International Journal of Religion
2024
Volume: 5| Number 5 | pp. 612 – 619
ISSN: 2633-352X (Print) | ISSN: 2633-3538 (Online)
ijor.co.uk
DOI: https://doi.org/10.61707/kqyq0505

Exploring the Interplay of Privacy Concerns, Mobile Cybersecurity Awareness, and Protective Motivation Behavior

Sariga Sajikumar[1], N. Ajithkumar[2] and Gopu Vijayan[3]

Abstract

This study delves into the uncharted realm of privacy concerns among Indian smartphone users, exploring their nexus with mobile cybersecurity awareness and protective behaviour. Employing the Mobile User's Information Privacy Concern (MUIPC) tool and Protection Motivation Theory (PMT), it addresses gaps by scrutinizing users' concerns, data protection motivations, and cybersecurity awareness impact. Focused on the Indian smartphone user base, this research illuminates crucial insights into mobile privacy dynamics, informing privacy policies, user education, and cybersecurity strategies. Surveys gathered 364 diverse responses. Statistical analysis using chi-square tests and PLS-SEM via smartpls4 revealed a significant positive association between MUIPC and Protective Motivation Behavior (PMB). Notably, mobile cybersecurity awareness partially mediated the link between MUIPC and PMB. These findings emphasize the intricate relationship between privacy concerns, cybersecurity awareness, and protective behaviours in India's mobile landscape.

Keywords: *Information Security, Information Privacy Concerns, MUIPC, Protection Motivation Behavior, Mobile Cybersecurity Awareness, India*

INTRODUCTION

In contemporary times, smartphones have assumed an indispensable role in the fabric of daily life, undergoing a transformative trajectory into sophisticated instruments featuring both internet connectivity and a spectrum of mobile applications. This research, thus, directs its focus towards the attendant privacy concerns stemming from this technological metamorphosis. Mobile applications, denoting software tailored for mobile devices, have engendered a paradigm shift in various life domains by facilitating seamless access to diverse services. Nevertheless, the escalating reliance on mobile technology introduces palpable apprehensions concerning the privacy of personal information. The mobile milieu is particularly vulnerable to data privacy challenges, owing to intrinsic factors such as sensor-rich devices, perpetual internet connectivity, deficient security protocols, and constraints affecting users' adept management of privacy configurations. The persistence of non-revocable app permissions further exacerbates these privacy concerns.

This empirical study seeks to probe into information privacy concerns among Indian mobile phone users, given the nation's standing as the second-largest global user base. Against the backdrop of India's rapid digital metamorphosis, comprehending the repercussions of digital privacy concerns on the assimilation of digital services assumes paramount significance. India's classification as a high-risk locus for data breaches underscores the exigency of identifying potential privacy risks. Methodologically, this research employs the Mobile User's Information Privacy Concern instrument, incorporating it within the theoretical framework of the Protection Motivation Theory, thereby elucidating the interplay between users' privacy concerns and their motivation to safeguard their privacy within the mobile milieu. The investigation also scrutinizes the impact of individuals' awareness of cybersecurity on their proclivity to protect privacy while utilizing mobile devices. To address these research objectives, a structured national-level empirical inquiry involving Indian smartphone users was undertaken through the online dissemination of a meticulously constructed questionnaire.

[1] Research Scholar, Department of Commerce and Management, School of Arts, Humanities and Commerce, Amrita Vishwa Vidyapeetham, Kochi Campus, Brahmasthanam, Kochi, India E-mail: sarigasajikumarphd@gmail.com, ORCID: https://orcid.org/0009-0003-8772-9418

[2] Professor, Department of Commerce and Management, School of Arts, Humanities and Commerce, Amrita Vishwa Vidyapeetham, Kochi Campus, Brahmasthanam, Kochi, India. E-mail: najithkumar3000@gmail.com

[3] Assistant Professor, Assistant Professor, Department of Commerce, V.T. Bhattathiripad College, Kerala, India. E-mail: gopuvijayan@gmail.com

THEORETICAL BACKGROUND

The surge in technology usage has intensified cyber threats, necessitating an in-depth exploration of information privacy and data security across diverse domains. Numerous studies spanning workplace, personal computing, cloud computing, smart home devices, social media, e-commerce, banking sectors, and mobile computing meticulously examine the nuances of information privacy. Mobile devices' expanded functionalities heighten privacy concerns, making them susceptible to exploitation by malicious entities, leading to identity theft and fraudulent activities. Users, crucially responsible for safeguarding sensitive data, must navigate privacy challenges in the evolving mobile environment.

