EMERGING APPLICATIONS ON SMART PHONES: THE ROLE OF PRIVACY CONCERNS AND ITS ANTECEDENTS ON SMART PHONES USAGE

Waleed Al-Ghaith

Department of Information Systems, Shaqra University, (Imam Muhammad Ibn Saud Islamic University), Riyadh, Saudi Arabia

ABSTRACT

Many applications on smart Phones can use various sensors embedded in the mobiles to provide users' private information. This can result in a variety of privacy issues that may lessening level of mobile apps usage. To understand this issue better the researcher identified the root causes of privacy concerns. The study proposed a model identifies the root causes of privacy concerns and perceived benefits based on our interpretation for information boundary theory. The proposed model also addresses the usage behavior and behavioral intention toward using mobile apps by using the Theory of Planned Behavior. The result shows that "Cultural values" alone explains 70% of "Perceived privacy concerns" followed by "Self-defense" which explains around 23% of "Perceived privacy concerns", and then "Context of the situation" with 5%. Whereas, the findings show that "Perceived effectiveness of privacy policy" and "Perceived effectiveness of industry self-regulation" both are factors which have the ability to reduce individuals "Perceived privacy concerns" by 9% and 8% respectively.

KEYWORDS

Mobile Phone, information boundary theory, Communication Privacy Management theory, Perceived privacy concerns, Theory of Planned Behavior

1. INTRODUCTION

In recent years, we have witnessed the rapid growth of mobile handheld devices such as cell phones and personal digital assistants (PDAs). According to a March 2020 CISCO report "By 2023, the number of IP-connected devices would be more than three times the global population and there will be 3.6 networked devices per capita, compared to 2.4 devices per capita in 2018. By 2023, there will be a total of 29.3 billion connected devices, up from 18.4 billion in 2018." [1].

This growth refers to mobile ability to communicate virtually from anywhere with an unprecedented level of flexibility and convenience. Thus, the use of mobile handheld devices has become pervasive in our life. Accessing the Web and checking emails through a handheld device has become a common daily routine. This leads to emergence the mobile application industry, especially since the appearance of smartphones such as the iPhone.

A mobile application software (widely known as "apps") is a computer program developed to run on mobile devices such as smartphones and tablet computers. Some applications are commonly preinstalled, such as a web browser, email client and mapping program. Others are usually available through application distribution platforms and are typically operated by the owner of the mobile operating system, for instance the App Store for apple products, Google Play for android operating systems, Windows Phone Store, and BlackBerry App World.

The latest generations of smartphone devices are equipped with significantly improved processing capacity that approaches to that of a personal computer. These devices provide numerous sensors, such as GPS, accelerometer, compass, microphone and cameras which enable capturing the users' context and using the context to addressing the mobile users' needs. These sensors also can be used by mobile applications to gather a lot of "facts" that can be used in deducing context and knowledge regarding users' habits, their whereabouts, their movements, and events, and then offer them personalized information and individually tailored services based on that information [2].

Companies in their pursuit of larger market share and higher profits usually tend to collect and transfer unauthorized customer private data. According to Angwin and Valentino-DeVries [3] android smart phones and iPhones secretly track user information and "Google and Apple are gathering location information as part of their race to build massive databases capable of pinpointing people's locations via their cellphones" [3]. Smart phone's applications can easily accessed user location information without having the user's permission, and able to gather information from users address books [4].

This fact has increased concerns about the privacy of users' personal information, particularly, among individuals who used to use smartphone devices to achieve their needs or to keep secrets or for pleasure. Thus, on March 26, 2012, the Federal Trade Commission (FTC) issued its final report setting forth best practices for companies to protect the privacy of American consumers and allow them better control over their collected data. The FTC has taken legal action against corporations that have breached users or customers' privacy rights by failing to secure their consumers' sensitive data. For example on August 9, 2012 Google was forced to pay 22.5 million dollars to FTC in order to settle its fees for not protecting the privacy rights of safari users.

A January 2015 FTC report addressed user privacy and security risks. This report intensively identified the term of "Internet of Things" and identified privacy risks related to use any physical objects which connected to the Internet or to each other through small, embedded sensors, wired, or wireless technologies. The FTC report stated that "Some of these risks involve the direct collection of sensitive personal information, such as precise geo location, financial account numbers, or health information risks already presented by traditional Internet and mobile commerce. Others arise from the collection of personal information, habits, locations, and physical conditions over time, which may allow an entity that has not directly collected sensitive information to infer it" [5].

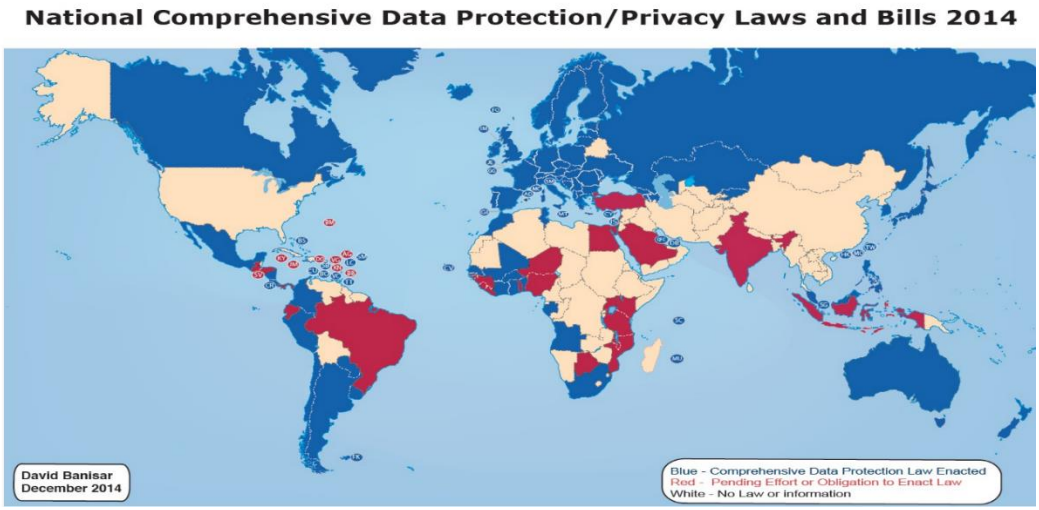

Figure 1. More than half of the world population still not covered by privacy laws [6].

Recognizing the notable effort made by FTC, however, USA still needs more effort in this field. Globally, privacy law is not a settled issue [7], since that more than half of the world population still not covered by privacy laws [6]. As shown in Figure 1, the white parts of the world represents areas or countries that not covered by any general privacy laws, the red or grey colors refer to areas that not covered by privacy law yet, but there is sort of legal debates happening, while the blue or darkest colors are areas of the world currently covered by privacy laws.

However, different view has been presented by DLA Piper's Data Protection Laws of the World Map which considers USA as a country with robust privacy legal requirements managed by the FTC which has jurisdiction over most commercial entities and has authority to issue and enforce privacy regulations (see Figure 2). In the Middle East and especially in Saudi Arabia there is no particular privacy laws or official national authority to protect the privacy of Saudi consumers and allow them greater control over the collection and use of their personal data [8].

