[1] Yaser Alhasawi

Privacy in the Palm: The Effect of Prior Privacy Experience on Mobile Information Privacy Concerns and User's Behavioral Intentions

Journal of Electrical Systems

Abstract: - The advancement of mobile network technology and smartphones has given mobile users unmatched access to the Internet and other services from their mobile devices. In this situation, privacy concerns become quite significant as suppliers could have access to a lot of personal data. The purpose of this research is to examine the impact of prior privacy experience (PPE) on mobile user information privacy concerns and behavioral intentions. We also incorporated the moderating role of technical security knowledge on the relationship between prior privacy experience and perceived surveillance (PSV). A survey was distributed among 574 participants in United States and analyzed using structural equation modeling technique. The findings revealed that prior privacy experience has a positive and significant influence on PSV, perceived intrusion (PIN), and secondary use of personal information (SUPI). Similarly, PSV, PIN, and SUPI have positive association with behavioral intention. In last, technical security knowledge has a negative moderation between the relationship of prior privacy experience and PSV. These findings have important research and practical implications for mobile software's and application developers.

Keywords: Prior privacy experience; Information security; Mobile users; Behavioral intentions.

I.INTRODUCTION

The development of smartphones and mobile network technology has given customers incomparable opportunities for Internet access and value-added services. The proliferation of smartphones has resulted in a remarkable growth curve for mobile applications. According to Wu and Ye (2013), mobile applications are projected to produce $15.9 billion in end-user spending in 2013. Additionally, they are likely to have a positive impact on smartphone sales, promotional expenditure, and technological advancements. Mobile apps are revolutionizing the user experience by offering context-aware features that adapt to the user's mobile environment. This has transformed the mobile app industry into a highly competitive industry that attracts various stakeholders such as manufacturers, traders, software developers, and marketing firms [2]. Xu et al. [3] claimed that the economic outlook predicts that revenues generated by mobile apps will increase from $69.7 billion in 2019 to $188.9 billion in 2023. This growth will be driven by $71.7 billion in income from app stores and $117.2 billion from in-app advertising.

Nevertheless, the use of mobile applications sometimes involves the sharing of an enormous amount of personal information instantly, hence creating a significant possibility for privacy violation [4]. The media has recently brought attention to this possible danger by stating that merchants and app developers are certainly gathering personal data from users' devices and sending it to other groups. The Wall Street Journal conducted a study on 101 widely used smartphone applications and discovered that 56 of these apps shared the phone's distinctive identities with other organizations without the users' knowledge, while 47 apps shared the phone's location with external parties [5]. It has been discovered that Apple iOS and Google Android mobile operating systems collect and send location data without the permission of device users [6].

Information privacy concerns have been a widely studied topic in the field of information systems (IS) research [7]–[9], particularly in relation to the use of mobile applications. Previous research has focused on various aspects such as app popularity, privacy seals, and location-based services. However, the role of prior privacy experience has been underestimated so far. In his work, Degirmenci [10] identified privacy as one of the four main ethical

[1] *Corresponding author: Yaser Alhasawi, Management Information System Department, King Abdulaziz University (KAU), Jeddah, Saudi Arabia (Yalhasawi@kau.edu.sa)

concerns that arise in the context of the digital age. The first apprehension around privacy has been remarkably specific, and advancements in technology as well as the evolving societal acceptance of technology continue to influence issues related to privacy. Hence, it is important for models aimed at comprehending private concerns to adapt and grasp the influence of these technological advancements on the user's privacy concerns. The user's choice to utilize the technology is influenced by these issues of privacy.

This research aims to examine the impact of previous privacy experiences on the level of concern for information privacy among mobile users. In order to fill this gap, we utilize the concept of mobile users' information privacy concerns (MUIPC) [3] to measure users' privacy concerns in a mobile context. Our study is situated within the parameters of the universal macro model known as "Antecedents-Privacy Concerns-Outcomes" (APCO) [11], with a particular emphasis on the antecedents of prior privacy experience.

There are mainly five sections in this paper. In the second section, literature review follows the introductory section, which discusses theories and establishes connections between hypotheses. The third section discusses the research approach. The fourth section discusses the results and findings of the study. Finally, the final section presents a conclusion and implications for future research.

II.LITERATURE REVIEW AND HYPOTHESES DEVELOPMENT

A. Prior Privacy Experience and Perceived Surveillance

The field of privacy has long been of interest to researchers [12], [13]; nonetheless, this interest has only grown as technology has advanced. Information privacy issue is often used as a substitute for the concept of privacy in the information system literature, and it has been included into several behavioral models [14]. Smith et al., [15] characterized information privacy concerns as centered on individual's apprehensions regarding organizations' information privacy practices. Conversely, Dinev and Hart [16] suggested that these concerns could also reflect individual's perception regarding the fate of the information they disclose online.

A greater awareness and sensitivity toward privacy concerns are commonly observed in individuals who have encountered privacy issues in the past, whether they were positive or negative [17]. They are more conscious of privacy issues in digital contexts because of their prior experiences, which have influenced their perception and beliefs. According to Ghosh et al. [18], people are more likely to carefully analyze the surveillance practices associated with mobile phone usage and compare them to their past experiences. A user's perception of surveillance risk may be reduced when they have positive experiences, such as effective privacy protection mechanisms or free information processing procedures [19]. Secondly, people who have positive experiences with privacy often feel empowered to make wise decisions about sharing and using their personal data. This empowerment adds to a feeling of less surveillance because it makes people feel more in control of their privacy [17]. Furthermore, positive experiences are linked with greater openness because transparency privacy rules and information about data practices foster a mutual respect and understanding between companies. Thus, in light of the preceding reasoning, we propose the accompanying hypothesis.

