PACIS 2023 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

7-8-2023

Will Security and Privacy Updates Affect Users' Privacy Choices of Mobile Apps

Baozhen Zhan
Xi'an Jiaotong University, zhanbz@stu.xjtu.edu.cn

Jin Li
Xi'an Jiaotong University, jinlimis@xjtu.edu.cn

Jiawen Zhu
Xi'an Jiaotong University, zhujiawen@mail.xjtu.edu.cn

Gengzhong Feng
Xi'an Jiaotong University, gzfeng@xjtu.edu.cn

Recommended Citation

Zhan, Baozhen; Li, Jin; Zhu, Jiawen; and Feng, Gengzhong, "Will Security and Privacy Updates Affect Users' Privacy Choices of Mobile Apps" (2023). *PACIS 2023 Proceedings*. 209.
https://aisel.aisnet.org/pacis2023/209

Will Security and Privacy Updates Affect Users' Privacy Choices of Mobile Apps?

Short Paper

Baozhen Zhan
School of Management
Xi'an Jiaotong University
Xi'an, China
zhanbz@stu.xjtu.edu.cn

Jin Li
School of Management
Xi'an Jiaotong University
Xi'an, China
jinlimis@xjtu.edu.cn

Jiawen Zhu
School of Management
Xi'an Jiaotong University
Xi'an, China
zhujiawen@xjtu.edu.cn

Gengzhong Feng
School of Management
Xi'an Jiaotong University
Xi'an, China
gzfeng@xjtu.edu.cn

Abstract

There is a growing emphasis among users on safeguarding personal privacy and authorization for applications. To address this, Security and Privacy Updates (SPU) are employed to bolster app security, alleviate user apprehensions regarding security, and encourage users to share data and permissions with greater confidence. Based on the Protection Motivation Theory (PMT), we propose that SPU, an IT technology itself, has a dual effect on users' privacy choices, security threat susceptibility and security response efficacy are the two key mediators to explain this phenomenon, and that this influencing process will be moderated by user's privacy trade-off. We will investigate this process through a set of online experiments.

Keywords: mobile application, security and privacy updates, protection motivation theory, privacy choice, privacy trade-off

Introduction

With the advancement of mobile technology and the increasing number of mobile apps in markets, users are becoming more aware of data that is being collected and shared through their mobile devices. User privacy security has become a critical issue in developing mobile applications. According to the survey conducted by the Pew Research Center, 90% of American adults believe it is important to carefully protect their personal information[1], and 81% of them think the potential risks of data collection would outweigh the benefits[2]. People are frequently alarmed about the potential privacy threats and being motivated to evaluate their privacy protection options (Mousavi et al., 2020), and they are becoming more concerned to protect their privacy when using mobile apps. Although data-driven personalized advertising may be more effective for consumers (Choi et al., 2020), many users are now disabling location services, denying apps access to their camera and microphone, and opting out of targeted advertising programs (Tucker, 2012). Such negative privacy choices, i.e., declining to share data or grant permissions, in mobile applications may

[1] https://www.pewresearch.org/internet/2015/05/20/

[2] https://www.pewresearch.org/internet/2019/11/15/

result in a lose-lose scenario. Users may not be able to access enhanced services, while app development companies may also miss out on potential profits.

Over the past few decades, researchers from various disciplines such as management and information systems, economics, marketing, and psychology have actively studied the motivations for privacy decision makings. For instance, customers may need to provide their privacy information in exchange for promotional coupons (Chellappa & Shivendu, 2010), personalized services (Chellappa & Shivendu, 2010; Xu et al., 2011), and social rewards in social activities (Jiang et al., 2013). The above literature reveals the individuals privacy choosing are the outcome of a mental calculation that balances the anticipated benefits of privacy choice against the costs (Dinev & Hart, 2006; Klopfer & Rubenstein, 1977). Personal characteristics (Goldfarb & Tucker, 2012) and other external factors such as online versus paper-and-pencil questionnaires (Moon, 2000) also affect privacy decision makings. We notice that these privacy decisions are from external stimuli, rather than IT technology itself, the underlying security risks persist and negatively affects users' willingness to share privacy information. To increase positive evaluation, developers often introduce new features or bug fixes through app updates. However, most previous studies have focused on the impact of functional updates on user satisfaction and evaluation, neglecting the role of security updates. In fact, correcting security defects or altering software attributes are often used by developers to reduce possible negative experiences (Popovic et al., 2001). Unlike customer satisfaction, which is a post-experience, privacy choices are pre-experience decisions based on users' own psychology and preference, which will be more likely be influenced by some important signals, such as security and privacy update descriptions in the App market. Therefore, in the context of privacy decision-making, security and privacy updates (SPU) seem to play a more significant role than general ones. Thus, our study aims to explore how SPU, an IT technology itself, affect users' privacy choices.