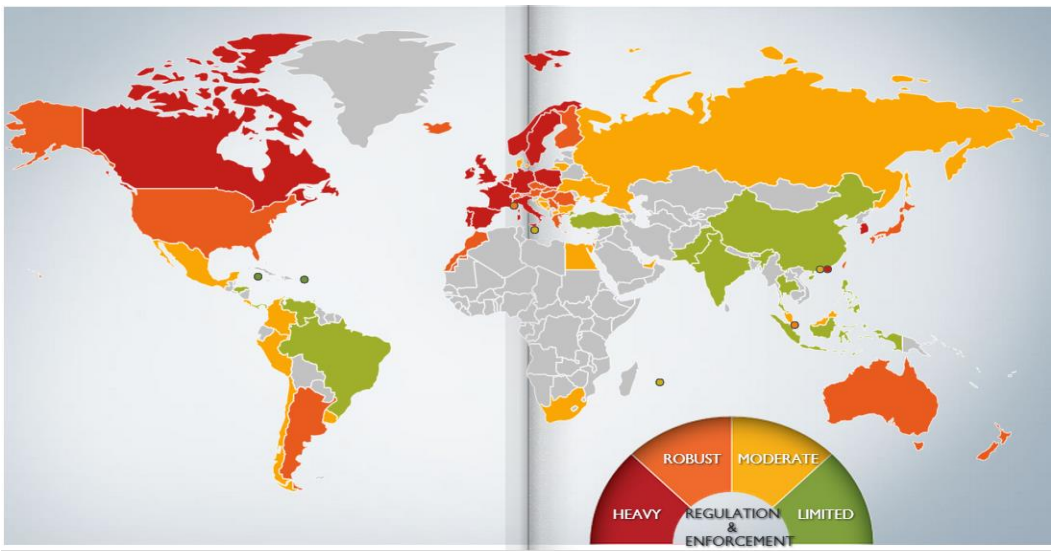

Figure 2. Data Protection Laws of the World [8].

In Saudi Arabia, there is no precise statistic number to measure rate of mobile apps usage however it can be predicted if we know that total number of active Twitter users in the Arab countries became 5,797,500 users as of March 2014 and Saudi Arabia is the country with the largest number of active Twitter users in the Arab world with 2.4 million users, accounting for over 40 percent of all active Twitter users in the Arab countries. In March2014, the total number of tweets created by Twitter users in the Arab world was 533,165,900, reflecting an average of 17,198,900 tweets per day [9]. Thus, we can conclude that rate of mobile apps usage is high among Saudi people (see Figure 3).

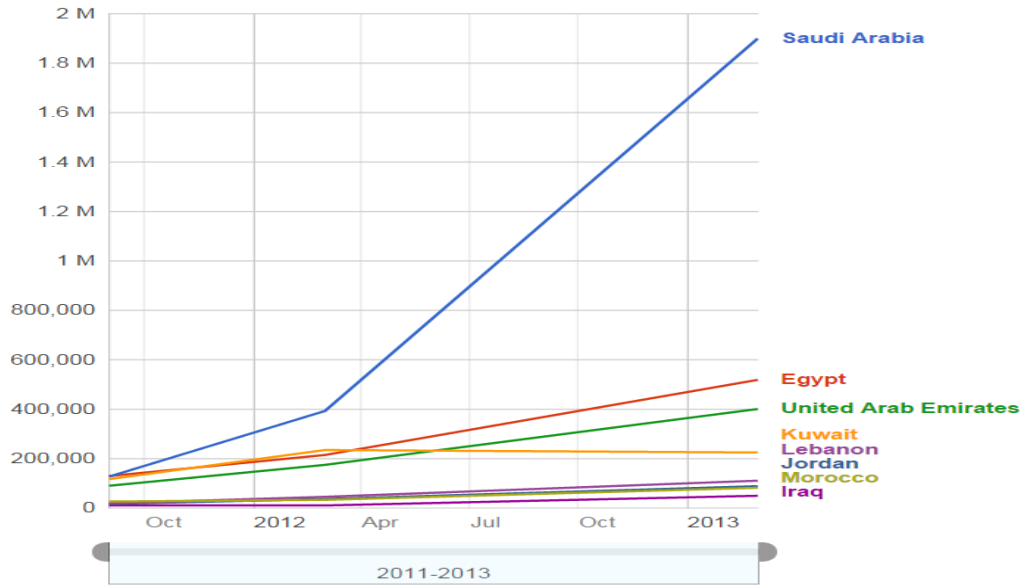

Figure 3. Number of Active Twitter users in the Middle East [9].

As a consequence, with high rate of mobile apps' usage and absence of privacy laws in Saudi Arabia, concerns about individuals' private information were increased. Since that the individual who is likely to perceive threats about absences of privacy laws that will lead to a higher level of privacy concerns. This may lessening level of mobile apps usage. To understand this issue better we should identify the root causes of privacy concerns [10]. Thus, the current study proposes an integrated theoretical framework brings together concepts from the Theory of Planned Behaviour (TPB) and Communication Privacy Management (CPM) theory.

The paper proceeds as follows. In section 2, we review new technologies which raised privacy concerns and present the study theoretical framework which includes Communication Privacy Management (CPM) theory, as a main theory that guides the development of the study model, and the Theory of Planned Behaviour (TPB). In section 2 also, the proposed hypotheses with the study model are presented. Thereafter, section 3, presents the methods of analysis. The findings of the study are then addressed in Section 4. Following that, in section 5, the Al-ghaith's equation [11] has been utilized to measure the contribution of every model's construct in the model's explanatory power. Section 5 presents discussion. Section 6 highlights the implications of the current study to theory and practice.

2. LITERATURE REVIEW AND THEORICAL FRAMWORK

2.1. New technologies raised privacy concerns

This section presents some of new technologies that coming into existence or development which may raise privacy concerns. The new technologies presented in this section are radio frequency identification (RFID) systems, GPS technology, Semantic Web Applications on smart Phones, Location Management Layer and Environment Layer.

2.1.1. RFID

Radio-frequency identification (RFID) is a technology uses electromagnetic fields to transfer data and provides a unique identifier for an object by attaching tag on that object. An RFID contains three basic components: A scanning antenna, a reader (transceiver), and a chip (transponder). A

chip or (transponder) is a RFID tag contains electronically information. A reader (transceiver) is a decoder to read and interpret the data from RFID chips. A scanning antenna provides the RFID chips with the energy to communicate [7]. The RFID is embedded in most android phones for several years and known as a Near-Field Communication (NFC) and there is a trend to adopt this technology as a convenient alternative for credit card, thus, mobiles with this technology could be used broadly for payments soon [12].

2.1.2. GPS Technology

A Global Positioning System (GPS) is a receiver utilizes four or more satellites to determine its dimensions from three known places to draw its current location. GPS, usually, is embedded in mobiles and cars [13].