H_1: Prior privacy experience will have a positive influence on PSV

B. Prior Privacy Experience and Perceived Intrusion

According to [14], PIN refers to the individuals' ability to decide how to use an individual data, including IoT devices and related services. PIN is essentially a violation of one's personal space, presence, or activity [20]. Moreover, Xu et al. [21] contend that mobile malware infestations could be viewed as intrusions., which could restrict data transfer among devices. The danger posed by malware is real in the context of IoT. The likelihood of malware infection or data loss increases with internet of thing (IoT) devices because they are built with many sensors and link to other devices and services over the internet. This increased danger is brought because by the large number and power of connected devices.

It is clearly mentioned in prior literature that people are more inclined to trust the organization handling their data if they have had positive privacy experiences, such as clear and transparent data handling procedures, efficient privacy protection measures, and open and respectful communication [10], [22], [23]. These people feel more confident and less fearful of intrusion because they trust that their personal space will be protected and respected. Solove [20] asserted in a similar manner that individuals who have a positive experience with privacy are often more capable of making informed decision about what information to share and with whom. The perception of control serves as a safeguard against PIN, as it enables individual to feel more assured in their ability to regulate and secure their privacy. In a similar vein, Wu et al. [24] also claimed that individuals who have had positive encounters with confidentiality are likely to demonstrate higher levels of caution and awareness when it comes to using their mobile phones. For instance, they should carefully check program permissions, update their privacy settings on a regular basis, and refrain from giving important information unnecessarily. This pattern of action lessens the possibility of running into circumstances that may be seen as an intrusion. Thus, in light of the preceding reasoning, we propose the accompanying hypothesis.

H_2: Prior privacy experience will have a positive influence on PIN

C. Prior Privacy Experience and Secondary Use of Personal Info.

According to Foltz and Foltz[23], SUPI refers to the process of gathering data from people for one use but using it for another such as sending marketing messages targeting them without their consent. This practice has the potential to harm people, threatens the capacity of individuals to manage who can access their personal data, and damage an organization's reputation when interacting with shareholders, customers and government agencies [3].

In prior literature, Willison [25] articulated that if people have experienced good privacy protections, such as explicit permission processes and transparent data use regulation, they are probably going to feel safer and at ease about their information being used for secondary purposes. The favorable encounter with the company managing their data cultivates confidence, resulting in increased consent for incidental applications such as customized services or advertising [26], [27]. Similarly, Yun et al. [28] user's involvement with privacy choices and preferences often goes up after a positive privacy experience. For example, customers are more likely to actively engage in managing how their data is used for secondary purposes if they are familiar with and have successfully handled their privacy setting in the past. This might include selecting their preferred degree of customization or opting in or out of particular data gathering techniques. Thus, in light of the preceding reasoning, we propose the accompanying hypothesis.

H_3: Prior privacy experience will have a positive influence on SUPI

D. Perceived Surveillance and Behavioral Intentions

In the context of mobile phone applications, the term "PSV" refers to the knowledge and perceptions of users about the observation or recording of their digital behaviours by applications or app makers [17]. This view may include a number of different elements of surveillance, including the collecting of data, the tracking of location or browsing behavior, and keeping track of activities inside the actual application.

When people feel their behaviors are being observed or captured, they become more aware of their digital practices. In prior literature, Maytin et al. [29] articulated that individuals tend to engage in greater self-regulation as a result of their enhanced awareness because they are more careful about the information they share, the applications they use, and the material they view. Furthermore, risk-reduction practices like using safe passwords, upgrading software on a regular basis, and staying away from potentially dangerous websites and programmers are all encouraged by the perception of monitoring [30]. The knowledge that one is being watched encourages adherence to regulations in areas where there are explicit norms or standards, such office buildings or educational institutions, since noncompliance may be discovered. Ioannou and Tussyadiah [19] claims that while monitoring makes users feel safer and more secure, it surprisingly increases their faith and confidence in the security features

of mobile phone systems. The author might believe that negative players, such hackers, or unauthorized access attempts, are discouraged by the existence of monitoring. Because consumers believe their personal information and data are protected, this view might provide them a feeling of security. Thus, in light of the preceding reasoning, we propose the accompanying hypothesis.

H_4: PSV will have a positive influence on behavioral intentions

E. Perceived Intrusion and Behavioral Intentions

The concept of PIN refers to consumers' awareness that mobile applications have the potential to track their interactions, activities, and behaviors [4]. This might entail monitoring surfing history, location information, user preferences, and other digital traces. When users believe that their activities are being watched over or recorded without their knowledge or agreement, they may feel violated.

It is possible for users to become more conscious of their online activity as they learn that they may be monitored, or their privacy invaded if they are aware of possible intrusions [24]. When users perceive that their cell phone activities are being observed or intruded upon, they get more aware of what they're doing, leading to a stronger sense of accountability in what they do. This awareness frequently prompts users to take precautions against anticipated attacks and protect their privacy, such as utilizing encoding software or modifying privacy settings [22]. In an ironic way, users' perception of the system's ability to detect and respond to intrusions can increase their faith in mobile device safety precautions, when possible, intrusions are detected. Therefore, individuals might grow to have favorable attitudes and intentions regarding safe phone use. Sigurdsson et al. [31] claims that people change their behavior in response to PIN, steering clear of harmful internet usage and encouraging more circumspect sharing of data. It is claimed by Wottrich et al. [22] that users are more likely to follow norms and guidelines in regulated environments—such as those subject to privacy regulations—when they feel an intrusion because they know that their actions are being watched. Thus, in light of the preceding reasoning, we propose the accompanying hypothesis.

H_5: PIN will have a positive influence on behavioral intentions

F. Secondary Use of Personal Information and Behavioral Intentions

There are many secondary reasons why personal information might be used, including market research, targeted advertising, improving user experience, developing new products or services, strengthening security protocols, or conducting scholarly or scientific research [3]. It is possible for developers to get insight into user behavior on their platforms by doing identity analysis. They may optimize interfaces, features, and content to provide a smooth and fulfilling user experience by determining pain areas, choices, and use trends.