Mobile User's Information Privacy Concern (MUIPC)

Privacy involves resisting external intrusions, safeguarding sensitive life details, actions, and associations. It is defined as individuals' desire to control data about themselves, encompassing diverse information [1]. Information privacy oversees personal data gathering, utilization, and sharing. Mobile computing faces heightened privacy threats due to portability, third-party apps, GPS tracking, vast cloud storage, open Wi-Fi use, and mobile payments. Mobile device vulnerability results from user negligence and unawareness of data collection consequences. User mindfulness is crucial for privacy responsibility despite security measures.

Mobile Applications and Information Privacy

Mobile apps play a crucial role in society, transforming communication, work, and information access. As technological advances integrate these apps further into daily life, processing significant data, privacy concerns emerge. Apps often request unnecessary data access, potentially collecting and selling it without explicit consent. Managing mobile devices during download, installation, and utilization significantly impacts information privacy. Users often accept app terms and permissions for benefits, despite heightened sensitivity to permissions amplifying privacy concerns. The decision to download involves weighing app benefits against privacy risks, revealing intricate dynamics in mobile users' privacy considerations.

Mobile User's Information Privacy Concern Scale

Various research tools explore attitudes and behaviors toward privacy in diverse contexts, like online interactions and healthcare. The Mobile User's Information Privacy Concern (MUIPC) instrument, crafted by [16], assesses privacy perceptions on mobile devices. Rooted in Communication Privacy Management (CPM) Theory, MUIPC, influenced by [15] Concern for Information Privacy Scale and [8] work on Internet Users Information Privacy Concerns (IUIPC), measures concern in three dimensions: perceived surveillance, intrusion, and secondary utilization of information. MUIPC is pivotal in understanding mobile users' evolving privacy apprehensions across various studies (e.g., [11]; [12]; [13]; [4]).

Protection Motivation Theory

The Protection Motivation Theory (PMT), introduced by [10], illuminates cognitive processes driving secure behaviors. It examines threat appraisal—perceived vulnerability, severity, and rewards—and coping appraisal, evaluating response efficacy, self-efficacy, and cost. PMT is widely applied in information security research, showing a positive correlation with adherence to information security policies. In mobile contexts, PMT is extensively used, yet a gap persists in understanding the correlation between Protection Motivation Behaviors (PMB) and mobile users' privacy concerns, necessitating further research on PMT factors in mobile computing.

Mobile Cybersecurity Awareness (MCA)

Mobile Cybersecurity Awareness (MCA) is crucial in recognizing and mitigating risks in mobile settings. Defined by [14] as understanding information security importance and implementing protective measures, MCA involves knowledge, attitudes, and skills for specific attacks [2]. This includes identifying vulnerabilities like malware, phishing, and unauthorized access, with best practices such as strong passwords and secure Wi-Fi. Despite awareness, individuals often hesitate in the mobile environment, underestimating risks. Recognizing mobile devices' susceptibility to cyber hazards, proactive steps must be implemented for safeguarding both devices and sensitive data to maintain security.

Research Model and Hypotheses Formulation

The conceptual framework (Figure 1) integrates Protection Motivation Theory (PMT) and Mobile Users' Information Privacy Concerns (MUIPC) to explore the association between users' privacy concerns on mobile devices and motivation for secure online practices on smartphones. The model additionally examines the mediating role of mobile cybersecurity awareness (MCA) in the relationship between individuals' information privacy concerns and their inclination to protect themselves in the mobile ecosystem. This holistic approach seeks to comprehensively understand the intricate dynamics among privacy concerns, MCA, and protective behavior (PMB) in the mobile context.