2.1.3. Semantic Web Applications on Smart Phones

The current Web pages are human understandable however a computer is not able to understand the content and the meaning of the data. Semantic Web is developed to allow machines understand the web contents. With semantic web environment, entities or objects which have not had any previous interaction may now be able to automatically interact with each other [14]. Semantic Web Applications on smart Phones can use various sensors embedded in the mobiles, for instance RFID, GPS, compass, microphone, accelerometer, and cameras to provide many accurate private information that can be used in deducing context and knowledge regarding users' habits, their whereabouts, their movements, and events [2].

2.2. Theoretical framework

In the following sections, the Theory of Planned Behaviour (TPB) and Communication Privacy Management (CPM) theory are reviewed and discussed in relation to adoption of mobile apps in order to extract the most suitable framework for the study.

2.2.1. The Theory of Planned Behaviour (TPB)

The TPB is an extension of the theory of reasoned action (TRA) [15], hence, TPB as a theory has the ability to explain conditions in which persons have no complete control over their actions [16]. TPB is broadly used in a variety of research disciplines such as social psychology, Information Systems and marketing research in order to predict and understand individuals' behavioural intention and then their behaviour [17].

TPB proposes that behaviour is a direct consequent of behavioural intention and perceived behavioural control. Behavioural intention is a consequent of three factors: attitude (human feelings towards performing a behaviour), subjective norms (pressure to perform a behaviour) and perceived behavioural control (constraints on performing a behaviour). Each factor is in turn generated by a number of beliefs and evaluations [18, 19] (see Fig.1).

In the context of mobile apps, attitude refers to general user feelings towards the use of mobile apps based on the positive or negative outcome evaluation of performing that behaviour. Moreover, subjective norms refer to user perceptions regarding the use of mobile apps by the opinions of referent group (such as friends or colleagues). Perceived behavioural control reflects beliefs regarding access to the resources needed to use mobile apps which, in other words, describes user perceptions of the availability of knowledge, resources, and opportunities necessary for using mobile apps. Thus, this study considers TPB model hypotheses to form part of the study hypotheses as follows:

Hypothesis 1. User behavioural intention will positively influence user behaviour.
Hypothesis 2. Perceived behavioural control will positively influence user behaviour.
Hypothesis 3. User Attitude will positively influence user behavioural intention.
Hypothesis 4. Subjective norms will positively influence user behavioural intention.
Hypothesis 5. Perceived behavioural control will positively influence user behavioural intention.

2.2.2. Privacy Concerns

Privacy or "the right to be left alone" [20] or "full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection" [20]. Individuals' fears regarding invasion of their privacy and consequences of this invasion such as humiliation, insult, exploitation and emotional distress have paved the way for the emergence of privacy concerns as a term or Phenomenon. Privacy concerns is a key social issue which influencing individuals, since that the lack of privacy prevents people from introducing themselves, as they are really, in social interactions [21].

In Information systems discipline, privacy concerns has been studied from various perspectives. Scholar in their pursuit to define ideal conditions where privacy exists; they found that identify the root causes of privacy concerns is an essential step to understand privacy as a construct [10]. Thus, majority of studies examine determinates of privacy concerns and have considered the privacy concerns construct as an antecedent to many behavior related variables. For instance, intention to disclose information [22], behavioral intention to use a website [21], location disclosure on a location based social network applications [23]. Thus, in this study, the dependent variable of our research model is the construct of adoption of mobile apps behavior. Moreover, this study utilizes TPB to examine the behaviour and intention to perform behaviour, and CPM to understand determinates of privacy concerns.

Individuals utilize mobiles or smartphones and their embedded applications due to the benefits that they have, however, individuals might refrain from using such technology due to their concerns about violating their privacy by misrepresenting or using their sensitive data [24]. Thus, privacy concerns represents the individual's need for privacy which should directly and negatively influences individual's attitude towards adoption of mobile apps, however, privacy concern is not the only factor that influences attitude, perceived benefits which represents the need for use should be considered also as a second factor however with a positive impact on individual's attitude. Therefore, the following hypotheses are proposed:

Hypothesis 6. Perceived benefits will positively influence user attitude.
Hypothesis 7. Privacy concerns will negatively influence user attitude.

2.2.3. Privacy Boundary Management

Individuals may create diverse threat perceptions about the same personal information which might be accessed by others; thus, the information boundary theory, also known as the communication boundary management theory [25] or the Communication Privacy Management (CPM) theory [26] was developed to understand how persons make decisions regarding disclose their information within interpersonal relationships and to evaluate individuals information access whether it is considered risky or not.

The CPM theory proposes that each person creates a special informational space around him with clearly defined boundaries, and these boundaries influence person decision to determine what information can be shared based on the situational and personal factors. Moreover, any attempt by others to breach these boundaries may be treated as a potential threat. The CPM theory uses such

boundaries to explain the motivation behind revealing or holding information. The situation of boundaries, whether it is open or close, controls the information flow [26]. When it is open, the information flow is open and when it is closed, the information flow is closed. The CPM theory explains factors that influencing individuals decisions regarding the situations of boundaries in dyadic relationships.

The CPM theory was used in many prior studies to understand the information flow in dyadic relationships such as marital, parental and doctor-patient relationships [26]. Thus and due to its success in understanding of information flow in dyadic relationships, many recent studies applied the theory to explain information privacy concerns generated by using various new technologies, for instance online social context [27] and e-commerce [28, 29].

The CPM theory is developed based on human mental decision process which in turn works based on three rules (boundary rule formation, boundary coordination, and turbulence). These rules, according to the CPM theory [26], are responsible to form, determine, and define boundaries around individuals which contain specific cognitive informational spaces and such boundaries determine what information can be shared based on the situational and personal factors. These three rules are discussed further in next section.

2.2.4. Boundary Rule Formation

The CPM theory proposes that individuals' decision process regarding to disclose or withhold their private information based on criteria they perceive [26]. According to boundary rule formation, the CPM theory posits that individuals use certain five criteria to establish privacy rules to manage their boundaries which are: gender, risk-benefit ratio, cultural' expectations, motivations for revealing and concealing, and context of the situation.

For gendered criteria, the CPM theory suggests that males and females have different ways of defining privacy boundaries, thus, men and woman have unalike set of rules for judging how revealing and concealing should be formed [26]. In this study, gender and other demographic variables are included as control variables in the study model. For risk-benefit ratio criteria, the CPM theory suggests that individuals estimate the risk and benefits for giving or rejecting access to privacy boundaries. People may expect more benefits than risks from revealing their private information, they mentally calculate the extent to which disclosure is a positive option and develop and implement rules reflect that choice. This criteria forms the basis for rule making, since that this criteria contributes to individuals' judgments regarding how to manage the balance of privacy concerns and expected benefits from revealing their private information [26].