In the event that a user discovers that personal information about them—such as their browsing history, location data, or purchase patterns—is being collected and used for reasons other than those for which they initially provided permission, they may become less trusting and feel as if their privacy has been violated [32]. This breach of trust may cause users to become more cautious and reluctant to interact with the app. These factors may influence their behavior, such as using the app less often, submitting less information, or even deleting it altogether. In previous works, Zhang et al. [34] asserted that consumers may suffer major repercussions from identity theft, individualized marketing, or security issues as a result of abuse or unauthorized sharing of personal information. These worries have the potential to severely discourage users from providing private information or actively engaging in app activities, which might result in unfavorable behavioral intents like avoidance or disengagement. According to Nikolopoulou et al.[36] , user trust and desire to interact with applications that utilize their personal information for secondary purposes might be further damaged by news stories or widely reported privacy violations. Thus, in light of the preceding reasoning, we propose the accompanying hypothesis.

H_6: SUPI will have a positive influence on behavioral intentions

G. Moderating Role of Technical Security Knowledge

The technical security knowledge of a mobile phone user includes a thorough understanding and familiarity with mobile device privacy and security features [37]. This entails being aware of the encryption techniques used to protect data, such as end-to-end encryption in chat applications or protected storage options for private data.

A person with more technical security knowledge may process surveillance cues more intricately in their minds. Frick et al. [17] claimed that a individuals will probably conduct a more thorough analysis of the surveillance environment, taking into account things like data handling procedures, encryption techniques, and the reliability of data gathering systems. Their ability to distinguish between harmless security measures and incurable surveillance is facilitated by their cognitive depth, which also mitigates the influence of previous privacy experiences on their PSV levels. Similarly, mobile phone users are better equipped to make privacy-related decisions when they are knowledgeable about technical security [38]. According to Foltz and Foltz [23], people can lessen the influence of previous privacy events on their perceived levels of surveillance by setting privacy preferences, managing data sharing, and adopting secure habits. This empowerment encourages a fair assessment of the dangers of mobile spying and privacy issues. It is also possible to reduce information processing biases associated with surveillance cues by gaining technical expertise in security. A higher knowledge level makes people less vulnerable to false information and sensationalized stories about surveillance, so they can critically assess surveillance-related material [39]. Due to people's reliance on factual evaluations of surveillance hazards rather than inflated views fueled by deception, past privacy experiences mitigate the impact of PSV. Thus, in light of the preceding reasoning, we propose the accompanying hypothesis (See Table 1).

H_7: Technical security knowledge will have a positive moderation effect between the relationship of prior privacy experience and PSV

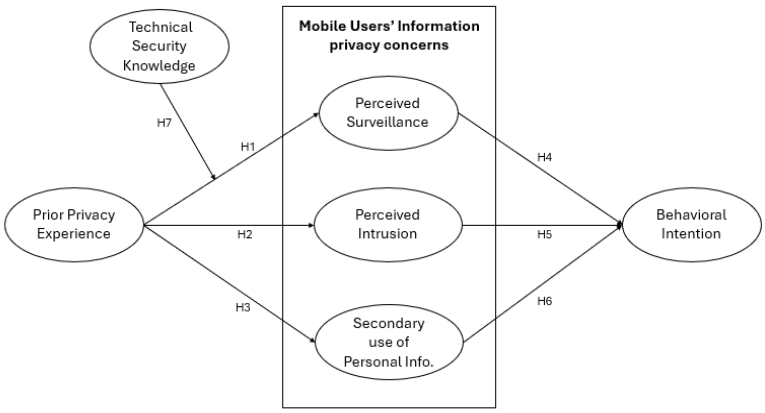

Fig. 1 Conceptual Framework

III.Method

A. Sampling and data collection

To assess the proposed hypotheses, we designed an online survey and recruited participants from an online social networking site. We specifically targeted individuals from the United States because of accessibility. The survey was entirely optional, and we provided rewards in the kind of three $50 vouchers to Amazon. It is standard procedure in survey methodology to provide incentives in return for participation. We recruited volunteers by posting notices with background information about the study. We refrained from revealing in the announcements that the study's primary emphasis was privacy concerns to mitigate the possibility of bias resulting from respondents' self-selection. We requested feedback from the audience on a mobile social networking app during the announcements. By using the URL included in the posting, the subjects could join with ease. Out of the 812

participants, 574 were able to provide data that could potentially be used with a response rate of 70.81%. Among the respondents, 335 were female (44.1%), with 39.1% under 20 years old and 36.3% aged 21-30. Students comprised 59.% of participants, while 35.3% were employed. The majority had a college degree (40.9%) and reported household incomes between ≤ $20,000 (27.0%) and $20,001-$40,000 (36.6%). Majority of the participants were using IOS as primary mobile operating systems (See Table 1).

B. Measures

The questionnaire items used in this study were adapted from previous research. A 7-point Likert scale was used by participants to rate each item with 1 representing "strongly disagree" and 7 representing "strongly agree" [40]. We adjusted the measurement items' meaning and in line them with mobile phone user context. *Prior Privacy Experience* is measured using three multi-item scales adapted from Xu et al. [3]. Similarly, a three-item scale was used to assess *PSV* and adapted from the study of [23]. In addition, *PIN* scale consists of three items and were adapted from [23]. Moreover, *SUPI* is also adapted from prior study Smith et al. (1996) and consist of three item scales. On the other hand, *behavioral intention* scale was adapted from the research of Xu et al. [3] and consist of four items scale. In last, technical security knowledge is also adapted from prior literature [41] and consist of four items scale.