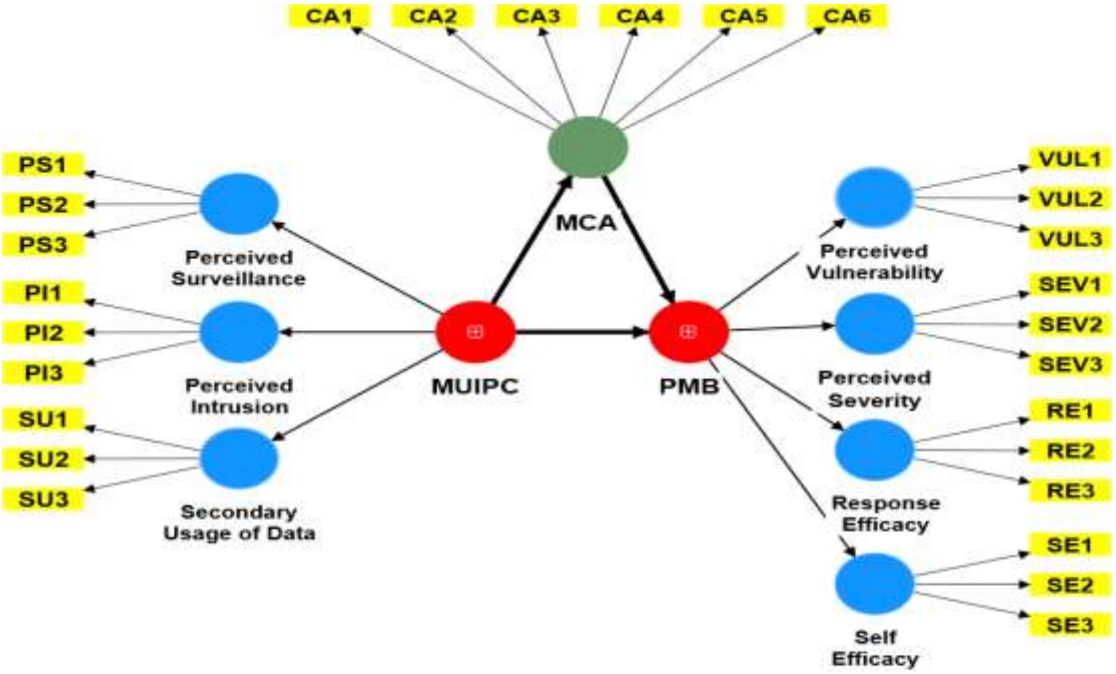

Figure 1. *Proposed Research Model*

This research aims to assess information privacy concerns among mobile phone users in India through the MUIPC scale. It is crucial for understanding challenges and opportunities arising from widespread smartphone adoption in India, impacting user protection, policy development, business strategies, and academic knowledge. The study hypothesizes:

H_1: Indian mobile phone users have the same level of MUIPC

H_2: MUIPC exerts a notable influence on an individual's PMB.

H_3: MUIPC has a significant relation with mobile cybersecurity awareness of the individual.

H_4: Mobile Cybersecurity awareness of an individual significantly correlates with an individual's PMB in the mobile environment.

H_5: Mobile Cybersecurity awareness significantly mediates the relationship between MUIPC and their protection motivation in the mobile environment.

RESEARCH METHODOLOGY

Measurement Scale

Following our theoretical framework, we employed a structured questionnaire for data collection. To assess mobile users' information privacy concerns, we utilized [16] Mobile Users' Information Privacy Concern (MUIPC) questionnaire, incorporating variables such as perceived surveillance, intrusion, and secondary data usage. Protection motivation assessment used a modified scale from [9], while cybersecurity awareness measurement adapted [7] instrument to align with our study's objectives. Employing a five-point Likert scale ensured detailed responses, ranging from 'strongly disagree' (1) to 'strongly agree' (5), fostering a comprehensive exploration of our research questions.

Data Collection Process

The study focused on smartphone users in India, employing online questionnaires for data collection. A total of 364 participants voluntarily provided insights, ensuring a diverse and geographically widespread representation. This dataset formed the basis for comprehensively analyzing the interconnections among the variables under study.