For cultural' expectations criteria, "people are socialized into certain norms for privacy in their culture and those norms are basic to the way they conceive privacy" [26]. The importance of privacy and privacy concerns regarding revealing certain information are varied from culture to culture, and individuals perceive privacy and define their boundaries in different ways according to their cultural values. Thus, in the CPM theory, cultural values are considered in developing privacy expectations.

Hypothesis 8. Cultural values will influence users' perceived privacy concerns.

For context of the situation criteria, the CPM theory sees context as an issue may influence the way privacy rules are formed and modified [26]. This issue can be categorized based on three live events or situations, ((1) traumatic events, (2) therapeutic situations, and (3) life circumstances), which highlight the way privacy rule establish and are changed to meet the immediate needs of the circumstances. Thus, the privacy implications of specific live events or situations may mean

something different to each person. For example when individuals experience traumatic events, their level of stress is dramatically increased, and there is a one clear way to cope is through disclosure [26]. While, life circumstances category represents situations that may be less stressful than traumatic events such as when people lose their jobs which temporarily influence the way people control their privacy boundaries and their privacy rules are temporarily changed to cope with the demands of this situation [26].

Hypothesis 9. Context of the situation will influence users' perceived privacy concerns.

For motivational criteria, motivations such as the expectations for rewards, attractions, liking or costs are motivating to reveal or conceal private information. Motivational basis for disclosure can be represented by three hypotheses which are (1) expressive need, (2) self-knowledge, and (3) self-defense. Expressive need, reflects the individuals need to express their feelings and thought to others, and self-knowledge is an alternative reason for revealing to others. Whereas self-defense can be seen when some people avoid engaging in self-disclosure due to their feeling that there is a great potential risk might be happened if they engage in such act. In this study, we belief that expressive need, and self-knowledge can impact perceived benefits for giving access to privacy boundaries. Therefore, the study consider examining self-defense as a construct reflects an individual's need to maintain certain boundaries that frame personal space.

Hypothesis 10. Expressive need will influence users' perceived benefits.
Hypothesis 11. Self-knowledge will influence users' perceived benefits.
Hypothesis 12. Self-defense will influence users' perceived privacy concerns.

2.2.5. Boundary Coordination

According to The CPM theory, when people disclose their personal information to other party, a boundary is transformed from a personal to a collective. "The recipient shares in the responsibility of the information. Hence, a personal boundary grows into a collectively managed border" [26] and then the coordination become necessary between both parties: discloser (e.g., costumer) and recipients (e.g., companies). In other words, recipient becomes a custodian who has responsibility for taking care of or protecting discloser personal information, and protection rules will be negotiated among both parties: discloser (e.g., costumer) and recipients (e.g., companies). Privacy policies which represents the agreement or sort of coordination between discloser (e.g., costumer) and recipients (e.g., companies) regarding gathering, using, disclosing, and managing a discloser or customer's data. In the context of this study, privacy policies is used to represent boundary coordination.

Hypothesis 13. Perceived effectiveness of privacy policy will negatively influence users' perceived privacy concerns.

2.2.6. Boundary Turbulence

Sometimes the boundary coordination process fails due to its complexity [26]. Boundary management may become turbulent, when the boundary coordination mechanism does not work well or when individuals private information are attacked from external parties. "Boundaries become turbulent when individuals are put into binds where the solutions are problematic" [26]. Therefore, individuals must therefore determine ways such as determine mechanism to manage the turbulent or the allowing other party to solve this turbulent with the least amount of negative outcome for all parties involved. Companies, to ensuring consumer confidence, relies on self-regulation to address various industry issues, including creating industry standards, developing and

applying codes of professional ethics. Thus, in this study industry self-regulation is used to represent boundary turbulence.

Hypothesis14. Perceived effectiveness of industry self-regulation will negatively influence users' perceived privacy concerns.

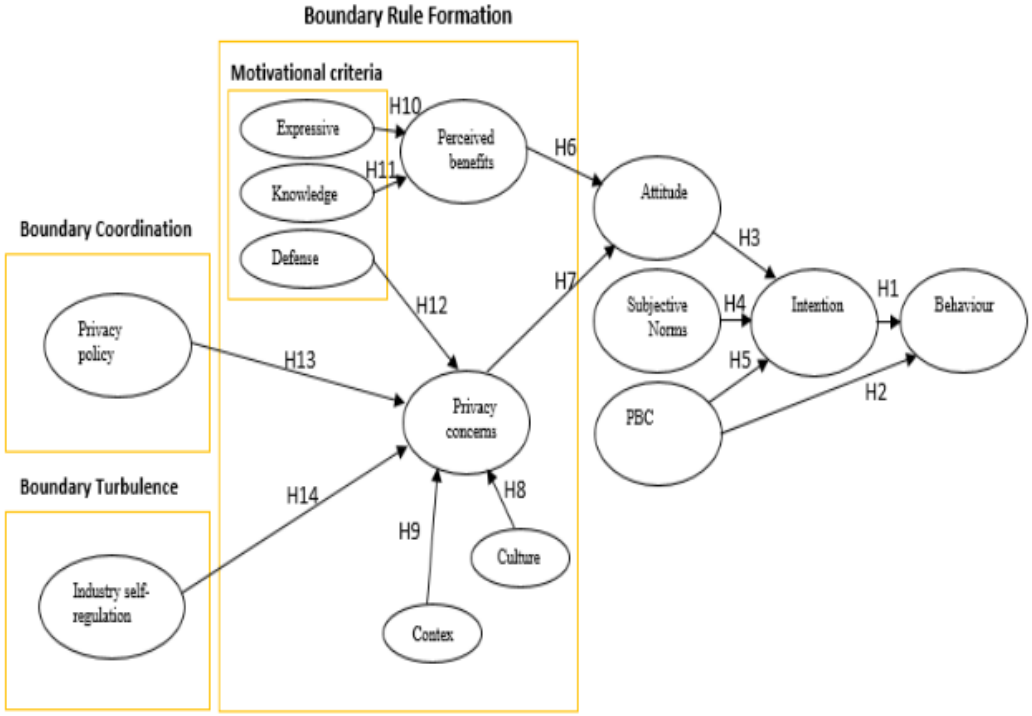

Figure 4. The study model.

3. METHODOLOGY

3.1. Measurement

Determining the constructs that will measured, and then select right measuring methods to measure those constructs is necessary and has an important influence on the accuracy of findings [30]. In order to test the study's hypotheses, the survey instrument has been developed. The items used in the survey instrument to measure the constructs were identified and adopted from prior research; particularly from the Communication field and IS research, in order to guarantee the validity of the face (content) of the scale used, we used the items which were broadly utilized in the most prior relevant studies which represent a sort of subjective agreement between scholars. In the majority of prior study, these measuring instruments logically appear to reflect accurate measure of the constructs of interest. Table 1 contains the items developed for each construct in this study along with a set of prior studies where these items have been adopted from.

