JKAU/ Econ. & Adm., **Vol. 38**, No. 2, pp: 121 - 141 (2024 A.D.)
DOI:10.4197/Econ.38-2.4

Examining the Factors Affecting Individual's Information Privacy Concerns of Mobile Apps

Salem Ali Alghamdi

Digital Transformation and Information Programs Department, Institute of Public Administration Jeddah, Saudi Arabia

ghamdisa@ipa.edu.sa

Abstract. Although mobile applications are on the cutting edge of mobile computing technology, security issues loom as a hindrance to their acceptance. Extant literature indicates that addressing security breaches may not primarily rely on advanced technologies but also factors such as security knowledge, prior privacy experience, and behavior. This has led to the emergence of several theories that mainly address the gap related to privacy concerns among mobile device users, especially assessing individual behavioral intention toward mobile applications. To fill this gap, the current study is built upon the Mobile User Information Privacy Concerns (MUIPC) framework. Therefore, a survey study comprising 290 participants' data was undertaken to empirically examine the proposed theoretical model regarding individual motivation to utilize mobile apps. The study's findings indicate that prior privacy experience, technical security knowledge, and download priority are significant predictors of perceived surveillance, perceived intrusion, and secondary use of information. However, the influence of desensitization was insignificant. Further, the findings show that secondary use of personal information has a negative and significant effect on the intention to use mobile apps. The findings also indicate that users' privacy and security perceptions vary depending on the level of information sensitivity in mobile apps.

Keywords: Prior Privacy Experience, Technical Security Knowledge, Download Priority, Perceived Sensitization, Perceived Intrusion, Intention to Use Mobile Apps.

1. Introduction

The exponential growth of smartphone and mobile app usage has revolutionized the way we live, work, and communicate (Bojjagani et al., 2023). Smartphones and mobile applications have become ubiquitous in modern society, but their design flaws have raised concerns about privacy and security (Pop, Hlédik, & Dabija, 2023). Kokolakis (2017) and Xu et al. (2012) have conducted studies and found that mobile apps are vulnerable to data theft and malware attacks, as they often collect personal data such as location and search history. One of the primary concerns is the way mobile apps handle permissions, as some apps request unnecessary permissions, leaving users vulnerable to data misuse or theft. Certain permission requests, such as those seeking access to a mobile device's location, camera, contacts, and so on, which pertain to privacy matters (Wottrich et al., 2018), may come across as intrusive to users' privacy and consequently trigger increased privacy concern (Degirmenci, 2020). When an app requests a greater number of permissions, mobile users tend to experience heightened discomfort, leading to an increased level of privacy concern regarding the app (Pentina et al., 2016;

Wu & Chen, 2017). Bisogni and Asghari (2020) analyzed that the consequences of such data breaches can be severe, compromising user privacy and potentially leading to identity theft or other forms of cybercrime.

Researchers in privacy concern is not a new phenomenon. Before the arrival of the internet and subsequent technological inventions like social media, mobile devices, and artificial intelligence, the concepts of personal data control where individuals exercise that control have developed (Hudson & Liu, 2023). Yun et al. (2019) posited that the work related to privacy concerns has seen significant growth over time. The impact of mobile app security breaches can be devastating, with data theft and malware attacks being some of the most common threats (Sun et al., 2021; Waldman, 2020). Attackers can steal login credentials, credit card information, and other sensitive personal information from vulnerable apps (Barth et al., 2022). Additionally, apps can track user activities and locations, sometimes without users' knowledge or consent.

The mobile app industry has seen tremendous growth in recent years. The Google Play Store hosts over 110 billion apps (Statista, 2022). These apps have revolutionized the way users interact with services and products, offering unparalleled convenience and accessibility (Rowe, 2020; Wang et al., 2021). However, with this convenience comes a significant risk to users' privacy and security. These vulnerabilities in mobile apps create an opportunity for cybercriminals to infiltrate security systems and steal confidential information. As mobile apps continue to gain popularity and are being used for various purposes, the risk of cyberattacks on these apps has increased significantly (Sun et al., 2021; Waldman, 2020).

Information Systems (IS) literature has explored individuals' perceptions of security and privacy in the context of various mobile technologies. Johnson, Kiser, Washington, and Torres (2018) studied factors influencing users' intentions to use mobile payment services and revealed that perceived security positively influences user intentions toward mobile app services. Keith et al. (2015) conducted a cost-benefit analysis of the factors that drive or deter the adoption of mobile apps. Their findings indicated that concerns related to privacy risks act as a deterrent, preventing users from adopting and sharing their information with mobile applications. Similarly, studies have been conducted on the technological dimensions which include examination into whether the gathered data are intended for direct marketing, utilized on the internet for e-commerce, acquired through mobile devices or location-enhanced technologies, or sourced from social networks (Mensah & Mwakapesa, 2022; Smith et al., 2011). Privacy risks associated with mobile apps are not limited to technical vulnerabilities. Many users unknowingly expose their personal information by granting unnecessary permissions to apps they download (Waldman, 2020). Apps often request access to sensitive information such as contacts, location, and camera, even when such permissions are not required for the app's functionality (Xu et al., 2012; Scherer et al., 2019). The importance of ensuring the security of mobile apps cannot be overstated as the consequences of a successful cyberattack can be severe, resulting in significant financial losses and damage to user privacy (Culnan & Williams, 2009).

The phenomenon of the privacy paradox is often observed where there exists a discrepancy between the expressed concern of users regarding their privacy and the actions they take while sharing their personal information (Xu et al., 2012). This behavior is widely recognized in various online platforms where users tend to reveal their personal information despite being aware of the potential risks associated with it (Culnan & Williams, 2009). Morando, Iemma, and Raiteri (2014) proposed that the privacy behavior of individuals varies depending on the context. Related to using and

downloading mobile applications, even customers show feelings of insecurity and safety concerns, the sharing of information within mobile apps continues to increase (Chennamaneni & Gupta, 2023; Zafeiropoulou et al. 2013). Research has indicated some factors behind the privacy paradox, which include weighing the privacy risk associated with using mobile apps against the benefits they offer, such as efficiency, convenience, and satisfaction (Barth & De Jong 2017). Previous research has been conducted in the context on non-mobile usage, such as mobile e-commerce, social networks, and electronic health records. There exists a scarcity of research regarding the privacy concerns of mobile app users and how these concerns influence users' intentions and behaviors in utilizing mobile applications. In addition, limited studies have focused on technical security knowledge and download priority intention to use mobile apps. In this regard, Degirmenci (2020) calls for further research to evaluate the factors that bridge the gap between users' privacy concerns and their behavior. Therefore, this study uses the Mobile Users' Information Privacy Concerns (MUIPC) framework to understand how users' prior experience, technical security knowledge, and download priority influence the intention to use mobile apps among mobile users. The MUIPC framework is particularly promising as it enables researchers to gain a better understanding of mobile users' information privacy concerns, which, in turn, can be leveraged to develop solutions that enhance users' privacy and security (Xu et al., 2012). Hence, the current study addresses the following research questions:

1. What is the level of knowledge about security and privacy concerns associated with mobile applications among mobile users?
2. What is the impact of prior privacy experiences on perceived surveillance, perceived intrusion, and secondary use of personal information?
3. What is the impact of customers' technical knowledge on perceived surveillance, perceived intrusion, and secondary use of personal information?
4. How does download priority influence perceived surveillance, perceived intrusion, and secondary use of personal information?
5. What is the impact of download priority on perceived surveillance, perceived intrusion, and secondary use of personal information?