Table 1. Sample Properties

Participants' characteristics	Frequency	Percentage
Gender		
Male	321	55.9
Female	253	44.1
Age		
>18 years	55	9.6
18-22 years	216	37.6
23-27 years	165	28.7
28-30 years	88	15.3
< 30 years	50	8.7
Profession		
Employed	191	33.3
Homemaker	55	9.6
Self	35	6.1
Student	281	49.0
Other	12	2.1
Educational background		
Less than high school	8	1.4
High school degree	133	23.2
College degree	235	40.9
Undergraduate degree	99	17.2
Graduate degree	88	15.3
Other	11	1.9
Yearly household net income		
≤ $20,000	155	27.0
$20,001-$40,000	210	36.6
$40,001-$60,000	95	16.6
$60,001-$100,000	79	13.8
> $100,000	35	6.1
Mobile operating system		
Android	238	41.5
iOS	321	55.9
Other	15	2.6

*IV.*4. Results

A. Measurement model validation

To examine the interrelationships among the variables, we employed correlation analysis. The statistical analysis revealed a very significant relationship between the tested variables (See Table 2). We used the square root of AVE to examine construct validity. The fact that AVE's square root is greater than its correlation with additional variables, the findings provide evidence for discriminant validity [42]. Alternately, discriminant validity may be determined by evaluating AVE by MSV value with all factors. If AVE exceeds MSV, discriminant validity is attained. [43]. According to discriminant validity model selection, the square root of the AVE is greater than its correlation with other variables [43]. Furthermore, Table 3 demonstrates that every variable has a composite reliability (CR) value greater than 0.70 [44]. A convergent validity assessment was then conducted by examining the relationship between these factors using AVE and item loadings [45]. The results show that every variable meets the requirement and shows more than 50% variability, with AVE values more than 0.5. The comprehensive test results are shown in Table 3.

Table 2. Discriminant validity.

Constructs	**1**	**2**	**3**	**4**	**5**	**6**
Technical Security Knowledge	**0.804**					
Behavioral Intention	0.629	**0.795**				
Perceived Surveillance	0.695	0.719	**0.881**			
Perceived Intrusion	0.443	0.659	0.568	**0.865**		
Prior Privacy Experience	0.529	0.511	0.588	0.350	**0.850**	
Secondary use of Personal Info.	0.726	0.562	0.610	0.428	0.460	**0.874**

The bold values are the √AVE.

B. Reliability analysis

We conducted reliability analyses for all constructs using the Cronbach's alpha approach, following the recommendation by Nunnally [46]. The results indicated that the Cronbach's alpha values for every construct exceeded the 0.70 criterion, ensuring the reliability of the data. To assess the internal consistency of the items within each construct, we also calculated the Composite Reliability (CR) values. The CR values were found to surpass the threshold amount of 0.70, as suggested by Hair Jr. et al. [47]. Details of these analyses are provided in Table 3.

Table 3. Factor loading, validity, and reliability of the indicators.

Constructs	**Items**	**Loadings**	**VIF**	**α**	**CR**	**AVE**
Technical Security Knowledge				0.821	0.880	0.647
	TSK1	0.767	2.306			
	TSK2	0.815	2.481			
	TSK3	0.805	1.740			
	TSK4	0.830	1.756			
Behavioral Intention				0.805	0.873	0.632
	BIN1	0.821	1.817			
	BIN2	0.850	1.987			
	BIN3	0.763	1.550			
	BIN4	0.742	1.538			
Perceived Surveillance				0.856	0.913	0.777
	PSV1	0.874	1.954			
	PSV2	0.889	2.278			
	PSV3	0.882	2.260			
Perceived Intrusion				0.834	0.899	0.749
	PIN1	0.920	2.577			
	PIN2	0.775	1.694			
	PIN3	0.893	2.126			
Prior Privacy Experience				0.806	0.886	0.723
	PPE1	0.815	1.878			

Secondary use of Personal Info.	PPE2	0.922	2.650	0.845	0.906	0.763
	PPE3	0.809	1.711			
	SUPI1	0.905	2.556			
	SUPI2	0.870	2.107			
	SUPI3	0.846	1.817			

C. Common method variance

Numerous statistical and methodological approaches been employed to evaluate common method variance (CMV). First, questions were designed with simplicity, specificity, and shortness in mind. A pilot research was carried out to evaluate the instruments' applicability [48]. Furthermore, the impact of CMV was assessed using Harman's single-factor test, which proposes that CMV exists if one component explains at least 50% of the overall variation [48], [49]. The research's main significant component explained 35.89% of the variation, which is less than the 50% criterion, and indicates that common method variance (CMV) is not present. Additionally, in order to analyze CMV, Bagozzi et al. [50] investigated the relationship between latent variables. The variable correlations were all less than 0.90. Therefore, it seems from our statistical studies that there is no CMV in the data.

D. Multicollinearity

A regression study was performed to determine the threshold values, variance inflation factor (VIF), and multicollinearity. VIF values shouldn't be higher than 0.3 [51]. Given that each variable's VIF score, and threshold are within the suggested ranges, the findings reveal that there are no multicollinearity problems with this model [52].

E. The predictive power of the model (Q^2)

We evaluated our structural model on SmartPLS by applying the Stone and Geisser test. When a theoretical framework's Q2 value is larger than zero (>0) for that particular theoretical framework, it indicates that the model itself has predictive power [53]. As a result, all of the dependent variables in a path model have Q2 values greater than zero, proving the path model's validity (see Table 4).

Table 4. Blindfolding statistics for the general model.