Table 1: List of items by construct

Construct	Items	Adapted from
Usage (US)	US1. On average, each week I use my mobile applications often. US2. For each log session, I use my mobile applications site long. US3. On my mobile applications, I often post something. US4. On my mobile applications, I often view something. US5. On my mobile applications, I often share something. US6. On my mobile applications, I often reply to others.	[24, 31]
Behavioural intention (BI)	BI1. I intend to use mobile applications in next three months. BI2. I expect my use of the mobile applications to continue in the future.	[32, 33, 34].
Subjective Norm (SN)	SN1. My friends would think that I should use mobile applications. SN2. My colleagues/classmates would think that I should use mobile applications. SN3. People who are important to me would think that I should mobile applications.	[32, 34].
Attitude (AT)	AT1. I have positive opinion in mobile applications. AT2. I think usage of mobile applications is good for me AT3. I think usage of mobile applications is appropriate for me	[16, 34].
Perceived behavioural control (BC)	BC1. Using mobile applications is entirely within my control BC2. Whether or not I use mobile applications is entirely up to me	[32, 34].
Perceived benefits (PB)	PB1. Mobile applications is more convenient than other traditional social networks options PB2. Mobile applications makes it easier to find information and people. PB3. Mobile applications improves my information and people seeking PB4. Mobile applications help me to find information more quickly PB5. I think that mobile applications is useful. Overall, I think that using the mobile applications is advantageous.	[32, 33].
Perceived privacy concerns (PC)	PC1. I am concerned that I could be identified by the company when using the application for [the focal activity] PC2. I am concerned with how information about me may be exploited by the company when using the application for [the focal activity] PC3. I am concerned with how the information captured during my use of the application to perform [the focal activity] can be employed by the company to identify me as an individual PC4. It bothers me when my personal information is gathered when I use the application for [the focal activity] PC5. I am concerned that my personal information gathered during my use of the application for [the focal activity] may be accessed by unauthorized people PC6. I am concerned that my personal information that is captured when I use the application for [the focal activity] may be kept in a non-accurate manner PC7. To what extent are you concerned that your privacy will be compromised when using the application for the specific activity?	[35, 2].
Cultural values (CV)	CV1. Your cultural values prevent you from sharing your' personal photos stored in your mobile phone to anyone. CV2. Your cultural values prevent you from sharing your' family photos stored in your mobile phone to anyone. CV3. Your cultural values prevent you from sharing your' private information to anyone. CV4. Your cultural values prevent you from sharing your' secretes to anyone.	Self-developed
Context of the situation (CS)	CS1. Your situation prevent you from sharing your' personal photos stored in your mobile phone to anyone. CS2. Your situation prevent you from sharing your' family photos stored in your mobile phone to anyone. CS3. Your situation prevent you from sharing your' private information to anyone. CS4. Your situation prevent you from sharing your' secretes to anyone.	Self-developed
Expressive need (EN)	EN1. You use some of mobile applications to express your feelings and thoughts to others. EN2. Mobile applications let you express your feelings and thoughts to others.	Self-developed
Self-knowledge (SK)	SK1. You use some of mobile applications to increase your knowledge. SK2. Mobile applications let you increase your knowledge.	Self-developed

Construct	Items	Adapted from
Self-defense (SD)	SD1. When you use some of mobile applications you avoid engaging in self-disclosure due to your feeling that there is a great potential risk might be happened if you engage in such act. SD2. Using some of mobile applications may cause self-disclosure.	Self-developed
Perceived effectiveness of privacy policy (PP)	PP1. I feel confident that these mobile applications' privacy statements reflect their commitments to protect my personal information. PP2. 2. With their privacy statements, I believe that my personal information will be kept private and confidential by these mobile applications. PP3. 3. I believe that these mobile applications' privacy statements are an effective way to demonstrate their commitments to privacy.	[31]
Perceived effectiveness of industry self-regulation (SR)	SR1. I believe that privacy seal of approval programs such as TRUSTe will impose sanctions for mobile applications' companies' noncompliance with its privacy policy. SR2. Privacy seal of approval programs such as TRUSTe will stand by me if my personal information is misused during and after transactions with mobile applications' companies. SR3. I am confident that privacy seal of approval programs such as TRUSTe is able to address violation of the information I provided to mobile applications' companies.	[31]

3.2. Data Collection Procedures

Data for this study were collected in four stages (3 months apart), from samples stratified into gender groups by means of a survey conducted in Saudi Arabia in 2013. This type of sampling method has been chosen due to the difficulty of drawing an actual representative sample in Saudi Arabia. Majority of houses in Saudi Arabia have no mail boxes and the postal services are not presented for every house. Moreover, due to the conservative nature of Saudi Arabian society, it is hard to approach women in Saudi Arabia. Therefore, stratified samples were drawn from numerous areas in the country and female relatives were engaged to distribute questionnaires to the female strata besides using electronic means to guarantee reaching females as well as males. The survey questionnaires were distributed to 2500 participants (1250 male and 1250 female). A total of 832 responses were received from male participants and 717 from female participants. After checking the data for validity, 1523 were deemed fit for use in the analysis.

4. DATA ANALYSIS AND RESULTS

4.1. Reliability and validity

Data, obtained from the pilot study of each construct in the instrument, have been used to test a reliability and internal consistency. The results shows that the alpha values ranged from .902 to .988 with an overall alpha value of .924. Table 2 shows the Cronbach's alpha reliability of constructs in the study. The result indicated that all constructs of the model were reliable. As a result, the internal consistency of the instrument was adequate.

Table 2 Cronbach's Alpha Reliability of Constructs in the Study

Construct	Number of Items	Cronbach's Alpha
Usage (US)	6	.982
Behavioural intention (BI)	2	.988
Subjective Norm (SN)	3	.970
Attitude (AT)	3	.961
Perceived behavioural control (BC)	2	.902
Perceived benefits (PB)	5	.982
Perceived privacy concerns (PC)	7	.974
Cultural values (CV)	4	.968

Construct	Number of Items	Cronbach's Alpha
Context of the situation (CS)	4	.953
Expressive need (EN)	2	.955
Self-knowledge (SK)	2	.962
Self-defense (SD)	2	.983
Perceived effectiveness of privacy policy (PP)	3	.988
Perceived effectiveness of industry self-regulation (SR)	3	.986
Overall alpha value	48	.924

Principal component factor analysis and the Kaiser–Meyer–Olkin (KMO) were used to investigate the adequacy of the study sample and the validity of the study instrument. As the value of KMO was 0.786 as in Table3, the study sample was considered adequate and the appropriateness of using principal component factor analysis on the collected data was assured.

Table 3. KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.786
Bartlett's Test of Sphericity	Approx. Chi-Square	30588.571
	df	91
	Sig.	.000

Construct validity was evaluated by using factor analysis to measure a principal components analysis with a Varimax rotation. This analysis helped in assessing the convergent and discriminant validity of items. The convergent validity was evaluated by examining whether items of a variable converged together on a single construct [36], and whether the factor loading for every item was > 0.45, as suggested by Comrey and Lee [37]. Comrey and Lee [37] indicated that loadings greater than 0.45 could be considered fair, while loadings greater than 0.55 might be considered good, and 0.63 could be considered as a very good, and those of 0.71 as excellent. The discriminant validity was assessed by using the cross loading of items on various factors. As the factor pattern shows in Table 4, loadings on the target factor are in the excellent range (36 out of 48), very good (7 out of 48), and good (5 out of 48). As illustrated in Table 4, no weak loading was discovered demonstrating the validity of constructs adopted in this study.