Results

Measuring MUIPC

The primary objective of this research paper is to assess the extent of concerns regarding information privacy among users of mobile phones. This evaluation is accomplished by employing the MUIPC scale. To facilitate this assessment, an index variable called MUIPC was constructed. MUIPC encompasses the aggregated scores of three distinct subscales, specifically, Perceived Severity (PS), Perceived Intrusion (PI), and Secondary Usage (SU) of data. The expected range for the MUIPC score lies between 9 and 45, as each of the nine scale elements is evaluated on a scale from "Strongly Disagree" (with a value of 1) to "Strongly Agree" (with a value of 5). Hence, the lowest achievable score is 9 (resulting from 3 items per subscale, each rated as 1), while the highest attainable score is 45 (stemming from 3 items per subscale, each rated as 5). A higher MUIPC score signifies an elevated level of information privacy concern among mobile device users, while a lower score suggests a diminished level of such concern. The scores have been divided into three specific levels: a score ranging from 9 to 20.9 indicates a low level of privacy concern, scores falling between 21 and 33 suggest a moderate level of privacy concern, and scores surpassing 33 up to 45 signify a high degree of privacy concern among users of mobile devices in India.

A statistical examination using chi-square was performed to assess the goodness of fit.

Table 2. ***Chi-square for testing goodness of fit***

Low		Medium		High		Chi-square	p	Hypothesis
Frequency	%	Frequency	%	Frequency	%			
24	6.5	128	33.06	213	58.35	147.293	<0.001*	H_1 not supported

* Significant at 1% level

Table 2 illustrates diverse levels of information privacy concerns among respondents in the mobile environment, with 58.35% expressing high concern, 33.06% indicating a moderate level, and 6.5% demonstrating low concern. The chi-square test confirms statistical significance (χ2 = 147.293, p < 0.05), rejecting the hypothesis of uniform Mobile User Information Privacy Concern (MUIPC) among Indian mobile phone users and highlighting varying levels of concern in their mobile interactions.

Partial Least Square Structural Equation Modelling (PLS-SEM)

The study utilized PLS-SEM, a robust method for predictive modeling and theory development, through Smart-PLS4 software. This involved two steps: assessing the measurement model and analyzing the structural model.

Measurement Model Assessment

Table 3 exhibits Cronbach's alpha, Composite Reliability (CR), item loadings, and Average Variance Extracted (AVE) values. All constructs surpass the 0.7 threshold for internal consistency, meeting established standards [6]. Item loadings and AVE values further confirm the robust convergent validity of the measurement model.

Table 3. ***Loadings, Validity, and Reliability***

Construct	Variable	Items		AVE	CR	Cronbach's Alpha
MUIPC	Perceived Surveillance	PS1	0.684	0.707	0.877	0.786
		PS2	0.903			
		PS3	0.914			
	Perceived Intrusion	PI1	0.892	0.776	0.912	0.856
		PI2	0.909			
		PI3	0.841			
	Secondary usage of data	SU1	0.903	0.854	0.946	0.914
		SU2	0.943			
		SU3	0.926			
PMB	Perceived Vulnerability	VUL1	0.889	0.802	0.924	0.877
		VUL2	0.913			
		VUL3	0.884			
	Perceived Severity	SEV1	0.926	0.817	0.931	0.888
		SEV2	0.921			
		SEV3	0.864			
	Response- efficacy	RE1	0.921	0.860	0.949	0.919
		RE2	0.943			
		RE3	0.918			
	Self- efficacy	SE1	0.944	0.861	0.949	0.919
		SE2	0.938			
		SE3	0.901			
MCA		CA1	0.512	0.462	0.770	0.649
		CA2	0.719			
		CA3	0.657			
		CA4	0.612			
		CA5	0.573			
		CA6	0.506			

Table 4 confirms discriminant validity using the Fornell-Larcker criterion. The square root of Average Variance Extracted (AVE) for each construct exceeds inter-construct correlation values, indicating distinct representation of model aspects with minimal correlation.

Table 4. ***Discriminant Validity- Fornell Larcker Criterion***

Construct	MCA	MUIPC	PMB
MCA	0.602		
MUIPC	0.254	0.87	
PMB	0.357	0.553	0.644

Note: *Bold values represent the square root of AVE, while non-bolded values indicate inter-construct correlation.*

Structural Model Assessment

After evaluating the measurement model, the next step is analyzing the structural model to determine path coefficients and their significance. Following [5] guidelines, the first step involves checking for collinearity using Variance Inflation Factor (VIF). The analysis showed no multicollinearity issues, with all VIF values below the recommended threshold of 3 (refer to appendix B for details).