Construct	SSO	SSE	(Q^2 = 1-SSE/SSO)
Technical Security Knowledge	800	635.121	0.206
Behavioral Intention	800	689.25	0.138
Perceived Surveillance	800	611.58	0.235
Perceived Intrusion	1000	947.225	0.052
Prior Privacy Experience	800	694.772	0.132
Secondary use of Personal Info.	1000	850.359	0.150

F. Structural model and hypothesis outcomes

An examination of the findings revealed a significant positive impact of prior privacy experience on PSV (H1–$\beta = 0.236$, $p < 0.01$). Furthermore, prior privacy experience has a positive and significant association with PIN (H2–$\beta = 0.350$, $p < 0.01$). The findings also revealed that prior privacy experience has strong and positive connection with SUPI (H3–$\beta = 0.460$, $p < 0.01$). Therefore, our first, second and third hypotheses supported the study. Additionally, the direct impact of the fourth hypothesis indicated that PSV was significantly related to behavioral intention (H4–$\beta = 0.428$, $p < 0.05$). In addition, PIN has a positive and significant impact on behavioral intention (H5–$\beta = 0.351$, $p < 0.01$). Furthermore, findings indicated that SUPI has a positive influence on behavioral intention (H6–$\beta = 0.151$, $p < 0.01$). In last, the findings articulate that technical security knowledge has a negative and significant moderation influence on the relationship between prior privacy experience and PSV (H7–$\beta = -0.081$, $p < 0.01$). As a result, our study's hypotheses H7 was supported (See Table 5).

Table 5. Hypotheses testing.

	Hypotheses	Beta	S.D	*t*-values	*p*-values	Decision
H1	Prior Privacy Experience -> Perceived Surveillance	0.236	0.081	2.910	0.004	Accepted
H2	Prior Privacy Experience -> Perceived Intrusion	0.350	0.080	4.398	0.000	Accepted
H3	Prior Privacy Experience -> Secondary use of Personal Info.	0.460	0.088	5.228	0.000	Accepted
H4	Perceived Surveillance -> Behavioral Intention	0.428	0.083	5.129	0.000	Accepted
H5	Perceived Intrusion -> Behavioral Intention	0.351	0.079	4.454	0.000	Accepted
H6	Secondary use of Personal Info. -> Behavioral Intention	0.151	0.062	2.435	0.001	Accepted
H7	Technical Security Knowledge × Prior Privacy Experience -> Perceived Surveillance	-0.081	0.025	3.240	0.013	Accepted

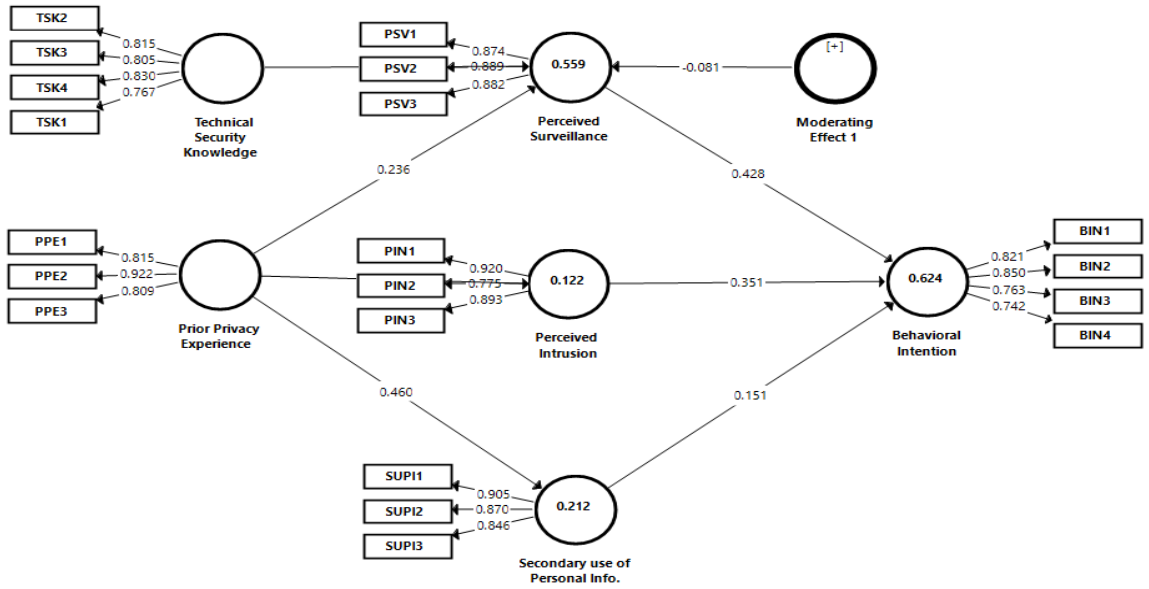

Fig. 2 Results of hypotheses

V.Discussion

A. Major findings

The aim of this study is to elucidate the influence of app authorization requests on the information privacy concerns of mobile users in relation to their behavioral intentions and prior privacy experiences. The findings of a PLS-SEM study including 574 participants showed that PSV, PIN, and SUPI have a significant effect on their behavioral intention. This analysis also considered technical security knowledge as a possible moderator in this research.

Firstly, the findings of the research revealed that prior privacy experience has a positive and significant influence on mobile user's information privacy concerns. These findings are in consistent with the previous research of Degirmenci [10] who believed that prior privacy experience is a more appropriate and sophisticated approach for resolving privacy problems related to mobile user data. According to Ghosh et al. [18], people are more likely to carefully analyze the surveillance practices associated with mobile phone usage and compare them to their past experiences. A user's perception of surveillance risk may be reduced when they have positive experiences, such as effective privacy protection mechanisms or free information processing procedures [19]. Similarly, it is clearly mentioned in prior literature that people are more inclined to trust the organization handling their data if they have

had positive privacy experiences, such as clear and transparent data handling procedures, efficient privacy protection measures, and open and respectful communication [10], [22], [23]. The findings posit that if people have experienced good privacy protections, such as explicit permission processes and transparent data use regulation, they are more likely to feel secure and at ease about their information being used for secondary purposes.