Table 4. Factor Analysis of Items Sorted by Construct (Rotated Component Matrix (a))

	Component					
	1	2	3	4	5	**Its assessment**
SR1	.367	**.863**	-.144	.076	.057	*Excellent > 0.71*
SR2	.276	**.895**	-.177	.130	.122	*Excellent > 0.71*
SR3	.270	**.889**	-.163	.140	.155	*Excellent > 0.71*
PP1	.283	**.897**	-.171	.034	.182	*Excellent > 0.71*
PP2	.288	**.911**	-.167	.032	.073	*Excellent > 0.71*
PP3	.283	**.885**	-.184	.028	.138	*Excellent > 0.71*
SD1	-.289	-.207	.232	-.295	**.799**	*Excellent > 0.71*
SD2	-.215	-.254	.171	-.358	**.807**	*Excellent > 0.71*
SK1	**.764**	.282	-.128	-.018	.490	*Excellent > 0.71*
SK2	**.750**	.249	-.138	.108	.417	*Excellent > 0.71*
EN1	**.736**	.387	-.257	.385	.072	*Excellent > 0.71*

	Component					
	1	2	3	4	5	**Its assessment**
EN2	**.609**	.556	-.262	.286	.012	*Good > 0.55*
CS1	-.344	.001	.201	**.843**	-.125	*Excellent > 0.71*
CS2	-.220	-.121	.112	**.895**	-.077	*Excellent > 0.71*
CS3	-.207	-.229	.045	**.875**	-.128	*Excellent > 0.71*
CS4	-.210	-.203	.103	**.845**	-.178	*Excellent > 0.71*
CV1	-.239	-.067	**.896**	-.065	.147	*Excellent > 0.71*
CV2	-.276	-.073	**.903**	-.068	.056	*Excellent > 0.71*
CV3	-.264	-.187	**.832**	-.140	.062	*Excellent > 0.71*
CV4	-.208	-.159	**.844**	-.068	.140	*Excellent > 0.71*
PC1	-.112	-.131	**.935**	.065	-.056	*Excellent > 0.71*
PC2	-.148	-.102	**.907**	-.132	-.147	*Excellent > 0.71*
PC3	.088	-.221	**.895**	-.011	-.160	*Excellent > 0.71*
PC4	-.007	-.204	**.911**	-.020	-.149	*Excellent > 0.71*
PC5	-.007	-.029	**.880**	-.040	-.167	*Excellent > 0.71*
PC6	-.108	-.100	**.878**	-.198	-.177	*Excellent > 0.71*
PC7	-.198	-.148	**.835**	-.213	-.143	*Excellent > 0.71*
PB1	.543	**.584**	-.234	.355	.041	*Good > 0.55*
PB2	**.650**	.550	-.248	.234	.084	*Very good > 0.63*
PB3	**.620**	.531	-.293	.340	.162	*Very good > 0.63*
PB4	**.677**	.434	-.122	.452	.176	*Very good > 0.63*
PB5	**.598**	.553	-.192	.316	.191	*Good > 0.55*
AT1	**.677**	.539	-.132	.240	.125	*Very good > 0.63*
AT2	**.640**	.458	-.162	.514	.046	*Very good > 0.63*
AT3	**.595**	.553	-.119	.409	.050	*Good > 0.55*
SN1	**.899**	.161	-.079	.088	-.074	*Excellent > 0.71*
SN2	**.902**	.248	-.102	.137	.061	*Excellent > 0.71*
SN3	**.878**	.194	-.153	.169	.053	*Excellent > 0.71*
BC1	**.803**	.049	-.164	.048	.216	*Excellent > 0.71*
BC2	**.801**	.236	-.177	.021	.322	*Excellent > 0.71*
BI1	**.772**	.485	-.146	.306	-.014	*Excellent > 0.71*
BI2	**.721**	.565	-.163	.297	.091	*Excellent > 0.71*
US1	**.735**	.527	-.135	.281	-.088	*Excellent > 0.71*
US2	.613	**.663**	-.159	.317	.051	*Very good > 0.63*
US3	**.679**	.568	-.139	.283	-.033	*Very good > 0.63*
US4	**.594**	.576	-.049	.268	-.051	*Good > 0.55*
US5	**.740**	.522	-.108	.239	-.003	*Excellent > 0.71*
US6	**.714**	.539	-.137	.300	-.006	*Excellent > 0.71*

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
a Rotation converged in 9 iterations.

4.2. Hypotheses testing

This study proposes an integrated theoretical model brings together concepts from the Theory of Planned Behaviour (TPB) and Communication Privacy Management (CPM) theory. This model is applied to determine significant factors that influence adoption of mobile apps in Saudi Arabia.

This model can be constituted through the examination of 14 hypotheses. The relationship between factors as independent variables and adoption behavior is identified by these hypotheses. Each accepted hypothesis shows an interpretation of adoption's behaviour as dependent variables. Explanations are nomothetic and advance via deductive reasoning. The correlation analysis amongst all the study variables was conducted using Pearson's correlation analysis as illustrated in Table 5. As variables represented significant relationships ($p \leq 0.01$), the study then used the regression model to inspect multicollinearity by testing collinearity statistics; i.e. Variance Inflation Factor (VIF) and tolerance.

Table 5. Correlation analysis amongst the variables.

	US	BI	BC	SN	AT	PB	PC	CV	CS	EN	SK	SD	PP
BI	.923*												
B C	.681*	.759*											
S N	.800*	.854*	.777*										
A T	.916*	.887*	.751*	.715*									
P B	.850*	.907*	.634*	.773*	.844*								
P C	-.280*	-.348*	-.327*	-.225*	-.283*	-.368*							
C V	-.351*	-.404*	-.366*	-.330*	-.327*	-.402*	.869*						
C S	-.532*	-.647*	-.411*	-.477*	-.596*	-.603*	.280*	.245*					
E N	.891*	.930*	.705*	.813*	.831*	.906*	-.369*	-.426*	-.631*				
S K	.644*	.738*	.802*	.789*	.705*	.619*	-.245*	-.245*	-.404*	.676*			
S D	-.418*	-.498*	-.548*	-.399*	-.540*	-.490*	-.430*	-.240*	-.514*	-.502*	-.617*		
PP	.712*	.732*	.444*	.469*	.737*	.759*	-.334*	-.303*	-.334*	.669*	.582*	-.429*	
S R	.764*	.726*	.501*	.436*	.834*	.710*	-.322*	-.320*	-.356*	.631*	.478*	-.439*	-.829*

US: Usage, BI: Behavioural intention, BC: Perceived behavioural control, SN: Subjective Norm, AT: Attitude, PB: Perceived benefits, PC: Perceived privacy concerns, CV: Cultural values, CS: Context of the situation, EN: Expressive need, SK: Self-knowledge, SD: Self-defense, PP: Perceived effectiveness of privacy policy, SR: Perceived effectiveness of industry self-regulation.
* $p \leq 0.01$

To determine whether any multicollinearity effects existed, we checked whether there was any warning message produced by the AMOS output that signalled a problem of multicollinearity. The findings showed that there was no evidence of multicollinearity. The potential issue of multicollinearity can be further studied formally in the context of regression analysis.