The study assessed hypotheses by examining path coefficients, t-statistics, and p-values (Table 5). Hypothesis 2 confirmed a significant influence of Mobile Users' Information Privacy Concerns (MUIPC) on Protection Motivation Behavior (PMB) ($\beta = 0.494$, $t = 9.466$, $p < 0.001$). Similarly, Hypothesis 3 validated the impact of MUIPC on Mobile Cybersecurity Awareness (MCA) ($\beta = 0.254$, $t = 4.558$, $p < 0.001$). Hypothesis 4 established a noteworthy correlation between Mobile Cybersecurity Awareness (MCA) and Protection Motivation Behavior (PMB) ($\beta = 0.232$, $t = 3.313$, $p = 0.001$). The detailed results are presented in Table 5.

Table 5. *Effect on the endogenous variable*

Hypothesis	β	Standard error	t-statistics	p- value	Decision	Effect size(f^2)	R^2 value	Q^2 value
H_2 MUIPC → PMB	0.494	0.052	9.466	<0.001*	Supported	0.355	0.356	0.300
H_3 MUIPC → MCA	0.254	0.056	4.558	<0.001*	Supported	0.069	0.065	0.052
H_4 MCA→PMB	0.232	0.070	3.313	0.001*	Supported	0.078		

* Significant at 1% level

Furthermore, the model's explanatory and predictive capacity was evaluated through the examination of the coefficient of determination (R^2), effect size (f^2), and predictive relevance (Q^2). R^2 signifies the proportion of variance in the endogenous variable explained by the exogenous variable (MUIPC), with acceptable values contingent upon the research context, where 0.10 is considered satisfactory [5]. The effect size (f^2) determines the exogenous variable's influence on the endogenous variable, with values exceeding 0.35 indicating substantial impact, 0.15 indicating moderate impact, and 0.02 suggesting a small impact as per [3] recommendations. Q^2 evaluates predictive relevance, where values above 0, 0.25, and 0.50 indicate small, medium, and large predictive relevance, respectively, following [5].