Secondly, the findings signify that PSV, PIN and SUPI are strongly connected with behavioral intention of mobile of user. The findings are in line with the prior literature Foltz and Foltz [23], emphasize information privacy concerns play an important role in shaping mobile device users' decisions and actions. In situations where people feel that their digital behaviors are observed or captured, they become more aware of them. Maytin et al. [29] assert that individuals engage in greater self-regulation because of their increased awareness since they are more cautious about the information they share, the applications they use, and the material they view. Furthermore, risk-reduction practices like using safe passwords, upgrading software on a regular basis, and staying away from potentially dangerous websites and programmers are all encouraged by the perception of monitoring [30]. Similarly, when users perceive that their cell phone activities are being observed or intruded upon, they get more aware of what they're doing, leading to a stronger sense of accountability in what they do. This awareness frequently prompts users to take precautions against anticipated attacks and protect their privacy, such as utilizing encoding software or modifying privacy settings [22]. In an ironic way, users' perception of the system's ability to detect and respond to intrusions can increase their faith in mobile device safety precautions, when possible, intrusions are detected. The findings suggest that consumers may suffer major repercussions from identity theft, individualized marketing, or security issues as a result of abuse or unauthorized sharing of personal information.

Lastly, the findings postulate that technical security knowledge has a negative moderation between the relationship of prior privacy experience and PSV. This finding is contradicts the research of Barth et al. [54]. The contradiction stems from the divergent views on the function of technical security knowledge. Barth et al. [54] suggested that a greater level of technical security knowledge lowers PSV, but the current hypothesis suggest that suggests a negative moderation effect, meaning that a higher level of technical security knowledge may not always relieve concerns about PSV based on past privacy experience. A higher knowledge level makes people less vulnerable to false information and sensationalized stories about surveillance, so they can critically assess surveillance-related material [39].

B. Research implications

Our research adds to the body of privacy knowledge in a number of ways. *Firstly*, our main contribution is to provide insight into how past privacy experience relate to mobile consumers' privacy concerns. While earlier research has concentrated on specific traits of mobile phone privacy concerns [54], [55], in this research, we analyze mobile users' concerns particularly PSV, PIN, and SUPI in respect of prior privacy expedience. By focusing on these specific aspects, we aim to get better understanding of how individual previous privacy experience impact their perceptions and reactions to possible privacy concerns in the mobile phone context. Our research contributes to more thorough knowledge of mobile phone user privacy behavior by enabling us to find subtle insights into the interaction between different aspects of privacy concerns and past privacy experience. *Secondly*, we address the call made by Smith et al. [56] for studies to look at a wider range of antecedents in various contexts within the APCO model. Our study focused on the mobile environment, incorporating factors such as technical security knowledge from previous privacy studies. *Third*, our work adds to the body of literature by putting these variables in as determinants in the APCO concept from the viewpoint of mobile. The reason for this is that mobile applications are becoming more and more common, which also raises more concerns about privacy.

C. Practical implications

Practically speaking, app stores and providers should be concerned about the impact that unfavorable prior experiences on users' privacy concerns. These concerns can discourage users from downloading and using mobile apps or cause them to feel uneasy, which may lead them to remove the app. Therefore, app developers must make sure that they only access user information kept on mobile devices when required and supported by value-added services, including location tracking for navigational reasons. Our findings indicate that worries over app authorization significantly influence mobile consumers' overall concerns about information privacy. Developers must prioritize privacy in design, ensuring that privacy controls and features are seamlessly integrated into the user experience. It's important for developers to follow transparent data standards, which include telling users up front in the app's setting and preferably before they install the app what data it gathers, how it's used and with whom its shared. To further strengthen user trust and privacy protection, it is important to establish explicit rules on data retention, undertake privacy impact assessment, and adhere to applicable regulation. A secure mobile eco-system that promotes trust and sustained user engagement is facilitated by ongoing changes based on user input, user education and transparency initiatives.

D. Limitations and future research direction

Firstly, our findings serve as a foundation for further research on information privacy issues among mobile users with an emphasis on prior privacy experiences, particularly in light of the growing privacy-related problems facing app stores and providers. Future research should delve into the awareness of IoT privacy risks among users. The privacy paradox, highlighting the disparity between user statements and behaviors regarding privacy, may partially stems from a lack of understanding about the extensive data collection and sharing practices of IoT devices. Investigating the impact of prior privacy experiences, particularly in the context of IoT, is crucial to understanding user's privacy concerns effectively. *Secondly*, exploring the effectiveness of training and education initiatives in addressing information privacy concerns is an important avenue for future research. *Thirdly*, the study's dependency on a single sample size limits its applicability; an expanded and more diverse sample of art students would strengthen the study robustness. *Lastly*, a more comprehensive understanding of the variables may need the use of objective measurements or mix method techniques, because the use of self-report measures or surveys may introduce response biases.

REFERENCES

[1] Y.-L. Wu and Y.-S. Ye, "Understanding impulsive buying behavior in mobile commerce," 2013.

[2] L. Gao, K. A. Waechter, and X. Bai, "Understanding consumers' continuance intention towards mobile purchase: A theoretical framework and empirical study - A case of China," *Comput. Human Behav.*, 2015, doi: 10.1016/j.chb.2015.07.014.

[3] H. Xu, S. Gupta, M. B. Rosson, and J. M. Carroll, "Measuring mobile users' concerns for information privacy," 2012.

[4] Y. Feng and Q. Xie, "Privacy concerns, perceived intrusiveness, and privacy controls: an analysis of virtual try-on apps," *J. Interact. Advert.*, vol. 19, no. 1, pp. 43–57, 2019.