Literature Review

1. Theoretical Foundation: Mobile users' Information Privacy Concerns (MUIPC)

The introduction of the MUIPC framework can be attributed to Xu et al. (2012), and it draws its foundations from the concepts of the concern for information privacy scale (CFIP) by Smith et al. (1996) and information privacy among Internet users (IUIPC) Malhotra et al. (2004). The CFIP scale evaluates individual concerns regarding the privacy practices of an organization. It uses four distinct subscales: unauthorized access, errors, data collection, and improper secondary utilization (Smith et al., 1996). The study conducted by Malhotra et al. (2004), used IUIPC as a means to assess how online consumers perceive and respond to different privacy risks on the internet. This approach is grounded in the principles of the social contract and justice theories and delineates three key aspects of privacy concerns: the management of personal information (related to procedural justice), gathering of personal data (related to distributive justice), and the awareness of an organization's information privacy practices (involving interactional and informational justice). Expanding upon these principles related to privacy, MUIPC leverages the communication privacy management theory

to address issues regarding information privacy in the context of mobile users. This framework categorizes mobile users' concerns into three dimensions for measurement: the perception of surveillance, the perception of intrusion, and the secondary use of personal information (Degirmenci, 2020).

This study further extends the body of literature by incorporating the antecedents of MUIPC. The current study proposes that prior privacy experience, download priority, technical knowledge, and desensitization are four potential antecedents of perceived surveillance, perceived intrusion, and secondary use of information that affect the individual's behavioral intention to use mobile apps.

1.1 Prior Privacy Experience

Prior privacy experience tends to exhibit greater levels of concern regarding an individual's information privacy (Smith et al., 1996; Degirmenci, 2020). Mobile users are likely to become more apprehensive about the privacy of their information when they have experienced information collection from the Internet or mobile applications (Belanger & Crossler, 2019). Individuals using mobile devices tend to feel like they are experiencing the misuse of their personal information (Zlatolas et al., 2015). The current study posits that mobile users are likely to encounter privacy-related issues. Therefore, it is assumed that prior privacy experience has a positive influence on privacy concerns. Hence, the following hypotheses are proposed:

H1: Prior privacy experience positively influences perceived surveillance.

H2: Prior privacy experience positively influences perceived intrusion.

H3: Prior privacy experience positively influences the secondary use of personal information.

1.2 Technical Security Knowledge

The increasing prevalence of interactive mobile technologies, especially, is expected to promote the sharing of personal data among the public (Park & Jang, 2014). The studies conducted in the United States samples revealed that the majority of consumers lack basic knowledge about marketing surveillance practices (Park, 2013). Likewise, another study revealed a lack of sufficient awareness regarding privacy among individuals when they use social networking platforms like Facebook (Acquisti & Gross, 2006).

Past empirical evidence in different domains of internet usage indicates that users exhibit varying levels of skill and knowledge that limit the ability of people to appropriately adapt to the digitization of personalized data on mobile platforms. Hence, the following hypotheses are proposed:

H4: Technical security knowledge negatively influences perceived surveillance.

H5: Technical security knowledge negatively influences perceived intrusion.

H6: Technical security knowledge negatively influences the secondary use of personal information.

1.3 Download Priority

Bansal (2017) posited that security is related to safeguarding, while privacy is primarily focused on governance and utilization. Past studies indicate that individuals with a strong overall concern for privacy might paradoxically proceed to acquire and install mobile applications (Kokolakis, 2017), even when these apps are known to excessively utilize or misuse their data (Zheng & Lee, 2016).

Despite the potential risks associated with mobile apps, many users continue to download and use them without fully considering the implications for their privacy (Pentina et al., 2016). Past studies indicate that down priority positively affects perceived surveillance, perceived intrusion, and secondary use of personal information. Hence, the following hypotheses are proposed:

H7: Download priority experience positively influences perceived surveillance.

H8: Download priority experience positively influences perceived intrusion.

H9: Download priority experience positively influences secondary use of personal information.

1.4 Desensitization

Desensitization denotes the trend where consumers progressively become less receptive to requests for permissions, especially when confronted with an excessive number of such requests, and subsequently proceed with the app installation (Harris et al., 2016). Desensitization has been explored across various domains including computer security warnings (Akhawe & Felt, 2013), and workplace warnings (Schwartz & Driver, 1983). Harris et al. (2016) revealed that desensitization served as an antecedent to trust and the assessment of risk concerning the intention to install applications. Based on these findings, it is assumed that desensitization has a negative influence on perceived surveillance, perceived intrusion, and secondary use of information. Hence, the following hypotheses are proposed:

H10: Desensitization will positively influence perceived surveillance.

H11: Desensitization will positively influence perceived intrusion.

H12: Desensitization will positively influence the secondary use of personal information.

1.5 Perceived Surveillance

Perceived surveillance refers to the monitoring and profiling of mobile device users using the functionalities of mobile technology, which include environmental sensors like integrated cameras, global positioning system (GPS) receivers, proximity sensors, and accelerometers (Xu et al., 2012). Concerning mobile apps, perceived surveillance of their activities, communications, and personal information being monitored, tracked, or recorded by others is referred to as a crucial factor (Wang et al., 2021). When personal information is collected without the users' knowledge or consent, they may feel uneasy about their privacy, leading to concerns. Past studies have identified that perceived surveillance negatively influences users' privacy concerns (Aditya et al., 2014; Xu et al., 2012). Hence, the following hypothesis is proposed:

H13: Perceived surveillance will negatively influence the behavioral intention of using mobile apps.

1.6 Perceived Intrusion

The concept of intrusion refers to the degree to which people perceive that their private space, data, or communication channels are being encroached upon by external sources (Xu et al., 2012). The sensors in mobile technology provide several benefits that include orientation, positioning, and motion which improve users' performance. However, these sensors posed potential privacy concerns, resulting in the inadvertent disclosure of information (Keith et al., 2015; Degirmenci, 2020), which is strongly associated with the intrusion of privacy. Solove (2006) posited that incursions into an

individual's personal life disrupt their daily routines, change their habits, erode their sense of privacy, and frequently result in feelings of discomfort and unease. Enck (2011) indicates that many apps often request location access needlessly which leads to privacy breaches. Hence, the following hypothesis is proposed:

H14: Perceived intrusion will positively influence the behavioral intention of using mobile apps.

1.7 Secondary Use of Personal Information

Secondary use of personal information refers to the use of data for objectives, without obtaining the consent of the data subject, which is not related to the purpose of data collection (Solove, 2006). The collection of personal information allows companies to utilize data for marketing objectives, such as enhancing the precision of tailored offers based on individual preferences (Culnan & Armstrong, 1999). For example, the recent Facebook privacy scandal involving Cambridge Analytica highlighted the unauthorized collection of personal data from around 87 million Facebook users, revealing a secondary use of their information without their explicit consent (Degirmenci, 2020).

When it comes to mobile apps, individuals may feel uncomfortable with the idea that their personal information is being utilized for purposes they did not explicitly agree to, which can result in heightened privacy concerns. This factor has been identified as a significant predictor of privacy concerns among mobile app users (Kusyanti et al., 2022; Wang et al., 2021). Hence, the following hypothesis is proposed:

H15: Secondary use of personal information will negatively influence the behavioral intention of using mobile apps.