SPU may have a dual effect on users' privacy decision-making. On one hand, SPU can signal to users that the information system's security is being continuously improved, potentially resulting in more positive privacy choices. On the other hand, these updates can draw users' attention to previously ignored security risks, prompting more cautious privacy decisions. For example, on January 6, 2021, WhatsApp updated the security and privacy policy, and issued a separate notification within the app. Although it explained in more detail how user data is used and protected, it still aroused some user concerns, which triggered a wave of social immigration, resulting in the downloads of its competing apps (i.e., Telegram and Signal) that month Ranked top 3 in the global App download list[3]. This case further illustrates the important impact of SPU on users' behavior. To gain a deeper understanding of this issue, we employ the Protection Motivation Theory (PMT) (Rogers, 1975) to investigate the underlying impact mechanism. In this research, we define privacy choices as the willingness or the number of additional permissions (not related to core function) that users authorize an app to obtain and use their preference or behavior data. Based on PMT, we find that threat susceptibility (Lee et al., 2008) and response efficacy (Lee et al., 2008; Rodríguez-Priego et al., 2022) are key factors in understanding the mechanisms by which SPU may affect users' privacy choices. Although we have gained insights into the impact mechanism, the negative effects of SPU on privacy choices have not been effectively addressed. To mitigate these negative effects, we also propose a moderating variable, privacy trade-off. Prior studies on information systems and marketing have consistently shown that people tend to be cautious with their personal information due to privacy concerns (Jiang et al., 2013; Son & Kim, 2008). However, it is important to note that individuals are still willing to compromise their privacy in exchange for material benefits such as monetary incentives or immaterial rewards like intangible benefits (Jiang et al., 2013). Thus, privacy concerns and rewards are two aspects of a privacy trade-off. We propose that in the context of mobile applications, feature rewards—better service and user experience brought about by privacy concessions—could lighten the negative effect of SPU on user privacy choices, and privacy concern will have the opposite effect for this process.

Overall, we postulate that the implementation of SPU holds a certain degree of influence over the privacy choices (e.g., granting more permissions for certain apps) made by users. Specifically, drawing on the PMT framework, we posit that susceptibility and efficacy are two critical factors in understanding the mechanism through which SPU may influence users' privacy choices. We hypothesize that SPU will have a negative impact on susceptibility, but a positive impact on efficacy, ultimately mixed influencing users' decisions about privacy. Furthermore, we also explore the moderating role of privacy trade-off in the context of

[3] https://www.business-standard.com/article/technology/whatsapp-says-latest-policy-update-doesn-t-affect-privacy-of-messages-121011200643_1.html

mobile apps, considering both feature rewards and privacy concerns. We aim to investigate how privacy trade-off can moderate the negative impact of susceptibility and enhance the positive effect of efficacy on users' privacy choices. The research questions of our research are summarized below:

(1) How do security and privacy updates influence users' privacy choices?

(2) Will security threat susceptibility and security response efficacy mediate the impact of security and privacy updates on user security choices?

(3) How does privacy trade-off regulate moderate the impact of the two factors on privacy choice?