[5] J. C. Sipior, B. T. Ward, and L. Volonino, "Privacy concerns associated with smartphone use," *J. Internet Commer.*, vol. 13, no. 3–4, pp. 177–193, 2014.

[6] D. J. Leith, "Mobile handset privacy: Measuring the data iOS and Android send to Apple and Google," in *Security and Privacy in Communication Networks: 17th EAI International Conference, SecureComm 2021, Virtual Event, September 6–9, 2021, Proceedings, Part II 17*, 2021, pp. 231–251.

[7] D. Zhang, B. Adipat, and Y. Mowafi, "User-centered context-aware mobile applications—The next generation of personal mobile computing," *Commun. Assoc. Inf. Syst.*, vol. 24, no. 1, p. 3, 2009.

[8] I. A. Junglas, N. A. Johnson, and C. Spitzmüller, "Personality traits and concern for privacy: an empirical study in the context of location-based services," *Eur. J. Inf. Syst.*, vol. 17, no. 4, pp. 387–402, 2008.

[9] Y. Jung and J. Park, “An investigation of relationships among privacy concerns, affective responses, and coping behaviors in location-based services,” *Int. J. Inf. Manage.*, vol. 43, pp. 15–24, 2018.

[10] K. Degirmenci, “Mobile users’ information privacy concerns and the role of app permission requests,” *Int. J. Inf. Manage.*, vol. 50, pp. 261–272, 2020.

[11] D. HJ, “Informing privacy research through information systems, psychology, and behavioral economics: thinking outside the ‘apco’ box,” *Inf. Syst. Res.*, vol. 264, pp. 639–655, 2015.

[12] F. Bélanger and R. E. Crossler, “Privacy in the digital age: a review of information privacy research in information systems,” *MIS Q.*, pp. 1017–1041, 2011.

[13] T. Dinev and P. Hart, “Internet privacy concerns and their antecedents-measurement validity and a regression model,” *Behav. Inf. Technol.*, vol. 23, no. 6, pp. 413–422, 2004.

[14] H. Xu, T. Dinev, H. J. Smith, and P. Hart, “Examining the formation of individual’s privacy concerns: Toward an integrative view,” 2008.

[15] H. J. Smith, S. J. Milberg, and S. J. Burke, “Information privacy: Measuring individuals’ concerns about organizational practices,” *MIS Q.*, pp. 167–196, 1996.

[16] T. Dinev and P. Hart, “An extended privacy calculus model for e-commerce transactions,” *Inf. Syst. Res.*, vol. 17, no. 1, pp. 61–80, 2006.

[17] N. R. J. Frick, K. L. Wilms, F. Brachten, T. Hetjens, S. Stieglitz, and B. Ross, “The perceived surveillance of conversations through smart devices,” *Electron. Commer. Res. Appl.*, vol. 47, p. 101046, 2021.

[18] A. K. Ghosh, K. Badillo-Urquiola, S. Guha, J. J. LaViola Jr, and P. J. Wisniewski, “Safety vs. surveillance: what children have to say about mobile apps for parental control,” in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018, pp. 1–14.

[19] A. Ioannou and I. Tussyadiah, “Privacy and surveillance attitudes during health crises: Acceptance of surveillance and privacy protection behaviours,” *Technol. Soc.*, vol. 67, p. 101774, 2021.

[20] D. J. Solove, “A taxonomy of privacy,” *U. Pa. l. Rev.*, vol. 154, p. 477, 2005.

[21] W. Cheng, Y. Xu, Z. Deng, and C. Gu, “GPS Radio Occultation Data Assimilation in the AREM Regional Numerical Weather Prediction Model for Flood Forecasts,” *Adv. Meteorol.*, vol. 2018, 2018, doi: 10.1155/2018/1376235.

[22] V. M. Wottrich, E. A. van Reijmersdal, and E. G. Smit, “The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns,” *Decis. Support Syst.*, vol. 106, pp. 44–52, 2018.

[23] C. B. Foltz and L. Foltz, “Mobile users’ information privacy concerns instrument and IoT,” *Inf. Comput. Secur.*, vol. 28, no. 3, pp. 359–371, 2020.

[24] D. Wu, G. D. Moody, J. Zhang, and P. B. Lowry, “Effects of the design of mobile security notifications and mobile app usability on users’ security perceptions and continued use intention,” *Inf. Manag.*, vol. 57, no. 5, p. 103235, 2020.

[25] D. Willison, “Privacy and the secondary use of data for health research: Experience in Canada and suggested directions forward,” *J. Health Serv. Res. Policy*, vol. 8, no. 1_suppl, pp. 17–23, 2003.

[26] G. D’Souza and J. E. Phelps, “The privacy paradox: The case of secondary disclosure,” *Rev. Mark. Sci.*, vol. 7, no. 1, p. 0000102202154656161072, 2009.

[27] M. Korzaan, N. Brooks, and T. Greer, “Demystifying personality and privacy: An empirical investigation into antecedents of concerns for information privacy,” *J. Behav. Stud. Bus.*, vol. 1, p. 1, 2009.

[28] H. Yun, G. Lee, and D. J. Kim, “A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs,” *Inf. Manag.*, vol. 56, no. 4, pp. 570–601, 2019.

[29] L. Maytin, J. Maytin, P. Agarwal, A. Krenitsky, J. Krenitsky, and R. S. Epstein, “Attitudes and perceptions toward COVID-19 digital surveillance: Survey of young adults in the United States,” *JMIR Form. Res.*, vol. 5, no. 1, p. e23000, 2021.

[30] G. Fox, T. Clohessy, L. van der Werff, P. Rosati, and T. Lynn, “Exploring the competing influences of privacy concerns

and positive beliefs on citizen acceptance of contact tracing mobile applications," *Comput. Human Behav.*, vol. 121, p. 106806, 2021.