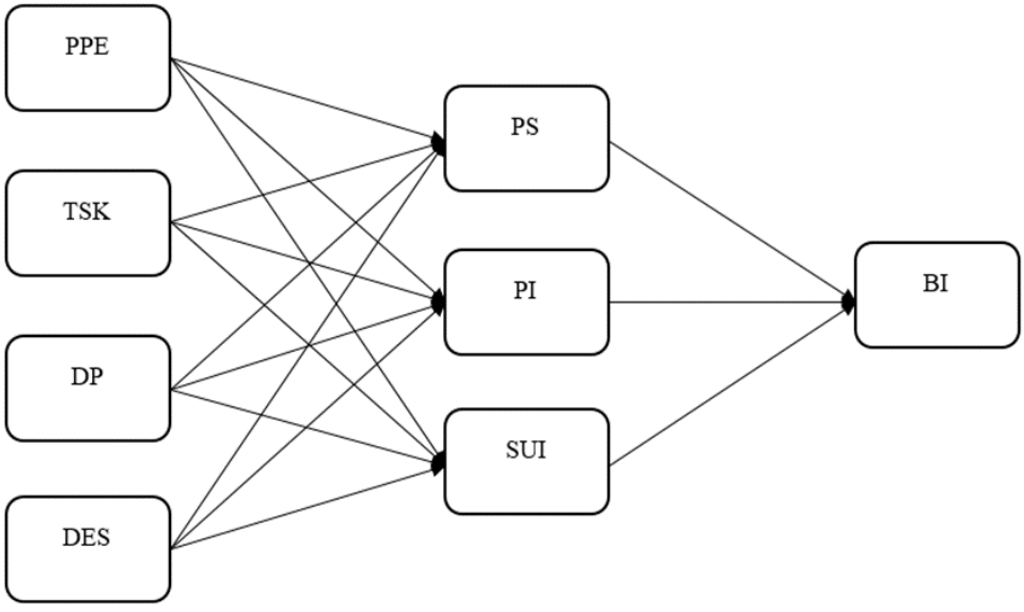

Fig. 1. Conceptual model.

Note(s): PPE = Prior privacy experience; TSK = Technical security knowledge; DP = Download priority; DES = Desensitization; PS = Perceived surveillance; PI = Perceived intrusion; SUI = Secondary use of information; BI = Behavioral intention to App.

Methodology

1. Instrument

The questionnaire used in the study consists of various demographic and psychographic questions to assess participants' privacy behavior and attitudes toward mobile app privacy. The demographic section includes questions such as year of birth, highest level of education, sex, and current country and state of residence. The psychographic section comprises seven questions on technical security knowledge (TSK), which has been modified from the original study by Barth et al. (2019), to assess participants' understanding of the technical aspects of mobile app security. The section also contains three questions on download priority (DP), modified from a self-developing questionnaire, which measures the extent to which participants consider different aspects when downloading mobile apps. Furthermore, the questionnaire includes two questions on desensitization (DES), modified from a study by Harris et al. (2016), to assess participants' tendency to ignore permission requests when installing mobile apps. It also comprises three questions on perceived surveillance (PS) and three questions on perceived intrusion (PI), which have been adapted from studies by Xu et al. (2012) and Dinev et al. (2013), respectively, to evaluate participants' beliefs about mobile app surveillance and invasion of privacy. Finally, the questionnaire includes three questions on prior privacy experience (PPE), which assesses participants' previous experiences with mobile app privacy and potential misuse of personal information, modified from an unpublished study. Participants were required to rate their level of agreement with the statements on a 5-point Likert scale, ranging from strongly disagree to strongly agree.

2. Sampling and Data Collection

The research methods used in this study were survey methods (Ketchen & Bergh, 2006), where a questionnaire was sent to mobile app users to assess their intention to use mobile apps. The survey was designed to capture information related to demographics, prior privacy experience, technical security knowledge, download priority, desensitization, mobile app use, and perceptions of privacy concerns. The convenience sampling method was employed to collect the data using an online survey. The survey questionnaire was distributed through various social media platforms and online forums. The target population for the study was individuals who use mobile apps, regardless of age or gender.

A total of 450 questionnaires have been disseminated through online platforms, out of which 290 respondents have filled them out, resulting in a response rate of 64.44%. The data collection took three months from March 2023 to May 2023.

Data Analysis

The data analysis was performed via SPSS 26 version and SmartPLS 4.0 version. SPSS was used to perform descriptive statistics including mean, standard deviation, frequency, and percentage (Ketchen & Bergh, 2006). SmartPLS was used for the Partial Least Squares Structural Equation Modeling (PLS-SEM).

Partial Least Squares Structural Equation Modeling (PLS-SEM) is a statistical technique used for analyzing the relationships between sets of variables. Compared to CB-SEM, PLS-SEM is a more suitable technique when the sample size is small or the data is non-normal, and when the focus is on predictive modeling rather than theory testing (Hair et al., 2019). In this study, PLS-SEM was chosen because the data collected had a small sample size, the variables were non-normal, and the focus was

on predicting the dependent variable. PLS-SEM estimates partial model structures by combining principal components analysis with ordinary least squares regressions (MateosAparicio, 2011). It is considered an alternative to Jöreskog's (1973) CB-SEM, which has numerous, typically very restrictive, assumptions (Hair et al., 2011).

CB-SEM estimates model parameters by considering only common variance in the covariance matrix and is often executed using software packages such as LISREL or AMOS. In contrast, PLS-SEM is variance-based and accounts for total variance to estimate parameters (Hair et al., 2017). It is also a multivariate technique that identifies latent variables that best explain the observed variance in the data.

PLS-SEM consists of two approach methods, assessment of measurement model and structural model. The measurement model was assessed to ensure that data is suitable for further analysis. A structural model was performed to test the hypotheses using the bootstrapping method. The results of the study are given in the following sections.

1. Participants Profile

A total of 290 respondents participated in the survey, and their birth years were categorized into four age groups: 18-29, 30-39, 40-49, and 50 or older. The largest age group among the respondents was 30-39, with 106 respondents (36.6% of the sample). The second largest group was 18-29, with 65 respondents (22.4% of the sample). The age groups of 40-49 and 50 or older had 58 and 61 respondents respectively, representing 20.0% and 21.0% of the sample. The results show that out of the 290 participants, the largest group was those who had completed a bachelor's degree in college, with 131 respondents, representing 45.2% of the sample. The second-largest group was high school graduates, with 79 respondents (27.2% of the sample). The third-largest group was those with a master's degree, with 36 respondents (12.4% of the sample). In addition, the data shows that 33 respondents (11.4% of the sample) had completed an associate degree in college (2 years), 5 respondents (1.7% of the sample) had completed a doctoral degree, and 6 respondents (2.1% of the sample) had completed a professional degree (JD, MD). The details of the participants' demographic are shown in Table 1.

Table 1. Participants' Demographic.

Description	Sample (N = 290)	Percentage (%)
Gender		
Male	146	50.3
Female	142	49.0
Other	2	0.7
Total	290	100
Age		
18 to 29	65	22.4
30 to 39	106	36.6
40 to 49	58	20.0
50 or more	61	21.0
Total	290	100
Education		
High School Graduate	79	27.1
Associate degree (2 years)	33	11.4
Bachelor's degree (4 years)	131	45.2
Master's degree	36	12.4
Doctorate	5	1.7
Professional Degree (JD and MD)	6	2.1
Total	290	100

2. Measurement Model Assessment

It is important to assess the internal consistency reliability of the constructs being measured. Cronbach's alpha and composite reliability values were assessed to ensure internal consistency in data reliability. Generally, values between 0.60 and 0.70 are considered acceptable in exploratory research, while values between 0.70 and 0.90 are considered satisfactory to good. However, values above 0.95 indicate that the items may be redundant and can lead to reduced construct validity (Hair, Risher, Sarstedt, & Ringle, 2019). In this study, the values of Cronbach's alpha for the variables Desensitization and Prior privacy experience are below 0.70. This is because Cronbach's alpha does not consider the individual loadings of each item in the construct. Although Cronbach's alpha is viewed as too conservative, composite reliability can be too liberal, and the true reliability of the construct typically lies within these two values (Hair et al., 2019). Composite reliability is based on weighted loadings, and therefore, it is a more precise measure of reliability. Jöreskog's composite reliability is a commonly used measure that indicates how well the different items in a construct are correlated with each other. A higher value of composite reliability indicates a higher level of reliability of the construct. According to the results obtained, the composite reliability values for all the variables are above 0.70 (as shown in Table 2 and Figure 2), indicating the internal consistency of the data.

Table 2. Measurement model validity.