There are three main potential contributions of this research. First, we investigate a widely used application scenario, i.e., app security and privacy updates, which has not been sufficiently studied in previous literature, from the perspective of IT technology itself, to determine if it influences user privacy choices. Second, we empirically validate the application scenarios of PMT by reasonably explaining the influence mechanism to explain this question, specifically, the mediating role of threat susceptibility and response efficacy. Thirdly, we innovatively introduce the moderating variable of privacy trade-off and combine it with the PMT theory to help app developers explore mitigation measures for the negative impact of security updates. Our findings could help app developers or firms improve users' willingness to share data from a subjective level (rather than IS external stimuli), obtain higher profits, and provide better personalized services to users, resulting in a win-win situation. Essentially, we hope to advance the literature stream in this field with a more holistic and comprehensive understanding of protection motivation theory and privacy trade-off in mobile application.

Theoretical Background and Hypotheses Development

Privacy Choices and Security Updates

The private sector's growing access to and utilization of extensive volumes and types of detailed consumer data has sparked widespread concerns regarding consumer privacy (Wedel & Kannan, 2016). The trade-off between privacy and disclosure, whereby consumers must decide whether to share or withhold personal information, has been extensively studied in the literature of Information Systems and Marketing (Adjerid et al., 2018). The literature reveals that the anticipated benefits of privacy choice are the main motivation for individuals to choose for disclosing personal information or sharing personal data regardless of privacy risks. These benefits mainly come from providing personal information in exchange for promotional coupons (Chellappa & Shivendu, 2010), personalized services (Chellappa & Shivendu, 2010; Xu et al., 2011), or social rewards in social interactions (Jiang et al., 2013). Some scholars have also investigated factors that affect individuals' willingness to share data from the perspective of subjective aspects and user characteristics, such as cognitive efforts required to make a privacy choice (Dinev et al., 2015), perception of risks associated with divulging personal information (Adjerid et al., 2018), perceived anonymity of oneself (Jiang et al., 2013), and perceived control over personal information (Xu et al., 2011). An individual's age, wealth, and technical proficiency can also play a role (Goldfarb & Tucker, 2012). Recent literature on privacy has also explored external factors that seemingly have little or no direct impact on the objective risks and benefits of disclosing personal information, such as online versus paper-and-pencil questionnaires (Moon, 2000), disclosures made online or face-to-face communication (Harper Jr & Harper, 2006), individuals' perceived control (Brandimarte et al., 2013), these factors can significantly impact people's privacy concerns and preferences for self-disclosure. Externalities like the willingness of others to divulge personal information or register for the do-not-call list can also impact an individual's decision (Acquisti et al., 2012; Adjerid et al., 2019).

The above literature shows that prior studies on privacy choice mainly focus on the exchange of interests with enterprises, user personal characteristics, external factors, etc., while ignoring the technical perspective itself. The potential risks of information system (IS) still exist, which have not improved the security of IS itself. Nevertheless, in the context of mobile apps, the security of information systems is continually being enhanced through irregular updates, which is a dynamic process. Most previous studies have focused on the impact of functional updates on user satisfaction and evaluation, while overlooking the role of security updates. For instance, Fleischmann et al. (2016) concluded that the favorable impacts of feature updates are not transferable to updates solely intended to address flaws. Frequent functional updates can lead to higher customer evaluation to the app (Foerderer et al., 2018). However, defects (e.g., app crashes) or security breaches can cause significant workflow interruptions and serious security issues, which may be more critical than lacking extra novelty functions. As a result, developers frequently depend on regular vulnerability fixes and continuous enhancements to privacy agreements as the most common and effective way to safeguard user privacy. These updates are typically highlighted in the version description (Kaushik & Gokpinar, 2023) to ensure users are aware of the key content. Therefore, we reasonably posit that SPU can be regarded as the signal that can influence on users' privacy decision-making base on signaling theory (Connelly et al., 2011). We consider the benefits and costs of the IT technology itself, namely the SPU, which can influence user privacy choices.

In this paper, **the privacy choices** are defined as the willingness or the number of non-core permissions users authorize to an app. As a positive privacy choice, the user will give app more permissions and disclose their information. For example, in mobile app settings, sharing the GPS and location information to the app is a positive privacy choice.

