409-419.

Syamsuar, D., Fahrezi, F., Favian, A., Irwansyah, E., & Irawan, A. F. (2024, August). Disclosure Privacy Information Social Media on TikTok. In *2024 International Conference on Information Managem*

ent and Technology (ICIMTech) (pp. 495-500). IEEE.

Sandoval, Z. V., Lingelbach, K., & Rigole, N. (2023). Privacy, security, and awareness perceptions on the use of social media: a TikTok focus. *Issues in Information Systems*, *24*(4), 16-24.

Shrestha, A. K., Barthwal, A., Campbell, M., Shouli, A., Syed, S., Joshi, S., & Vassileva, J. (2024). *Navigating AI to unpack youth privacy concerns: An in-depth exploration and systematic review*. *arXiv preprint arXiv:2412.16369,p1*.

Stevens, R., Gibler, C., Crussell, J., Erickson, J., & Chen, H. (2012, May). Investigating user privacy in android ad libraries. In *Workshop on Mobile Security Technologies (MoST)* (Vol. 10, pp. 195-197).

Tiara, N. L., Aulia, S. R., Farhana, H., & Batubara, S. (2024). Analysis of Data Security and Privacy on Tiktok Social Media Applications Based on Blockchin Technology. *International Journal Of Computer Sciences and Mathematics Engineering*, *3*(1), 61-65.

Tsavli, M., Efraimidis, P. S., Katos, V., & Mitrou, L. (2015). Reengineering the user: privacy concerns about personal data on smartphones. *Information & Computer Security*, *23*(4), 394-405.

*Sierra, F., & Ramirez, A. (2015, September). Defending your android app. In Proceedings of the 4th Annual ACM Conference on Research in Information Technology,*p29).

Werthmann, T., Hund, R., Davi, L., Sadeghi, A. R., & Holz, T. (2013, May). Psios: bring your own privacy & security to ios devices. In *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security* (pp. 13-24).

Wottrich, V. M., van Reijmersdal, E. A., & Smit, E. G. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision support systems*, *106*, 44-52.

Yadav, C. S., Singh, J., Yadav, A., Pattanayak, H. S., Kumar, R., Khan, A. A., ... & Alharby, S. (2022). *Malware analysis in IoT & android systems with defensive mechanism. Electronics, 11*(15), 2354.

Yang, K. C., & Kang, Y. (2015). Exploring big data and privacy in strategic communication campaigns: A cross-cultural study of mobile social media users' daily experiences. *International Journal of Strategic Communication*, *9*(2), 87-101.

Zhao, J., Lyngs, U., & Shadbolt, N. (2018). *What privacy concerns do parents have about children's mobile apps, and how can they stay SHARP? arXiv preprint arXiv:1809.10841*.

Zhang, S., Lei, H., Wang, Y., Li, D., Guo, Y., & Chen, X. (2023, September). How android apps break the data minimization principle: an empirical study. In *2023 38th IEEE/ACM International Conference on Automated Software Engineering (ASE)* (pp. 1238-1250). IEEE.

Zhu, X., Cao, Q., & Liu, C. (2022). Mechanism of platform interaction on social media users' intention to disclose privacy: A case study of Tiktok app. *Information*, *13*(10), 461.

Appendix

Survey Questionnaire

What is your age?

a: 18-25

b: 26-40

c: 41-60

What is your gender?

a: Male

b: Female

What region are you in?

a: European Union

b: UK

c: China

d: Singapore

What type of mobile app do you use most often? (Multiple choice)

a: Social media (WeChat/Instagram/Facebook, etc.)

b: E-commerce shopping (Taobao/Amazon, etc.)

c: Entertainment content (short videos/music/games, etc.)

d: Utility apps (maps/translation/office tools, etc.)

e: Financial services (banking apps, etc.)

Please answer the following questions according to the following scoring criteria: 1-Strongly disagree 2-Disagree 3-Neutral 4-Agree 5-Strongly agree (This questionnaire is conducted anonymously, so the privacy information of the respondents will not be disclosed)					
	1	2	3	4	5
Privacy leakage of mobile applications.					
Have you encountered the following privacy security issues?					
Have you ever encountered an application that frequently asks for permissions unrelated to functionality?					
Have you received harassing ads/scam messages related to the use of the app?					
Do you find most app permissions confusing and difficult to understand?					

Do you use ios often?					
Do you use Android?					
Different countries and service areas.					
If you have used the same app in different countries, do you feel the privacy policy is different?					
Do you think users attitudes to privacy are different in different regions?					
Do you think Asian users are more receptive to data exchange for convenience?					
Do you think users in developing countries have a low awareness of privacy risks?					
User privacy awareness.					
Do you often refuse to grant non-essential permissions?					
Do you regularly check your app permissions					
Will you uninstall apps with vague privacy policies?					
Did you report an app that collected excessive data to the platform?					
If an app is free but requires you to watch ads, would you voluntarily refuse it?					
Are you concerned about privacy issues?					
Do you think privacy laws are important?					