	Items	FL	VIF	Cronbach's α	CR	AVE
Behavioral intention	BI1	0.938	3.527	0.924	0.952	0.867
	BI2	0.927	3.405			
	BI3	0.929	3.534			
Desensitization	DES1	0.942	1.254	0.620	0.825	0.705
	DES2	0.723	1.254			
Download Priority	DP1	0.851	1.644	0.739	0.852	0.657
	DP2	0.778	1.452			
	DP3	0.801	1.403			
Perceived Intrusion	PI1	0.864	2.166	0.873	0.922	0.797
	PI2	0.909	2.495			
	PI3	0.905	2.419			
Prior privacy experience	PPE1	0.690	1.266	0.663	0.809	0.589
	PPE2	0.697	1.266			
	PPE3	0.898	1.417			
Perceived Surveillance	PS1	0.651	1.146	0.717	0.844	0.647
	PS2	0.868	2.090			
	PS3	0.875	2.074			
Secondary use of personal information	SUI1	0.935	3.637	0.925	0.952	0.869
	SUI2	0.935	3.468			
	SUI3	0.927	3.484			
Technical security knowledge	TSK1	0.705	1.209	0.867	0.891	0.579
	TSK2	0.739	1.892			
	TSK3	0.842	2.695			
	TSK4	0.844	3.139			
	TSK5	0.702	2.123			
	TSK7	0.718	2.078			

Note(s): FL = Factor loading; CR = Composite reliability; AVE = Average variance extracted; VIF = Variance inflation factor.

The second step in assessing the reflective measurement model is to evaluate the convergent validity of each construct measure. Convergent validity refers to the extent to which a construct explains the variance of its items. This is measured using the average variance extracted (AVE) for all items on each construct. An acceptable AVE is 0.50 or higher, which indicates that the construct

explains at least 50% of the variance of its items (Hair et al., 2019). Based on the results presented in Table 2, it can be observed that all variables have attained the recommended threshold value 0.50, thus confirming the convergent validity.

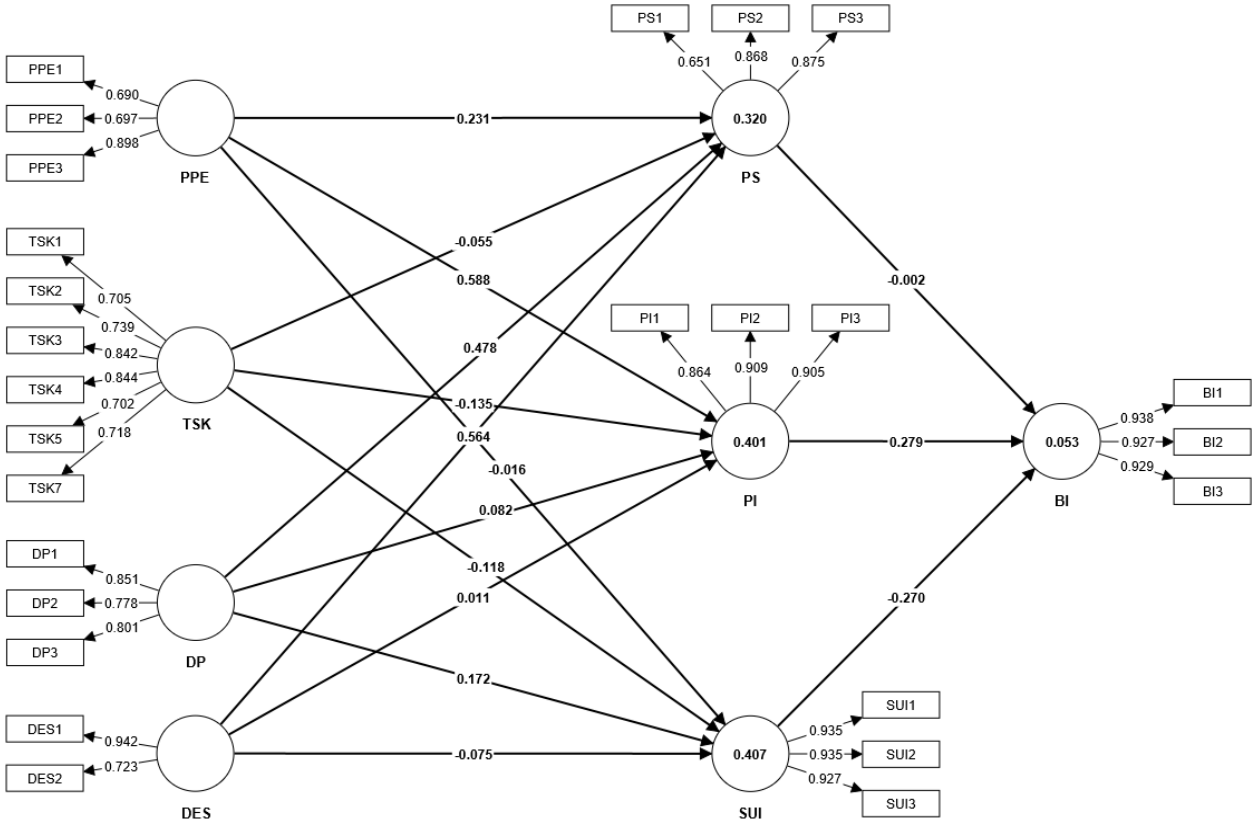

Fig. 1.

The third step of measurement model evaluation is the assessment of discriminant validity. Discriminant validity refers to the extent to which a construct is empirically distinct from other constructs in the structural model (Hair et al., 2019). Fornell and Larcker (1981) proposed the traditional metric, which compares each construct's AVE to the squared inter-construct correlation. In order to confirm the discriminant validity via Fornell and Larcker (1981) criterion, the values squared root of AVE of each variable must be greater than the inter-correlation among other variables. The values of AVE The results presented in Table 3 confirm the discriminant validity via Fornell and Larcker (1981) criterion. However, Henseler et al. (2015) showed that this criterion does not perform well when the indicator loadings on a construct differ only slightly. Therefore, they proposed the heterotrait-monotrait (HTMT) ratio of the correlations as a replacement for the Fornell-Larcker criterion (Voorhees et al., 2016).

The HTMT is the mean value of the item correlations across constructs relative to the average correlations for the items measuring the same construct (Hair et al., 2019). Discriminant validity problems arise when HTMT values are high. Henseler et al. (2015) suggest a threshold value of 0.90 for structural models with constructs that are conceptually very similar. For constructs that are conceptually more distinct, a lower, more conservative threshold value of 0.85 is suggested (Henseler

et al., 2015). According to the results presented in Table 4, it can be concluded that the model achieves discriminant validity, as the HTMT values are below the recommended threshold values.

Table 3. Discriminant validity via Fornell-Larcker criterion.

	BI	DES	DP	PI	PPE	PS	SUI	TSK
BI	**0.931**							
DES	0.233	**0.840**						
DP	0.015	0.012	**0.811**					
PI	0.103	0.024	0.168	**0.893**				
PPE	0.049	0.026	0.157	0.615	**0.768**			
PS	0.008	-0.005	0.512	0.379	0.311	**0.805**		
SUI	-0.090	-0.062	0.254	0.648	0.601	0.354	**0.932**	
TSK	0.058	0.024	0.043	-0.191	-0.101	-0.059	-0.170	**0.761**

Table 4. Discriminant Validity via Heterotrait-monotrait ratio (HTMT) Criterion.

	BI	DES	DP	PI	PPE	PS	SUI	TSK
BI								
DES	0.263							
DP	0.045	0.066						
PI	0.112	0.068	0.211					
PPE	0.117	0.164	0.208	0.737				
PS	0.088	0.066	0.706	0.466	0.437			
SUI	0.100	0.074	0.305	0.720	0.702	0.423		
TSK	0.067	0.144	0.080	0.178	0.257	0.088	0.151	

2. Structural Model Assessment

Once the measurement model assessment has been deemed satisfactory, the next step in evaluating the results of PLS-SEM is to assess the structural model. To ensure that collinearity does not bias the regression results, it is necessary to examine collinearity before assessing the structural relationships. VIF values greater than 5 are indicative of potential collinearity issues among the predictor constructs, although collinearity problems can occur at VIF values between 3 and 5. Ideally, the VIF values should be close to 3 or lower. If collinearity is an issue, one frequently used option is to construct higher-order models that are supported by theory (Hair et al., 2017). The values of VIF as presented in Table 2 indicate that collinearity is not an issue for this study. Therefore, the data is suitable for the analysis of the structural model.