Protection Motivation Theory

The Protection Motivation Theory (PMT) was originally proposed by Rogers (1975). It describes that fear appeal within a persuasive communication could affect people's cognitions about the threat and countermeasures, which further incur their protective motivation and motivate them to take the recommended actions to protect themselves (Maddux & Rogers, 1983; Rogers, 1975). Drawing from the Parallel Process Model (Leventhal, 1970), PMT proposes that the fear-inducing communication triggers two cognitive processes, namely threat appraisal and coping appraisal (Maddux & Rogers, 1983). The threat appraisal process, or fear control process, comprises three constructs including threat severity, threat susceptibility, and maladaptive reward. The threat susceptibility refers to the likelihood of the threat occurring. The coping appraisal process, or danger control process, encompasses self-efficacy, response efficacy, and response cost. The response efficacy refers to an individual's belief in the effectiveness of suggested countermeasures. Studies have shown that threat susceptibility and response efficacy have a positive impact on individuals' protective behaviors (Lee et al., 2008). As we mentioned above, SPU may have a two-sided impact on users' privacy choice. Corresponding to the above two effects, threat sensitivity and response efficacy are key theoretical variables that help to better understand how SPU affects user privacy choices.

There are also evidences showing that the Protection Motivation elements are affecting privacy protection behavior. Literature employing the PMT suggests that security countermeasure awareness is a precursor to desktop security behavior among home users, revealing the motivational factors that drive individuals to adopt particular protective measures (Hanus et al., 2018). D'Arcy et al. (2009) have defined security countermeasure awareness as the knowledge of formal security policies and guidelines, security education and etc.. This includes awareness of potential security threats, knowledge of security policies and guidelines, and familiarity with security policies (Pahnila et al., 2007; Rhee et al., 2012). The study conducted by Mousavi et al. (2020) investigates the impact of privacy assurance mechanisms on the privacy preserving actions of users on social networking sites (SNS). Vishwanath et al. (2018) conduct a study to examine personal privacy choices on Facebook, specifically focusing on the individual's perception of severity and susceptibility to privacy risks. Rodríguez-Priego et al. (2022) employ the PMT to assess the association between motivation and behavior in the context of Location-based Mobile Applications (LBMA).

In conclusion, the PMT has been extensively applied in the investigation of information security behavior. In this study, we focus on evaluating the effects of response efficacy and threat susceptibility. As we mentioned above, response efficacy refers to individuals beliefs that the protective measures are to prevent the risk, and threat susceptibility refers to the likelihood of the threat occurring based on PMT (Rogers, 1975; Vishwanath et al., 2018). Hence, we can define the user's belief in the effectiveness of security and privacy countermeasures as **security response efficacy**. That is, when users receive the signal that an app has improved its security, they develop a personal belief in the efficacy of the update and in the app developer's ability to better protect their private data. **Security threat susceptibility** can be defined as the psychological prediction of an app user regarding the potential occurrence of a threat. That is to say, when users receive a signal indicating improved app security, their concerns about potential app vulnerabilities and security risks other than the content of this security update.

Privacy Trade-off

Prior research has devoted considerable attentions to the matter of privacy concerns in various domains such as online healthcare, e-commerce, and marketing (Malhotra et al., 2004). While studies in the fields of Information Systems and Marketing have consistently demonstrated that privacy concerns elicit cautious behavior in individuals when it comes to handling their personal information (Jiang et al., 2013; Son & Kim, 2008), it is worth noting that people are still willing to compromise their privacy for some material (e.g., monetary incentives) and immaterial (e.g., intangible benefits) rewards (Jiang et al., 2013).

According to previous research, individuals may be willing to trade certain social commodities, such as information privacy, for other benefits through a form of exchange. For instance, Dinev and Hart (2006) discovered that people were more inclined to provide personal information for internet transactions when their interests in the content outweighed their privacy concerns. In the context of mobile applications, intangible benefits are of particular importance. For instance, individuals may socialize in online chat rooms solely for communication, relaxation, and enjoyment. Chatting with others online can be a source of joy in itself (Jiang et al., 2013). Additionally, the hedonistic value of entertainment apps and the efficiency of functional apps are also critical factors for customers to usage (Gong et al., 2021; Tafesse, 2021).