In Table 6, the tolerance values ranged from 0.875 to 0.302. One way to measure collinearity is with variance inflation factors (VIF). The (VIF) is generally recommended to be less than or equal to 10 (i.e. tolerance >0.1) [38, 39]. In this study, a variance inflation factor (VIF) greater than 4 is considered to indicate a serious problem of multicollinearity. However, as shown in Table 3, there were no VIF values over 4 in the model; since the VIFs values ranged from 1.143 to 3.313. Thus there was no evidence of multicollinearity.

Table 6. Multicollinearity test

Dependent variable	Path direction	Independent variables (predictors)	Collinearity Statistics	
			Tolerance	VIF
Usage	←	Intention	.424	2.357
Usage	←	Perceived behavioural control	.424	2.357
Intention	←	Attitude	.392	2.551
Intention	←	Subjective Norm	.357	2.802
Intention	←	Perceived behavioural control	.318	3.143
Attitude	←	Perceived benefits	.865	1.157
Attitude	←	Perceived privacy concerns	.865	1.157
Perceived privacy concerns	←	Cultural values	.875	1.143
Perceived privacy concerns	←	Context of the situation	.850	1.176
Perceived privacy concerns	←	Perceived effectiveness of privacy policy (PP)	.310	3.229
Perceived privacy concerns	←	Perceived effectiveness of industry self-regulation (SR)	.302	3.313
Perceived benefits	←	Expressive need	.531	1.883
Perceived benefits	←	Self-knowledge	.439	2.276
Perceived benefits	←	Self-defense	.606	1.650

After assuring that necessary requirements are all adequately met, multiple regression analysis was used to evaluate the study hypotheses.

First, "Intention" and "Perceived behavioural control" were regressed on "Usage". As in Fig. 5, it was found that "Intention" ($\beta = 0.958$, Standardized path coefficient, $p < 0.05$), and "Perceived behavioural control" ($\beta = 0.046$, Standardized path coefficient, $p < 0.05$) are significantly and positively related to "Usage" (adjusted $R^2=0.85$) (see Table 7, Table 8 and Fig. 5). Thus, H1 and H2 are supported.

Table 7. Coefficients for Proposed model

Dependent variable	Path direction	Independent variables (predictors)	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
			B	Std. Error	Beta		
Usage	←	Intention	.893	.014	.958	63.395	.000
Usage	←	Perceived behavioural control	.055	.018	.046	3.076	.002
Intention	←	Attitude	.555	.013	.585	42.432	.000

Dependent variable	Path direction	Independent variables (predictors)	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
			B	Std. Error	Beta		
Intention	←	Subjective Norm	.595	.018	.474	32.787	.000
Intention	←	Perceived behavioural control	.062	.019	.049	3.175	.002
Attitude	←	Perceived benefits	1.042	.018	.856	57.937	.000
Attitude	←	Perceived privacy concerns	-.036	.017	-.032	-2.159	.031
Perceived privacy concerns	←	Cultural values	.977	.016	.840	62.934	.000
Perceived privacy concerns	←	Context of the situation	.077	.018	.058	4.288	.000
Perceived privacy concerns	←	Perceived effectiveness of privacy policy	-.159	.033	-.107	-4.763	.000
Perceived privacy concerns	←	Perceived effectiveness of industry self-regulation	-.126	.026	-.098	-4.811	.000
Perceived benefits	←	Expressive need	.873	.014	.899	61.068	.000
Perceived benefits	←	Self-knowledge	.011	.014	.011	.772	.440
Perceived privacy concerns	←	Self-defense	.382	.019	.271	19.623	.000

P values less than 0.05 were considered statistically significant

Table 8. Standardized Regression Weights

Criterion variable	Path direction	Criterion variable predictors	Estimate	(Significance)
Usage	←	Intention	.958	Significant
Usage	←	Perceived behavioural control	.046	Significant
Intention	←	Attitude	.585	Significant
Intention	←	Subjective Norm	.474	Significant
Intention	←	Perceived behavioural control	.049	Significant
Attitude	←	Perceived benefits	.856	Significant
Attitude	←	Perceived privacy concerns	-.032	Significant
Perceived privacy concerns	←	Cultural values	.827	Significant
Perceived privacy concerns	←	Context of the situation	.058	Significant

Criterion variable	Path direction	Criterion variable predictors	Estimate	(Significance)
Perceived privacy concerns	←	Perceived effectiveness of privacy policy	-.107	Significant
Perceived privacy concerns	←	Perceived effectiveness of industry self-regulation	-.098	Significant
Perceived benefits	←	Expressive need	.899	Significant
Perceived benefits	←	Self-knowledge	.011	Insignificant
Perceived privacy concerns	←	Self-defense	.271	Significant

Thereafter, the three independent variables (i.e. "Attitude", "Subjective norms" and "Perceived behavioural control") were regressed on "Behavioral Intention". Results, as in Fig. 5, indicate that all three variables are significantly and positively related to "Behavioral Intention" (adjusted R^2=0.89): "Attitude" ($\beta = 0.585$, Standardized path coefficient, $p < 0.05$), "Subjective norms" ($\beta = 0.474$, Standardized path coefficient, $p < 0.05$) and "Perceived behavioural control" ($\beta = 0.049$, Standardized path coefficient, $p < 0.05$) (see Table 7, Table 8 and Fig. 5). Thus, H3, H4 and H5 are supported.

"Perceived benefits" and "Perceived privacy concerns" were regressed on "Attitude". As in Fig. 5, it was found that "Perceived benefits" ($\beta = 0.856$, Standardized path coefficient, $p < 0.05$), and "Perceived privacy concerns" ($\beta = 0.032$, Standardized path coefficient, $p < 0.05$) are significantly and positively related to "Attitude" (adjusted R^2=0.71) (see Table 7, Table 8 and Fig. 5). Thus, H6 and H7 are supported.

Then, the five independent variables: (1) Self-defense, (2) Perceived effectiveness of industry self-regulation, (3) Cultural values, (4) Perceived effectiveness of privacy policy and (5) Context of the situation were regressed on "Perceived privacy concerns". Results, as in Fig. 5, indicate that all five variables are significantly and positively related to "Perceived privacy concerns" (adjusted R^2=0.81): "Cultural values" ($\beta = 0.827$, Standardized path coefficient, $p < 0.05$), "Context of the situation" ($\beta = 0.058$, Standardized path coefficient, $p < 0.05$), "Self-defense" ($\beta = 0.271$, Standardized path coefficient, $p < 0.05$), "Perceived effectiveness of privacy policy" ($\beta = -0.107$, Standardized path coefficient, $p < 0.05$) and "Perceived effectiveness of industry self-regulation" ($\beta = -0.098$, Standardized path coefficient, $p < 0.05$) (see Table 7, Table 8 and Fig. 5). Thus, H8, H9, H12, H13 and H14 are supported.