Criteria for standard assessment include the coefficient of determination (R2), the Q2 measure based on blindfolding cross-validation, and the statistical significance and relevance of path coefficients. The R^2 measures the amount of variance that is explained by each of the endogenous constructs and serves as an indicator of the model's explanatory power (Shmueli & Koppius, 2011). The R^2 is also referred to as in-sample predictive power (Rigdon, 2012), and it ranges from 0 to 1, with higher values indicating a greater degree of explanatory power. Generally, R^2 values of 0.75, 0.50, and 0.25 are considered substantial, moderate, and weak, respectively (Hair et al., 2011; J. Henseler et al., 2009). Based on the results presented in Table 5, it can be concluded that secondary use of information has the highest R^2 values (0.407).

Behavioral intention, on the other hand, has the lowest R^2 value (.053), which is considered weak. To evaluate the predictive accuracy of the PLS path model, another approach is to compute the Q^2 value (Geisser, 1974; Stone, 1974). As a general guideline, Q^2 values should be greater than zero for a particular endogenous construct to indicate the predictive accuracy of the structural model for that construct. In general, Q^2 values above 0, 0.25, and 0.50 are indicative of small, medium, and

large predictive relevance of the PLS path model, respectively (Hair et al., 2019). Based on the findings presented in Table 5, it can be concluded that all endogenous constructs have Q^2 values greater than zero, which supports the model's predictive relevance.

Table 5. Model predictive power.

Construct	R square	Q Square
Behavioral Intention	0.053	0.002
Perceived Intrusion	0.401	0.374
Perceived Surveillance	0.320	0.290
Secondary use of information	0.407	0.380

3. Out-of-sample Predictive Power

It is common for researchers to consider the R^2 statistic as an indicator of their model's predictive ability. However, this is not entirely accurate because R^2 only measures the model's explanatory power on the sample data, without considering its ability to predict out-of-sample data (Hair et al, 2019). To address this issue, Shmueli et al. (2015) proposed the PLS prediction procedure, which involves estimating the model on a training sample and evaluating its predictive performance on a holdout sample. When using PLS prediction, it is recommended to focus on the key endogenous construct rather than on all indicators. Researchers should compare the RMSE (or MAE) values with a naïve benchmark to evaluate the predictive performance of the model. The Q^2 prediction statistic should be evaluated first to verify if the predictions outperform the most naïve benchmark (Hair et al, 2019).

When comparing the RMSE (or MAE) values with the naïve LM benchmark, several guidelines apply. If the PLS-SEM analysis yields higher prediction errors in terms of RMSE (or MAE) for all indicators compared to the naïve LM benchmark, it indicates that the model lacks predictive power. If the majority of the dependent construct indicators in the PLS-SEM analysis produce higher prediction errors compared to the naïve LM benchmark, this indicates that the model has low predictive power. If the minority or the same number of indicators in the PLS-SEM analysis yields higher prediction errors compared to the naïve LM benchmark, it indicates medium predictive power. If none of the indicators in the PLS-SEM analysis have higher RMSE (or MAE) values compared to the naïve LM benchmark, it indicates that the model has high predictive power.

According to the results presented in Table 6, all Q^2_predict values in the final model are greater than 0, indicating that the model performs better than a naïve prediction. The PLS-based prediction yields more accurate out-of-sample predictions (i.e., smaller prediction errors) for the minority of indicators. The model has low predictive power for Behavioral intentions.

4. Hypotheses Testing

Once the model's explanatory and predictive power has been established, the final stage is to evaluate the statistical significance and relevance of the path coefficients. The path coefficients are interpreted in a similar way to the formative indicator weights, and bootstrapping is required to determine their significance. Typically, path coefficients range from -1 to +1, and their values should be evaluated (Nitzl, 2016; Hair et al., 2019).

The assessment of the structural model included 15 hypotheses as shown in Figure 3. The results of the study indicate that out of 15 proposed hypotheses, 9 are accepted. Hypotheses 1, 2, and 3 proposed positive influence of prior privacy experience on perceived surveillance ($\beta=0.231$, $p<0.05$), perceived intrusion ($\beta=0.588$, $p<0.05$), and secondary use of personal information ($\beta=0.564$, $p<0.05$),

are supported. Hypotheses 4 proposed the negative influence of technical security knowledge on perceived intrusion was insignificant (β=-0.055, p>0.05). Hypotheses 5 and 6 proposed the negative influence of technical security knowledge on perceived intrusion (β=-0.135, p<0.05) and secondary use of personal information (β=-0.118, p<0.05), are supported. Hypotheses 7 and 9 proposed positive and significant influence of download priority on perceived surveillance (β=0.478, p<0.05), and secondary use of personal information (β=0. 172, p<0.05), were supported. Hypothesis 8 proposed a positive influence of download priority on perceived intrusion (β=0.082, p>0.05), was not supported. Hypotheses 10, 11, and 12 proposed the negative influence of desensitization on perceived surveillance (β=-0.016, p>0.05), perceived intrusion (β=0.011, p>0.05), and secondary use of personal information (β=-0.075, p>0.05), are not supported. Hypothesis 13 proposed the negative influence of perceived surveillance on behavioral intention to use mobile apps (β=-0.002, p>0.05), was not supported. Hypothesis 14 proposed negative influence of perceived intrusion on behavioral intention to use mobile apps (β=0.279, p<0.05), was not supported. Hypothesis 15 proposed the negative influence of secondary use of information on behavioral intention to use mobile apps (β=-0.270, p<0.05), was supported. The results are summarized in Table 7.

Table 6. PLS predict values.

Constructs indicators	Q^2predict	PLS-SEM_RMSE	PLS-SEM_MAE	LM_RMSE	LM_MAE
BI1	0.001	1.081	0.907	1.076	0.913
BI2	-0.001	1.036	0.872	1.046	0.893
BI3	0.005	1.052	0.861	1.044	0.875
PI1	0.208	0.848	0.664	0.857	0.662
PI2	0.326	0.770	0.589	0.777	0.580
PI3	0.347	0.739	0.567	0.712	0.514
PS1	0.142	0.790	0.596	0.794	0.605
PS2	0.190	0.822	0.652	0.847	0.678
PS3	0.229	0.805	0.631	0.828	0.646
SUI1	0.325	0.774	0.583	0.775	0.572
SUI2	0.381	0.754	0.569	0.755	0.557
SUI3	0.274	0.790	0.586	0.779	0.572