Hence, we contend that feature rewards, which refer to the pleasure, extra satisfaction, and gratification individuals derive from using non-core functions of apps, are the alternative benefits in privacy exchanged. The **feature reward** is defined as positive experiences (non-core app functions or features) resulting from information sharing or permissions changing behavior. When we share the location information to a short-form video app, we will watch short videos shared by users living in the same community. Also, the app may make personalized recommendations, such as videos about nearby restaurants and gyms to save your searching time. Such convenience obtained by sharing data based on privacy location is considered a feature reward in this scenario. Then, **privacy concerns** refer to the apprehension that app users experience regarding the ability of the app or its developer to ensure effective protection of user data, after any modifications are made to personal information sharing or privacy settings, such as the fear of individual data breach or being subjected to price discrimination.

Research Model and Hypotheses

Based on above theoretical analyses, we develop a research model as shown in Figure 1 and propose hypotheses as followings.

Considerable research has indicated that consumers' privacy choices can be influenced by alterations in their anticipated privacy gains and hazards. Sharing personal information, for instance, can yield benefits for consumers, including personalized product offerings and personalized services, promotional deals (e.g. promotional coupons), and tailored user interfaces in the retail industry, and also social rewards in social interactions (Ansari & Mela, 2003; Jiang et al., 2013; Xu et al., 2011). However, the literature has also noted potential risks associated with sharing personal privacy data, such as data misuse (Featherman & Pavlou, 2003), sharing of personal information with third parties, or price discriminations (Viswanathan et al., 2007). Similarly, we can reasonably assume that the SPU also have the two-sided effects on user security protection behavior and privacy choices.

On the one hand, the SPU, which include both privacy updates and the fixing of defects, play a pivotal role in shaping users' security belief. Based on the signaling theory (Connelly et al., 2011), the SPU can improve the reliability and security of mobile applications or provide higher levels of privacy protection. The SPU may signal to users that the security of information systems is continuously being enhanced, thus improving their belief of app security and developer. On the other hand, SPU may draw users' attention to previously overlooked security risks. Such updates can reveal unexpected vulnerabilities in the app or compatibility issues with new mobile systems. More importantly, consumers may therefore perceive that there are more potential security risks overlooked. Therefore, we propose that,

Hypothesis 1a: Security and Privacy Updates positively influences Security Response Efficacy.

Hypothesis 1b: Security and Privacy Updates positively influences Security Threat Susceptibility.

Based on PMT, response efficacy and threat susceptibility are both protection motivation elements that can affect privacy protection behavior. Researches demonstrate that consumer trust plays a critical role as a mediating variable between consumers' perceived risk and their behaviors (Kim et al., 2008; Vance et al., 2008). Joinson (2010) argues that trust plays a mediating role in the relationship between perceived privacy and actual behavior. Xu et al. (2011) conclude that the perceived effectiveness of privacy policies may enhance individuals' perceived control over online information disclosure, and increase their confidence in sharing personal information. Xu et al. (2012) find that industry self-regulation and government regulation can increase consumer trust in privacy. The user's belief regarding the security improvement of the app can have a significant impact on their behavior, particularly in terms of the privacy choices they make in the information system. Hence, we propose that,

Hypothesis 2: Security Response Efficacy positively influences Privacy Choices.

Hypothesis 3: Security Threat Susceptibility negatively influences Privacy Choices.

Previous research has investigated privacy concerns. Son and Kim (2008) discovered that internet users who had concerns about the misuse of their information often refrained from sharing their personal details in online transactions. Additionally, Stewart and Segars (2002) analyzed privacy concerns in direct marketing and revealed that consumers declined to disclose their financial information to insurance companies when they were apprehensive about the handling of their sensitive data. Here, we define privacy concerns as the worries of app users regarding the security performance of the app after they have made changes to personal information sharing or privacy rights. We suggest that privacy concerns may have a negative moderating effect. Users who are more concerned about privacy tend to amplify the negative impact of susceptibility on privacy while simultaneously attenuating the positive effect of efficacy. Therefore, we propose that,

Hypothesis 4a: Privacy Concern negatively moderates the negative effect of Security Threat Susceptibility on Privacy Choices.

Hypothesis 4b: Privacy Concern weakens the positive effect of Security Threat Susceptibility on Privacy Choices.