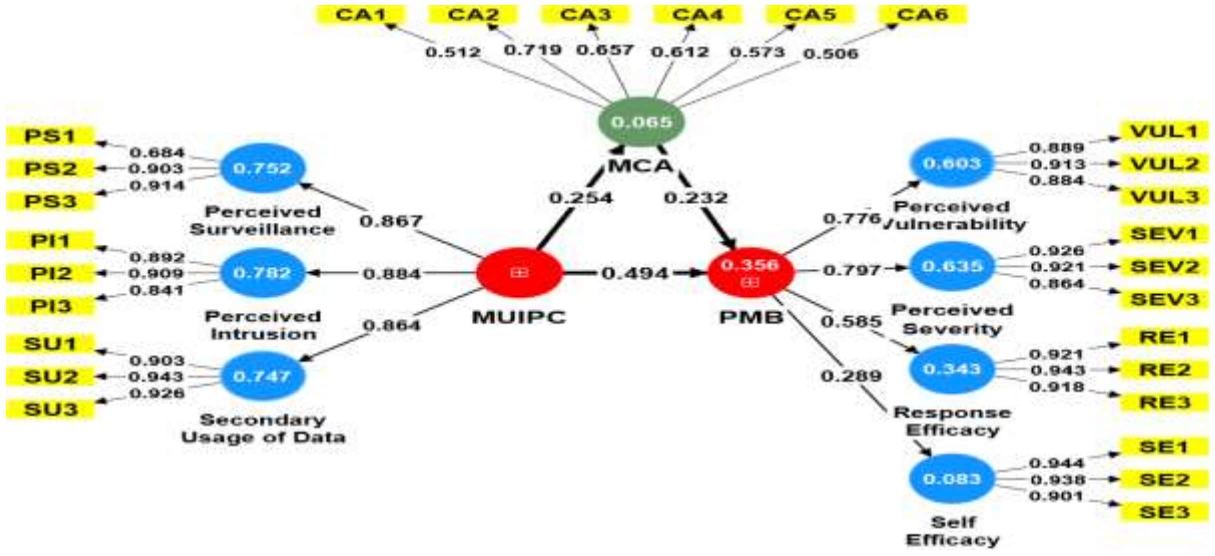

Figure 2. *Structural model*

Mediation Assessment

A mediation analysis investigated Mobile Cybersecurity Awareness (MCA) as a mediator between Mobile Users' Information Privacy Concerns (MUIPC) and their protection motivation in the mobile environment (H5). Results, detailed in table 6, showed a significant indirect effect of MUIPC on Protection Motivation Behavior (PMB) (β = 0.059, t = 0.062, p = 0.018). The total effect of MUIPC on PMB was also significant (β = 0.553, t = 0.557, p < 0.001). Despite the inclusion of the mediator (MCA), the effect of MUIPC on PMB remained substantial (β = 0.494, t = 0.495, p < 0.001), indicating a partial mediating role of mobile cybersecurity awareness in the relationship between mobile users' information privacy concerns and their protection motivation behavior.

DISCUSSIONS

Cybersecurity is a major contemporary challenge, posing a pervasive threat globally, especially through mobile phones and their applications. These devices often serve as vulnerable points, leading to identity theft and the compromise of sensitive information. This research focuses on information privacy concerns among Indian mobile users, revealing varied levels influenced by awareness of mobile ecosystem vulnerabilities. The study highlights the significant impact of privacy concerns on motivating users to protect their data and establishes a positive association between Mobile Users' Information Privacy Concerns (MUIPC) and Mobile Cybersecurity Awareness (MCA). The research underscores the pivotal role of MCA in influencing Protection Motivation Behavior (PMB), revealing its mediating role between MUIPC and PMB in shaping users' motivation to safeguard information privacy within the mobile environment.

Practical Implications

These findings have crucial implications for stakeholders. Mobile service providers and developers should recognize varied information privacy concerns, necessitating customized privacy features and enhanced user education. Raising awareness about mobile cybersecurity threats can potentially alleviate concerns and enhance the security of the mobile environment. For policymakers and regulators, the study underscores the need for robust data privacy regulations that consider diverse user concerns and awareness levels. Strengthening regulations can instill confidence in information security and bolster overall trust in mobile platforms. The study also emphasizes the importance of user awareness in combating mobile cybersecurity threats. Increasing awareness about potential risks and taking proactive measures can empower individuals to better protect their information privacy during mobile transactions.

Limitations Of the Study

The study's limitations encompass several facets that warrant consideration for future research. Firstly, the examination concentrated on Indian mobile users, yet the sample size and demographics might inadequately encapsulate the multifaceted population and behaviors prevalent in the country. Secondly, potential response biases or inaccuracies might have arisen due to the reliance on self-reported measures, potentially impacting the reliability of the collected data. Furthermore, the study primarily centered on information privacy concerns, cybersecurity awareness, and protection motivation behavior without delving deeply into other influential variables such as socio-economic status, cultural nuances, and technological literacy. Exploring these additional factors may contribute to a more holistic comprehension of the intricate dynamics that shape individuals' conduct in the mobile setting.

Future Direction for Research

In future research, exploring the multifaceted nature influencing users' behaviors in safeguarding privacy within mobile environments, as evidenced by the partial mediation role of mobile cybersecurity awareness, stands as a crucial avenue. Investigating the diverse factors contributing to the varying levels of Mobile Users' Information Privacy Concerns (MUIPC) among individuals presents a promising direction. Understanding the specific factors shaping these varying levels could elucidate the nuanced dynamics involved in privacy concerns. Additionally, future studies could delve deeper into the role of individuals' awareness levels in shaping MUIPC. Taking into account how awareness shapes the degree of concerns regarding information privacy could offer valuable perspectives into the elements that steer users' views and actions within mobile environments. These directions hold the potential for comprehensive elucidation of the complexities underpinning privacy concerns in mobile environments.

Acknowledgement

The research was supported by the University Grants Commission (UGC), Government of India, through a Junior Research Fellowship (JRF) (Grant Ref No: 190510138646), providing crucial financial assistance. The data can be shared upon request, and there are no competing interests to declare.