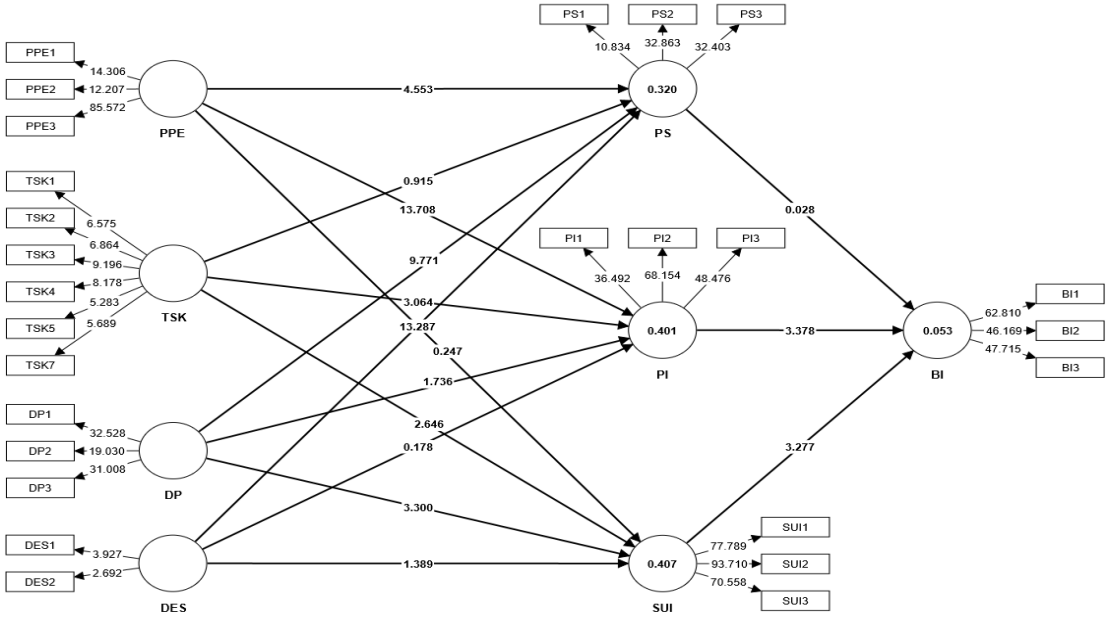

Fig. 1. Structural model.

Table 7. Hypotheses testing.

	Path coefficient	T values	P values	Decision
H1: Prior privacy experience -> Surveillance	0.231	4.553	0.000	**Supported**
H2: Prior privacy experience -> Perceived intrusion	0.588	13.708	0.000	**Supported**
H3: Prior privacy experience -> Secondary use of information	0.564	13.287	0.000	**Supported**
H4: Technical security knowledge -> Perceived Surveillance	-0.055	0.915	0.360	Not supported
H5: Technical security knowledge -> Perceived intrusion	-0.135	3.064	0.002	**Supported**
H6: Technical security knowledge -> Secondary use of information	-0.118	2.646	0.008	**Supported**
H7: Download Priority -> Perceived Surveillance	0.478	9.771	0.000	**Supported**
H8: Download Priority -> Perceived intrusion	0.082	1.736	0.083	Not supported
H9: Download Priority -> Secondary use of information	0.172	3.300	0.001	**Supported**
H10: Desensitization -> Perceived Surveillance	-0.016	0.247	0.805	Not supported
H11: Desensitization -> Perceived intrusion	0.011	0.178	0.859	Not supported
H12: Desensitization -> Secondary use of information	-0.075	1.389	0.165	Not supported
H13: Perceived Surveillance -> Behavioral intention	-0.002	0.028	0.978	Not supported
H14: Perceived intrusion -> Behavioral intention	0.279	3.378	0.001	**Supported**
H15: Secondary use of information -> Behavioral intention	-0.270	3.277	0.001	**Supported**

Discussion

This study aimed to investigate the effect of technical security knowledge, prior privacy experience, download priority, perceived intrusion, perceived surveillance, and secondary use of personal information on behavioral intention to use mobile apps. The study used the MUIPC framework proposed by Degirmenci (2020) and Kusyanti et al. (2022) suggests that perceived risk and perceived benefit interact with each other to influence users' privacy behavior and ultimately determine whether or not they adopt privacy protection measures. The framework MUIPC is important to understand the complex nature of privacy concerns among mobile users.

The study's results also support the importance of prior privacy experience in influencing users' perceptions of surveillance, intrusion, and secondary use of personal information. This suggests that users who have had more prior experience with privacy concerns may be more aware of potential privacy threats when using mobile apps. This finding is consistent with previous studies that have found prior experience to be an important factor in determining users' privacy concerns (Ketelaar & Balen, 2018; Xu et al., 2012). These findings indicate that individuals previous experiences regarding the breach of privacy have greatly influenced privacy concerns. It also shows that individuals have become more skeptical towards mobile apps and sharing personal data online due to their past experiences. The study's results suggest that technical security knowledge may also play a role in influencing users' perceptions of surveillance and intrusion. Specifically, individuals with higher technical security knowledge may perceive less intrusion and surveillance when using mobile apps, while individuals who are more desensitized to privacy concerns may perceive less surveillance. These findings are consistent with previous research that has identified the importance of technical knowledge in mitigating privacy concerns (Harborth & Pape, 2020), and the impact of desensitization on users' privacy perceptions (Dinev & Hart, 2006).

In addition, the results indicate that download priority positively influences perceived surveillance and secondary use of personal information, which is consistent with the findings of

Pentina et al. (2016). These results indicate that individual users are aware that downloading apps has no adverse impact on users' surveillance and use of information. However, the positive influence of download priority on perceived intrusion was insignificant signifying app deterrence in individual privacy. The findings indicate that download priority has no effect on the individual feeling of intrusion. In other words, it depicts that download priority for mobile apps does not bother users because they don't feel that their privacy is being intruded upon. The findings indicate that desensitization did not significantly affect perceived surveillance, perceived intrusion, or secondary use of personal information. This suggests that users who are more desensitized to privacy concerns may perceive less surveillance when using mobile apps. However, these factors did not significantly affect users' willingness to use mobile apps.

Furthermore, the results indicate that the negative influence of perceived surveillance on behavioral intention was not significant. This suggests that individual users perceive that mobile app surveillance is breaching their privacy. These findings are consistent with past researchers who argued that surveillance from app developers contributes to users' privacy concerns (Wang et al., 2021; Aditya et al., 2014; Xu et al., 2012). The study's findings further suggest that perceived intrusion has a positive effect on behavioral intention to use mobile apps, which is inconsistent with previous research (Pentina et al., 2016). They highlighted that intrusion has a negative effect on the use of mobile apps. This suggests that users may be less concerned about these factors when deciding to use mobile apps, and that other factors, such as perceived benefit and trust, significantly influence their decision-making. The present study also found that secondary use of personal information had a negative and significant effect on users' behavioral intention to use mobile apps. This suggests that users were concerned about the secondary use of their personal information, which affected their willingness to use mobile apps. This finding is consistent with previous studies that have found secondary use of personal information to be a significant predictor of privacy concerns among mobile app users (Kusyanti et al., 2022; Wang et al., 2021).

Implications

1. Theoretical Implications

Theoretically, this study adds to the MUIPC framework in several ways. First, the study adds to the literature on mobile app usage among customers. Past studies have only focused on mobile payment, e-commerce transactions, or online purchasing security risks. Second, this study used a comprehensive MUIPC framework that confirmed the influence of prior privacy experience, technical security knowledge, and downloading priority on user mobile users' privacy concerns. Previous studies have assessed the influence of privacy information, technical knowledge, technical awareness, and privacy risk associated (Degirmenci, 2020; Barth et al., 2019; Johnson et al., 2018). Third, this study confirmed the positive influence of prior privacy experience on surveillance, perceived intrusion, and secondary use of personal data. Fourth, the study established the positive influence of technical security knowledge and perceived intrusion and secondary use of personal data. The conceptual framework of the current study provides a comprehensive understanding of various factors affecting privacy concerns among mobile users.