In the context of our study, we may posit that feature rewards could potentially moderate the adverse effects of security threat susceptibility on privacy choices behavior. Specifically, when an app offers an extra feature except the core function, a more favorable user experience based on the user's privacy choices, and garners positive impressions, users may be more likely to ignore that the app may have more potential security risk. Hence, we propose that,

Hypothesis 5: Feature Rewards weaken the negative effect of Security Threat Susceptibility on Privacy Choices.

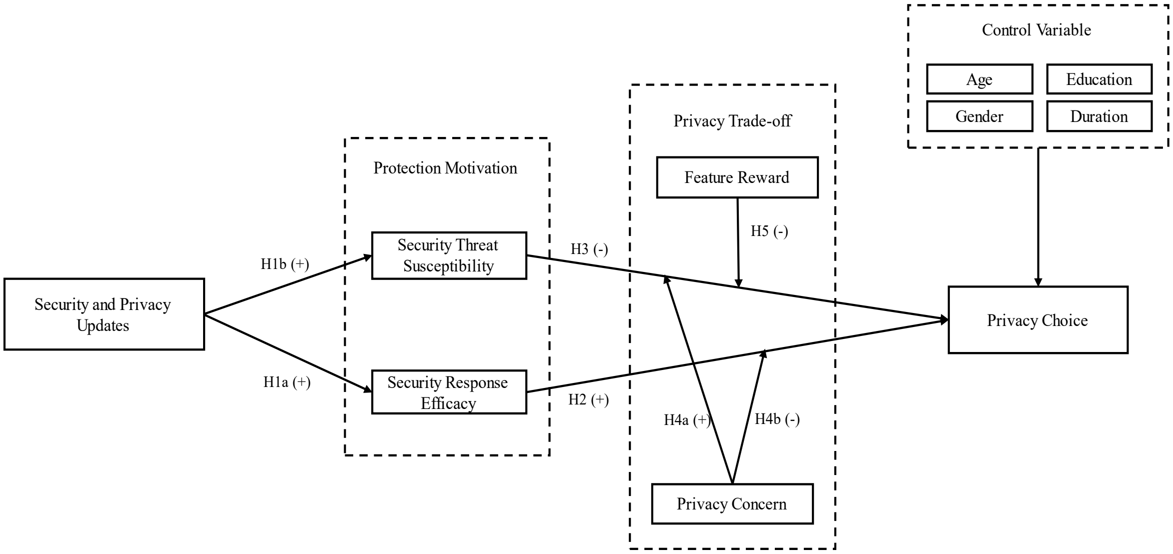

Figure 1 Proposed Research Model

Proposed Research Methodology and Future Plan

The data for this study will be collected through an online experiment targeting smartphone or tablet users. We will recruit participants through paid participant pools on Amazon Mechanical Turk. Subjects will be randomly assigned to four different experimental groups (Group A1-A4) and two control groups (Group B1-B2). All the constructs are measured by mature scales adopted from existing literature (as shown in Table 1).

We first observe the protection motivation (Security Response Efficacy & Security Threat Susceptibility) and privacy choices of the subjects in the six groups of initial state. Subsequently, the four experimental groups will be presented with the SPU signal and will be informed about the update details through the app version description and a separate notification. It is noted that these signals are not the same.

Group A1 only receives a basic signal (signal of security and privacy updates, including the specifically content of the update), and we will measure the protection motivation and privacy choices. Group A2 will receive two signals, one is the basic signal, and the other will introduce the personalized services other than non-core functions; and we will measure protection motivation, privacy choices and feature reward at the same time. Group A3 will also receive two signals, including the basic signal and the others for privacy concerns; that is, if there may be hidden dangers in sharing data, we will also measure protection motivation, privacy choices and privacy concern. Group A4 will receive those three kinds of update signals, and all the variables will be measured. At the same time, we will provide the control group B1 with a general update (i.e., function-adding update) signal and control group B2 without any updates. Protection motivation and privacy choices will be both observed again in groups B1 and B2.