[31] V. Sigurdsson, R. G. V. Menon, A. G. Hallgrímsson, N. M. Larsen, and A. Fagerstrøm, "Factors affecting attitudes and behavioral intentions toward in-app mobile advertisements," *J. Promot. Manag.*, vol. 24, no. 5, pp. 694–714, 2018.

[32] S. Y. Park, M. Nam, and S. Cha, "University students' behavioral intention to use mobile learning: Evaluating the technology acceptance model," *Br. J. Educ. Technol.*, vol. 43, no. 4, pp. 592–605, 2012.

[33] L. Zhang, W. Ran, S. Jiang, H. Wu, and Z. Yuan, "Understanding consumers' behavior intention of recycling mobile phone through formal channels in China: The effect of privacy concern," *Resour. Environ. Sustain.*, vol. 5, p. 100027, 2021.

[34] L. Zhong, X. Zhang, J. Rong, H. K. Chan, J. Xiao, and H. Kong, "Construction and empirical research on acceptance model of service robots applied in hotel industry," *Ind. Manag. Data Syst.*, vol. 121, no. 6, pp. 1325–1352, 2021.

[35] K. Nikolopoulou, V. Gialamas, and K. Lavidas, "Habit, hedonic motivation, performance expectancy and technological pedagogical knowledge affect teachers' intention to use mobile internet," *Comput. Educ. Open*, vol. 2, p. 100041, 2021.

[36] A. Misargopoulos *et al.*, *Building a Knowledge-Intensive, Intent-Lean, Question Answering Chatbot in the Telecom Industry - Challenges and Solutions*, vol. 652 IFIP. Springer International Publishing, 2022.

[37] K. Khando, S. Gao, S. M. Islam, and A. Salman, "Enhancing employees information security awareness in private and public organisations: A systematic literature review," *Comput. Secur.*, vol. 106, p. 102267, 2021.

[38] I. Androulidakis and G. Kandus, "Mobile phone security awareness and practices of students in budapest," in *Proceedings of the 6th International Conference on Digital Telecommunications*, 2011, pp. 17–22.

[39] T. Moletsane and P. Tsibolane, "Mobile information security awareness among students in higher education: An exploratory study," in *2020 conference on information communications technology and society (ICTAS)*, 2020, pp. 1–6.

[40] G. Albaum, "The Likert Scale Revisited:," *Int. J. Mark. Res.*, vol. 39, no. 2, pp. 331–348, Jan. 2018, doi: 10.1177/147078539703900202.

[41] E. C. Whipple, K. L. Allgood, and E. M. Larue, "Third-year medical students' knowledge of privacy and security issues concerning mobile devices," *Med. Teach.*, vol. 34, no. 8, pp. e532–e548, 2012.

[42] M. Ahmad *et al.*, "Modeling heterogeneous dynamic interactions among energy investment, SO2 emissions and economic performance in regional China," *Environ. Sci. Pollut. Res.*, vol. 27, no. 3, pp. 2730–2744, 2020, doi: 10.1007/s11356-019-07044-3.

[43] C. Fornell and D. F. Larcker, "Structural equation models with unobuervable variables and measurement error: Algebra and statistics," *J. Mark. Res.*, vol. 18, no. 3, p. 382, 1981, doi: 10.2307/3150980.

[44] J. F. Hair, W. C. Black, B. J. Babin, and R. E. Anderson, *Multivariate Data Analysis*. New Jersey: Prentice-Hall, Inc., 2006.

[45] K. K. K.-K. Wong, "Partial Least Squares Structural Equation Modeling (PLS-SEM) Techniques Using SmartPLS," *Mark. Bull.*, vol. 24, no. 1, pp. 1–32, 2013.

[46] J. C. Nunnally, *Psychometric theory 3E*. New York, NY.: Tata McGraw-hill education, 1994.

[47] J. F. Hair Jr., L. M. Matthews, R. L. Matthews, and M. Sarstedt, "PLS-SEM or CB-SEM: Updated guidelines on which method to use," *Int. J. Multivar. Data Anal.*, vol. 1, no. 2, p. 107, 2017, doi: 10.1504/ijmda.2017.10008574.

[48] P. M. Podsakoff, S. B. MacKenzie, J. Y. Lee, and N. P. Podsakoff, "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies," *Journal of Applied Psychology*, vol. 88, no. 5. pp. 879–903, Oct. 2003, doi: 10.1037/0021-9010.88.5.879.

[49] H. H. Harman, *Modern factor analysis, 3rd rev. ed.* 1976.

[50] R. P. Bagozzi, Y. Yi, and L. W. Phillips, "Assessing construct validity in organizational research," *Adm. Sci. Q.*, pp. 421–458, 1991.

[51] A. Field, *Discovering statistics using IBM SPSS statistics*. Sage, 2013.

[52] L. Strupeit and A. Palm, “Overcoming barriers to renewable energy diffusion: Business models for customer-sited solar photovoltaics in Japan, Germany and the United States,” *J. Clean. Prod.*, vol. 123, pp. 124–136, 2016, doi: 10.1016/j.jclepro.2015.06.120.

[53] J. F. Hair, G. T. M. Hult, C. Ringle, and M. Sarstedt, “A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM),” *SAGE Publication Inc*, 2016. .

[54] S. Barth, M. D. T. de Jong, M. Junger, P. H. Hartel, and J. C. Roppelt, “Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources,” *Telemat. informatics*, vol. 41, pp. 55–69, 2019.

[55] A. F. Westin, “Social and political dimensions of privacy,” *J. Soc. Issues*, vol. 59, no. 2, pp. 431–453, 2003.

[56] H. J. Smith, T. Dinev, and H. Xu, “Information privacy research: an interdisciplinary review,” *MIS Q.*, pp. 989–1015, 2011.