2. Practical Implications

There are numerous implications of the current research based on the findings. First, the findings of the study proved that prior privacy experience has a positive influence on surveillance,

perceived intrusion, and secondary use of data. These findings suggest that individuals who have prior privacy experience are aware of the potential consequences of surveillance and tend to be more conscious of using mobile apps. People who experienced privacy intrusion are more resilient towards intrusion which reduces their vulnerability while using mobile apps. The positive influence of prior privacy experience on secondary data usage suggests individuals who experienced the privacy breach and use of personal data may expect transparency from the organizations using their data. Therefore, the companies involved in mobile app design must ponder on the regulations and policies that eventually benefit the users and reduce skepticism towards mobile apps. The positive influence of technical security knowledge on perceived intrusion and secondary use of information suggests that users with technical knowledge have enriched their knowledge of the potential intrusion through mobile app usage. Therefore, it is recommended to integrate a system protection mechanism that will detect the intrusion and make sure personal data will not be compromised. These measures will help to increase the installation and usage of mobile apps and increase the company's credibility. Furthermore, the findings indicate that the download priority of the app has a positive influence on surveillance and secondary use of data. It is recommended that app developers should properly communicate with users regarding app downloading by providing the guidelines of using the app and how they will use the data. These measures will develop the trust and mitigate privacy concerns of the users regarding app downloading. Furthermore, the study's findings confirmed the negative influence of secondary use of information on intention to use mobile apps. The results indicate that mobile users are very cautious regarding the use of data by the app developers, therefore, they avoid frequent usage of mobile apps. It is recommended to app developers to provide option to users to limit the usage of data for secondary purposes. In this way, individual will have higher control over the data usage for secondary purpose. In addition, it will help to build trust and enhance app developer reputation that positively influences the adoption of mobile apps.

Conclusion

This study intends to understand mobile users' behavioral intention to use mobile apps. The study employed the MUIPC framework to investigate the factors influencing individuals' perceptions of surveillance, intrusion, and secondary use of personal information when using mobile apps, and their impact on behavioral intention. Prior privacy experience, technical security knowledge, and desensitization were set as predictors of the MUIPC framework. A survey method was utilized to collect the data from the users of smartmobile phones. The findings of the study indicate that individual prior experience, technical security knowledge, and download priority have a significant impact on perceived surveillance, perceived intrusion, and secondary use of personal information. However, the findings of the study revealed that desensitization does not influence the adoption of mobile apps. Further, the study findings confirm the significant effect of perceived intrusion and secondary use of personal information. Overall, the present study provides valuable insights into the complex nature of privacy concerns among mobile users. The findings suggest that factors such as perceived surveillance, prior privacy experience, and technical security knowledge are important determinants of users' privacy concerns and behavior when using mobile apps. These findings can inform the design of privacy-aware mobile applications that take into account users' privacy concerns and provide them with the necessary tools to protect their privacy. Further research is helpful to understand the underlying factors that contribute to users' privacy concerns and behavior when using mobile apps and to develop effective privacy protection measures that address these concerns.

Limitations and Future Research

The current study comprehensively studied the factors affecting the adoption of mobile apps among smartphone users, but it also has limitations. The primary limitation of the study current study is that the data were collected using a self-reported survey, which may be subject to response bias. Therefore, it is recommended that future researchers should employ a mixed approach to understand the underlying factors of mobile users' privacy concerns. Secondly, the study focused only on three factors influencing privacy concerns, while other factors, such as perceived benefit and trust, may also play a significant role in users' privacy attitudes and behaviors. Future research should explore these factors in greater depth and investigate their impact on mobile app users' privacy concerns.

References

Acquisti, A., & Gross, R. (2006). Imagined communities: awareness, information sharing, and privacy on the Facebook. Proceedings of Privacy Enhancing Technologies Workshop (PET), Lecture Notes in Computer Science, Springer, 36–58.

Aditya, P., Bhattacharjee, B., Druschel, P., Erdélyi, V., & Lentz, M. (2014, September). Brave new world: Privacy risks for mobile users. In Proceedings of the ACM MobiCom workshop on Security and privacy in mobile environments (pp. 7-12).

Akhawe, D., & Felt, A. P. (2013). Alice in warningland: a {Large-Scale} field study of browser security warning effectiveness. In 22nd USENIX security symposium (USENIX Security 13) (pp. 257-272).

Bansal, G. (2017). Distinguishing between privacy and security concerns: An empirical examination and scale validation. Journal of Computer Information Systems, 57(4), 330-343.

Barth, S., & De Jong, M. D. (2017). The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. Telematics and informatics, 34(7), 1038-1058.

Barth, S., de Jong, M. D., & Junger, M. (2022). Lost in privacy? Online privacy from a cybersecurity expert perspective. Telematics and informatics, 68, 101782.

Barth, S., de Jong, M. D., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. Telematics and informatics, 41, 55-69.

Bélanger, F., & Crossler, R. E. (2019). Dealing with digital traces: Understanding protective behaviors on mobile devices. The Journal of Strategic Information Systems, 28(1), 34-49.

Bisogni, F., & Asghari, H. (2020). More than a suspect: An investigation into the connection between data breaches, identity theft, and data breach notification laws. Journal of Information Policy, 10, 45-82.

Bojjagani, S., Sastry, V. N., Chen, C. M., Kumari, S., & Khan, M. K. (2023). Systematic survey of mobile payments, protocols, and security infrastructure. Journal of Ambient Intelligence and Humanized Computing, 14(1), 609-654.

Chennamaneni, A., & Gupta, B. (2023). The privacy protection behaviours of the mobile app users: Exploring the role of neuroticism and protection motivation theory. Behaviour & Information Technology, 42(12), 2011-2029.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. Organization Science, 10(1), 104- 115.

Culnan, M.J., &Williams, C.C. (2009). How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and Tjx Data Breaches, MIS Quarterly. 33(4), 673-687.

Degirmenci, K. (2020). Mobile users' information privacy concerns and the role of app permission requests. International Journal of Information Management, 50, 261-272.

Degirmenci, K. (2020). Mobile users' information privacy concerns and the role of app permission requests. International Journal of Information Management, 50, 261-272.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. Information Systems Research, 17(1), 61-80.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. European Journal of Information Systems, 22(3), 295-316.

Enck, W. (2011). Defending users against smartphone apps: Techniques and future directions. In S. Jajodia & C. Mazumdar (Eds.), Information systems security (Lecture Notes in Computer Science ed., Vol. 7093, pp. 49-70). Berlin: Springer.

Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. Journal of Marketing Research, 18(1), 39. https://doi.org/10.2307/3151312.

Geisser, S. (1974). A predictive approach to the random effect model. Biometrika, 61(1), 101–107. https://doi.org/10.1093/biomet/61.1.101.

Gu, J., Xu, Y. C., Xu, H., Zhang, C., & Ling, H. (2017). Privacy concerns for mobile app download: An elaboration likelihood model perspective. Decision Support Systems, 94, 19-28.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM).

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. Journal of Marketing Theory and Practice, 19(2), 139–152. https://doi.org/10.2753/MTP1069-6679190202.

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. European Business Review, 31(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203.

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. European business review, 31(1), 2-24.

Harborth, D., & Pape, S. (2020). How Privacy Concerns, Trust and Risk Beliefs, and Privacy Literacy Influence Users' Intentions to Use Privacy-Enhancing Technologies. ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 51(1), 51–69.

Harris, M. A., Chin, A. G., & Brookshire, R. (2015). Mobile app installation: the role of precautions and desensitization. Journal of International Technology and Information Management, 24(4), 3.

Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. In P. N. Sinkovics, R.R. and Ghauri (Ed.), Advances in International Marketing (pp. 277–320). Emerald, Bingley.

Henseler, Jörg, Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. Journal of the Academy of Marketing Science, 43(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8.

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.

Jang, C., & Sung, W. (2021). Beyond the privacy paradox: The moderating effect of online privacy concerns on online service use behavior. Telematics and Informatics, 65, 101715.

Johnson, V. L., Kiser, A., Washington, R., & Torres, R. (2018). Limitations to the rapid adoption of M-payment services: Understanding the impact of privacy risk on M-Payment services. Computers in Human Behavior, 79, 111-122.

Keith, M. J., Babb, J. S., Lowry, P. B., Furner, C. P., & Abdullat, A. (2015). The role of mobile-computing self-efficacy in consumer information disclosure. Information Systems Journal, 25(6), 637-667.

Ketchen Jr, D. J., & Bergh, D. D. (2006). Research methodology in strategy and management. Emerald Group Publishing.

Ketelaar, P. E., & van Balen, M. (2018). The smartphone as your follower: The role of smartphone literacy in the relation between privacy concerns, attitude and behaviour towards phone-embedded tracking. Computers in Human Behavior, 78, 174–182.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & security, 64, 122-134.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & security, 64, 122-134.