Table 1 Reference about Variable Measurement

Theory	Variable	Definition of constructs	Reference
Protection Motivation	Security Threat Susceptibility	Likelihood of the threat occurring in the app	Lee et al., 2008
	Security Response Efficacy	User's belief in the security and privacy update	Lee et al., 2008; Rodríguez-Priego et al., 2022
Privacy Trade-off	Feature Reward	Unexpected positive experiences from privacy choices changing	Myyry et al., 2009
	Privacy Concern	Concerns about ability to effectively protect privacy data	Jiang et al., 2013; Malhotra et al., 2004

Intended Contribution

This study may potentially make both theoretical and practical contributions. Firstly, we consider how IT technology itself, namely app security and privacy updates (SPU), affects user privacy choices, which has not been sufficiently explored in previous literature. While prior research on app updates focused on user satisfaction and continued use intentions, our study supplements the existing work on app updates by examining their influence on individual privacy protection. In addition, we contribute to the literature of exploring the antecedents of privacy choice behavior. Secondly, we expand the application scenarios of the Protection Motivation Theory (PMT) by providing a reasonable explanation of its influence mechanism. Specifically, we extend the PMT to examine the privacy choices impact of SPU, with a focus on the mediating role of security threat susceptibility and security response efficacy, which helps us to understand the mechanism by which SPU affects privacy choices. Thirdly, we introduce the moderating variable of privacy trade-off and combine it with the PMT to explore mitigation factors for the negative impact of SPU, which also enrich the literature on privacy trade-off. Our study also has practical contributions. Firstly, we reveal a phenomenon, that is, the double-sided impact of SPU on privacy choice, which provides a new perspective for mobile app development companies to understand the motivation of users to share data and permissions. Secondly, we provide developers and firms with methods, that is increasing the extra function reward, to alleviate user privacy concerns and improve their willingness to share data, thereby achieving a win-win situation for both parties.

Acknowledgements

This work received support from the National Social Science Foundation of China (20&ZD053) and the National Natural Science Foundation of China (72201205).

References

Acquisti, A., John, L. K., & Loewenstein, G. (2012). The Impact of Relative Standards on the Propensity to Disclose. Journal of Marketing Research, 49(2), 160–174.

Adjerid, I., Peer, E., Bar-Ilan University, & Acquisti, A. (2018). Beyond the Privacy Paradox: Objective Versus Relative Risk in Privacy Decision Making. MIS Quarterly, 42(2), 465–488.

Adjerid, I., Acquisti, A., & Loewenstein, G. (2019). Choice Architecture, Framing, and Cascaded Privacy Choices. Management Science, 65(5), 2267-2290

Ansari, A., & Mela, C. F. (2003). E-Customization. Journal of Marketing Research, 40(2), 131–145.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced Confidences: Privacy and the Control Paradox. Social Psychological and Personality Science, 4(3), 340–347.

Chellappa, R. K., & Shivendu, S. (2010). Mechanism Design for “Free” but “No Free Disposal” Services: The Economics of Personalization Under Privacy Concerns. Management Science, 56(10), 1766–1780.

Choi, H., Mela, C. F., Balseiro, S. R., & Leary, A. (2020). Online Display Advertising Markets: A Literature Review and Future Directions. Information Systems Research, 31(2), 556–575.

Connelly, B. L., Certo, S. T., Ireland, R. D., & Reutzel, C. R. (2011). Signaling Theory: A Review and Assessment. Journal of Management, 37(1), 39–67.

D’Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research, 20(1), 79–98.

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. Information Systems Research, 17(1), 61–80.

Dinev, T., McConnell, A. R., & Smith, H. J. (2015). Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the “APCO” Box. Information Systems Research, 26(4), 639–655.

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. International Journal of Human-Computer Studies, 59(4), 451–474.

Fleischmann, M., Amirpur, M., Grupp, T., Benlian, A., & Hess, T. (2016). The role of software updates in information systems continuance—An experimental study from a user perspective. Decision Support Systems, 83, 83–96.

Foerderer, J., Kude, T., Mithas, S., & Heinzl, A. (2018). Does Platform Owner’s Entry Crowd Out Innovation? Evidence from Google Photos. Information Systems Research, 29(2), 444–460.

Goldfarb, A., & Tucker, C. (2012). Shifts in Privacy Concerns. American Economic Review, 102(3), 349–353.