REFERENCES

Bélanger, & Crossler. (2011). Privacy in the digital age: A review of information privacy research in information systems. MIS Quarterly: Management Information Systems, 35(4), 1017. https://doi.org/10.2307/41409971

Bitton, R., Finkelshtein, A., Sidi, L., Puzis, R., Rokach, L., & Shabtai, A. (2018). Taxonomy of mobile users' security awareness. Computers & Security, 73, 266–293. https://doi.org/10.1016/j.cose.2017.10.015

Cohen, J. (1988). Statistical power analysis for the behavioral sciences (2nd Ed.). New York: Routledge.

Degirmenci, K. (2020). Mobile users' information privacy concerns and the role of app permission requests. International Journal of Information Management, 50, 261–272. https://doi.org/10.1016/j.ijinfomgt.2019.05.010

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., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Danks, N. P., & Ray, S. (2021). Partial least squares structural equation modeling (PLS-SEM) using R: A workbook. Springer International Publishing.

Khan, A. Z., Mirza, H. H., Khan, T. I., & Khan, M. M. (2020). Efficiency Analysis of Mudarabah and Leasing Firms in Pakistan. Journal of Islamic Business and Management, 10(2), 390-401.

Koyuncu, M., & Pusatli, T. (2019). Security awareness level of smartphone users: An exploratory case study. Mobile Information Systems, 2019, 1–11. https://doi.org/10.1155/2019/2786913

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 : ISR, 15(4), 336–355. https://doi.org/10.1287/isre.1040.0032

Jam, F. A., Singh, S. K. G., Ng, B., & Aziz, N. (2018). The interactive effect of uncertainty avoidance cultural values and leadership styles on open service innovation: A look at malaysian healthcare sector. International Journal of Business and Administrative Studies, 4(5), 208-223.

Handayani, S., Muhyi, R., Suhartono, E., & Noor, M. S. (2020). Analysis of Factors Related to the Utilization of the Community Health Center by BPJS Participants in Three Puskesmas in Banjarmasin City, 2020. Journal of Advances in Health and Medical Sciences, 6(1), 01-06.

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. https://doi.org/10.1016/j.jbusres.2021.11.022

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. The Journal of Psychology: Interdisciplinary and Applied, 91(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Sandhu, R. K., Vasconcelos-Gomes, J., Thomas, M. A., & Oliveira, T. (2023). Unfolding the popularity of video conferencing apps – A privacy calculus perspective. International Journal of Information Management, 68(102569), 102569. https://doi.org/10.1016/j.ijinfomgt.2022.102569

Jam, F. A., Rauf, A. S., Husnain, I., Bilal, H. Z., Yasir, A., & Mashood, M. (2014). Identify factors affecting the management of political behavior among bank staff. African Journal of Business Management, 5(23), 9896-9904.

Serah, Y. A., Setiawati, R., & Septinawati, S. A. (2020). Empowerment of community laws in efforts to decide distribution of COVID-19 in era new normal. Journal of Advances in Humanities and Social Sciences, 6(3), 114-120.

Seberger, J. S., & Patil, S. (2021). Us and them (and it): Social orientation, privacy concerns, and expected use of pandemic-tracking apps in the United States. Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems.

Seberger, J. S., & Patil, S. (2022). Beyond the pandemic and privacy concerns: Perceived benefit and expected use of pandemic-tracking apps in India. Proceedings of the ACM on Human-Computer Interaction, 6(CSCW2), 1–29. https://doi.org/10.1145/3555596

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. Computers & Education, 52(1), 92–100. https://doi.org/10.1016/j.compedu.2008.06.011

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. MIS Quarterly: Management Information Systems, 20(2), 167. https://doi.org/10.2307/249477

Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). Measuring mobile users' concerns for information privacy. Psu.edu. Retrieved March 24, 2023, from https://faculty.ist.psu.edu/xu/papers/xu_etal_icis_2012a.pdf

Wang, C. H., & Wu, K. C. (2022). Interdisciplinary Collaborative Learning with Modular Programming and Information Visualization of Urban Smart Spaces. , 8(1), 24-32.