Kusyanti, A., Santoso, N., Catherina, H. P. A., & Oktavia, E. (2022). Investigating mobile users' intention: Technology acceptance and privacy perspectives. Procedia Computer Science, 197, 576-582.

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.

Mateos-Aparicio, G. (2011). Partial least squares (PLS) methods: Origins, evolution, and application to social sciences. Communications in Statistics-Theory and Methods, 40(13), 2305-2317.

Mensah, I. K., & Mwakapesa, D. S. (2022). The impact of context awareness and ubiquity on mobile government service adoption. Mobile Information Systems, 2022, 1-20.

Morando, F., Iemma, R., & Raiteri, E. (2014). Privacy evaluation: what empirical research on users' valuation of personal data tells us. Internet Policy Review, 3(2), 1-12.

Nitzl, C. (2016). The use of partial least squares structural equation modelling (PLS-SEM) in management accounting research: Directions for future theory development. Journal of Accounting Literature, 37(March), 19–35. https://doi.org/10.1016/j.acclit.2016.09.003

Park, Y. J. (2013). Digital literacy and privacy behavior online. Communication research, 40(2), 215-236.

Park, Y. J., & Jang, S. M. (2014). Understanding privacy knowledge and skill in mobile communication. Computers in Human Behavior, 38, 296-303.

Pentina, I., Zhang, L., Bata, H., & Chen, Y. (2016). Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. Computers in Human Behavior, 65, 409-419.

Pop, R. A., Hlédik, E., & Dabija, D. C. (2023). Predicting consumers' purchase intention through fast fashion mobile apps: The mediating role of attitude and the moderating role of COVID-19. Technological Forecasting and Social Change, 186, 122111.

Rigdon, E. E. (2012). Rethinking Partial Least Squares Path Modeling: In Praise of Simple Methods. Long Range Planning, 45(5–6), 341–358. https://doi.org/10.1016/j.lrp.2012.09.010

Rowe, F. (2020). Contact tracing apps and values dilemmas: A privacy paradox in a neo-liberal world. International Journal of Information Management, 55, 102178.

Scherer, R., Siddiq, F., & Tondeur, J. (2019). The technology acceptance model (TAM): A meta-analytic structural equation modeling approach to explaining teachers' adoption of digital technology in education. Computers & Education, 128, 13-35.

Schwartz, V. E., & Driver, R. W. (1983). Warnings in the workplace: The need for a synthesis of law and communication theory. U. Cin. L. Rev., 52, 38.

Shmueli, G., & Koppius, O. R. (2011). Predictive analytics in information systems research. MIS Quarterly, 35(3), 553–572.

Shmueli, G., Ray, S., Velasquez Estrada, J. M., & Chatla, S. (2015). The Elephant in the Room: Evaluating the Predictive Performance of Partial Least Squares (PLS) Path Models. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2659233.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. MIS quarterly, 989-1015.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. MIS quarterly, 167-196.

Solove, D. J. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154(3), 477-560.

Statista (2022). Annual number of app downloads from the Google Play Store worldwide from 2016 to 2021(in billions). Accessed from https://www.statista.com/statistics/734332/google-play-app-installs-per-year/

Stone, M. (1974). Cross-Validatory Choice and Assessment of Statistical Predictions. Journal of the Royal Statistical Society: Series B (Methodological), 36(2), 111–133. https://doi.org/10.1111/j.2517-6161.1974.tb00994.x.

Sun, Y., Wang, N., & Shen, X. L. (2021). Calculus interdependency, personality contingency, and causal asymmetry: Toward a configurational privacy calculus model of information disclosure. Information & Management, 58(8), 103556.

Voorhees, C. M., Brady, M. K., Calantone, R., & Ramirez, E. (2016). Discriminant validity testing in marketing: an analysis, causes for concern, and proposed remedies. Journal of the Academy of Marketing Science, 44(1), 119–134. https://doi.org/10.1007/s11747-015-0455-4

Waldman, A. E. (2020). Cognitive biases, dark patterns, and the 'privacy paradox'. Current Opinion in Psychology, 31, 105-109.

Wang, C., Zhang, N., & Wang, C. (2021). Managing Privacy in the Digital Economy. Fundamental Research, 1(5), 543-551.

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.

Wu, B., & Chen, X. (2017). Continuance intention to use MOOCs: Integrating the technology acceptance model (TAM) and task technology fit (TTF) model. Computers in human behavior, 67, 221-232.

Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). Measuring Mobile Users' Concerns for Information Privacy. Thirty Third International Conference on Information Systems, Orlando, 1-16

Yun, H., Lee, G., & Kim, D. J. (2019). A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs. Information & Management, 56(4), 570-601.

Zheng, X., & Lee, M. K. (2016). Excessive use of mobile social networking sites: Negative consequences on individuals. Computers in Human Behavior, 65, 65-76.

Zlatolas, L. N., Welzer, T., Heričko, M., & Hölbl, M. (2015). Privacy antecedents for SNS self-disclosure: The case of Facebook. Computers in Human Behavior, 45, 158-167.

دراسة العوامل المؤثرة على مخاوف خصوصية معلومات الأفراد من تطبيقات الهاتف المحمول

سالم علي الغامدي

قسم برامج التحول الرقمي والمعلومات، معهد الإدارة العامة، جدة، المملكة العربية السعودية

ghamdiSA@ipa.edu.sa

المستخلص. على الرغم من أن تطبيقات الهاتف المحمول تعتبر من أحدث تقنيات الحوسبة المتنقلة، إلا أن مشكلات الأمان والخصوصية تُعد عقبة أمام قبولها لدى بعض المستخدمين. وتشير الدراسات السابقة إلى أن معالجة خروقات الأمان قد لا تعتمد بشكل أساسي على التقنيات المتقدمة فقط، ولكن تعتمد أيضًا على عوامل مثل معرفة المستخدم بخصائص الأمان، وتجربة المستخدم السابقة للخصوصية، ونية السلوك الفردية. وهذا أدى الى ظهور عدد من النظريات التي تعالج بشكل أساسي الفجوة المتعلقة بمخاوف الخصوصية بين مستخدمي الأجهزة المحمولة خصوصا تقييم نية السلوك الفردية تجاه تطبيقات الأجهزة المحمولة. ولسد هذه الفجوة تستخدم الدراسة الحالية إطار مخاوف الخصوصية لمعلومات مستخدمي الأجهزة المحمولة (MUIPC) لذلك تم إجراء دراسة استقصائية شملت بيانات ٢٩٠ مشاركًا للفحص التجريبي للنموذج النظري المقترح بشأن الدافع الفردي لاستخدام تطبيقات الأجهزة المحمولة. وتشير نتائج هذه الدراسة إلى أن تجربة الخصوصية السابقة، والمعرفة بخصائص الامان في الهواتف المحمولة، وأولوية التنزيل هي عوامل تنبؤيه ذات دلالة احصائيا للمراقبة المتصورة، والتطفل المتصور، والاستخدام الثانوي للمعلومات. بينما أظهرت النتائج ان تأثير عامل اللامبالاة لدى المستخدمين غير ذا دلالة احصائيا. علاوة على ذلك، تُظهر النتائج أن الاستخدام الثانوي للمعلومات الشخصية له تأثير سلبي وذا دلالة احصائيا على النية لاستخدام تطبيقات الأجهزة المحمولة. وتشير النتائج أيضًا إلى أن تصورات المستخدمين للخصوصية والأمان تختلف اعتمادًا على مستوى حساسية المعلومات في تطبيقات الأجهزة المحمولة.

الكلمات المفتاحية: تجربة الخصوصية السابقة، المعرفة بخصائص الأمان، أولوية التنزيل، الحساسية المتصورة، التطفل المتصور، النية لاستخدام تطبيقات الأجهزة المحمولة.