Gong, X., Razzaq, A., & Wang, W. (2021). More Haste, Less Speed: How Update Frequency of Mobile Apps Influences Consumer Interest. Journal of Theoretical and Applied Electronic Commerce Research, 16(7), 2922–2942.

Hanus, B., Windsor, J. C., & Wu, Y. (2018). Definition and multidimensionality of security awareness: Close encounters of the second order. ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 49(SI), 103–133.

Harper Jr, V. B., & Harper, E. J. (2006). Understanding student self-disclosure typology through blogging. The Qualitative Report, 11(2), 251–262.

Jiang, Z. (Jack), Heng, C. S., & Choi, B. C. F. (2013). Research Note—Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions. Information Systems Research, 24(3), 579–595.

Joinson, A., Reips, U.-D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, Trust, and Self-Disclosure Online. Human-Computer Interaction, 25(1), 1–24.

Kaushik, N., & Gokpinar, B. (2023). Sequential Innovation in Mobile App Development. Manufacturing & Service Operations Management, 25(1), 182-199.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. Decision Support Systems, 44(2), 544–564.

Klopfer, P. H., & Rubenstein, D. I. (1977). The concept privacy and its biological basis. Journal of Social Issues, 33(3), 52–65.

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: A model of online protection behaviour. Behaviour & Information Technology, 27(5), 445–454.

Leventhal, H. (1970). Findings and theory in the study of fear communications. Advances in Experimental Social Psychology, 5, 119–186.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. Journal of Experimental Social Psychology, 19(5), 469–479.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. Information Systems Research, 15(4), 336–355.

Moon, Y. (2000). Intimate Exchanges: Using Computers to Elicit Self - Disclosure From Consumers. The Journal of Consumer Research, 26(4), 323–339.

Mousavi, R., Chen, R., Kim, D. J., & Chen, K. (2020). Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory. Decision Support Systems, 135, 113323.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. European Journal of Information Systems, 18(2), 126–139.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07), 156b–156b.

Popovic, M., Atlagic, B., & Kovacevic, V. (2001). Case study: A maintenance practice used with real-time telecommunications software. Journal of Software Maintenance and Evolution: Research and Practice, 13(2), 97–126.

Rhee, H.-S., Ryu, Y. U., & Kim, C.-T. (2012). Unrealistic optimism on information security management. Computers & Security, 31(2), 221–232.

Rodríguez-Priego, N., Porcu, L., & Kitchen, P. J. (2022). Sharing but caring: Location based mobile applications (LBMA) and privacy protection motivation. Journal of Business Research, 140, 546–555.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. The Journal of Psychology, 91(1), 93–114.

Son, J.-Y., & Kim, S. S. (2008). Internet users' information privacy-protective responses: A taxonomy and a nomological model. MIS Quarterly, 503–529.

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. Information Systems Research, 13(1), 36–49.

Tafesse, W. (2021). The effect of app store strategy on app rating: The moderating role of hedonic and utilitarian mobile apps. International Journal of Information Management, 57, 102299.

Tucker, C. E. (2012). The economics of advertising and privacy. International Journal of Industrial Organization, 30(3), 326–329.

Vance, A., Elie-Dit-Cosaque, C., & Straub, D. W. (2008). Examining Trust in Information Technology Artifacts: The Effects of System Quality and Culture. Journal of Management Information Systems, 24(4), 73–100.

Vishwanath, A., Xu, W., & Ngoh, Z. (2018). How people protect their privacy on facebook: A cost-benefit view. Journal of the Association for Information Science and Technology, 69(5), 700–709.

Viswanathan, S., Kuruzovich, J., Gosain, S., & Agarwal, R. (2007). Online infomediaries and price discrimination: Evidence from the automotive retailing sector. Journal of Marketing, 71(3), 89–107.

Wedel, M., & Kannan, P. K. (2016). Marketing Analytics for Data-Rich Environments. Journal of Marketing, 80(6), 97–121.

Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. Decision Support Systems, 51(1), 42–52.

Xu, H., Teo, H.-H., Tan, B. C. Y., & Agarwal, R. (2012). Research Note—Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services. Information Systems Research, 23(4), 1342–1363.