Finally, the two antecedents of "Perceived benefits" construct were tested using multiple regression analysis which showed that "Expressive need" ($\beta = 0.899$, Standardized path coefficient, $p < 0.05$) has a significant and positive effect on "Perceived benefits" (adjusted R^2=0.821) (see Table 7, Table 8 and Fig. 5). Thus, H10 is supported. Whereas, "Self-knowledge" ($\beta = 0.011$, Standardized path coefficient, $p < 0.05$) has no effect on "Perceived benefits", Therefore, H11 is not supported.

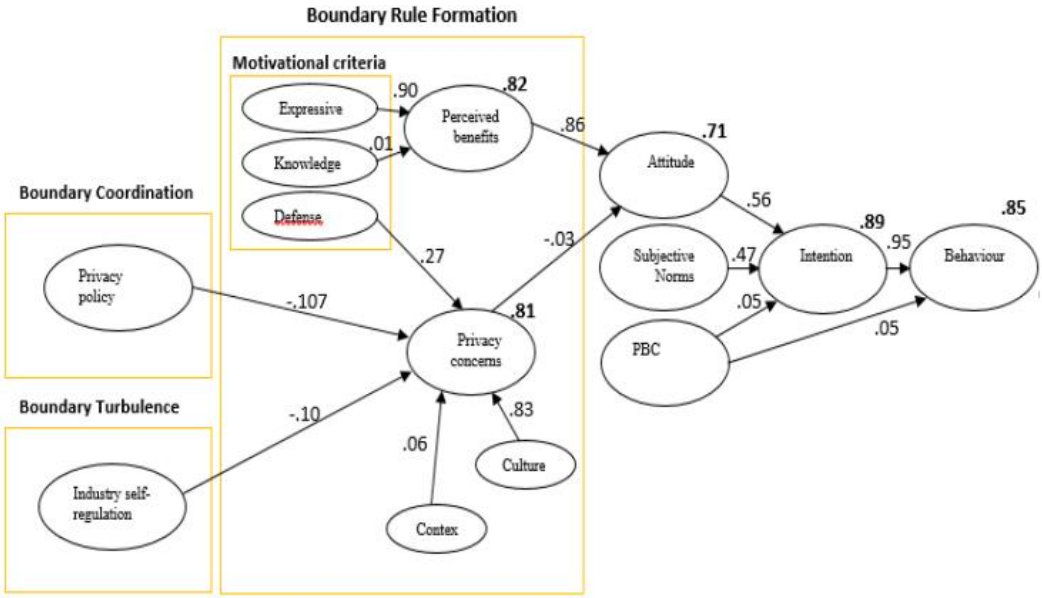

Figure 5. The study model.

5. DISCUSSION

The results of this study are practically and theoretically relevant and showing an accurate and deep understanding of factors that might lessening level of mobile apps usage. In the context of mobile apps usage, there is no detailed theoretical model to describe individuals' attitudes and their two main antecedents (privacy concerns and perceived benefits) toward using apps on mobile. This study develops a new model to identify the root causes of privacy concerns and perceived benefits through using theoretical framework brings together concepts from the Theory of Planned Behaviour (TPB) and Communication Privacy Management (CPM) theory.

The study proposed model includes three major parts; the first part identifies the root causes of privacy concerns and perceived benefits based on our understanding and interpretation for information boundary theory and Communication Privacy Management (CPM) theory, the second part explores attitude towards using mobile apps and influences of its two main antecedents (privacy concerns and perceived benefits) toward using apps on mobile. The third part addresses the usage behavior and behavioral intention toward using mobile apps.

For the first part, “Cultural values”, “Context of the situation”, “Self-defense”, “Perceived effectiveness of privacy policy” and “Perceived effectiveness of industry self-regulation” are the antecedents of individuals “Perceived privacy concerns” towards using apps on mobile, which explain the 81% of the “Perceived privacy concerns” variance. Whereas, “Expressive need” and “Self-knowledge” are able to explain the 82% of individuals “Perceived benefits”. All of the hypotheses relating to “Perceived privacy concerns” are endorsed. Whereas, from the two antecedents of “Perceived benefits” construct (i.e. “Expressive need”, and “Self-knowledge”) “Expressive need” ($\beta = 0.899$, Standardized path coefficient, $p < 0.05$) only has a significant and positive effect on “Perceived benefits”.

In his research, Waleed Al-ghaith developed an equation to quantify the contribution of each model's variable or factor to the explanatory power of the model [11].

$$A_x = \frac{{\beta_x}^2}{\sum_{k=1}^{n} {\beta_x}^2} \times {R_{PC}}^2$$

Where:

A_x = Participation of variable A_x in a model' explanatory power

${\beta_x}^2$ = Square of beta coefficients or standardized coefficients of variable

${\mathrm{R_{PC}}}^2$ = Model' explanatory power (perceived privacy concerns)

$\sum_{k=1}^{n} {\beta_x}^2$ = Total of causal effects for the model's constructs

This equation has been adopted in this study to calculate the participation of each constructs and their antecedents in the model's explanatory power and to calculate rate of participation of every antecedents in their constructs' explanatory power. The equation has been applied on the antecedents of the "Perceived privacy concerns", the results have been summarised in Table 9. The result shows that "Cultural values" alone explains 70% of "Perceived privacy concerns" followed by "Self-defense" which explains around 23% of "Perceived privacy concerns", and then "Context of the situation" with 5%. Whereas, the findings show that "Perceived effectiveness of privacy policy" and "Perceived effectiveness of industry self-regulation" both are factors which have the ability to reduce individuals "Perceived privacy concerns" by 9% and 8% respectively.

Table 9. Participation of Perceived privacy concerns 's variables in its explanatory power

Antecedents	**Perceived privacy concerns**
Cultural values	70%
Self-defense	23%
Context of the situation	5%
Perceived effectiveness of privacy policy	-9%
Perceived effectiveness of industry self-regulation	-8%
Total	81%

The study findings show that, in Saudi Arabia, "Cultural values" alone explains 70% of individuals "Perceived privacy concerns". The conservative nature of Saudi Arabian society which take its values from the Islamic religion rules, Arab traditions and tribal norms formed the Saudi culture [40]. In such culture, conservative values are the basis for judging levels of disclosure or privacy, thus, people tend to protect their information boundaries motivated by their concerns of shame or scandal. For instance in Saudi Arabia women are not welcomed to be highly observable and audible for anyone. As this example shows, for the Saudi culture, the conservative nature of Saudi Arabian society maintains the boundaries around sharing personal photos and private information and abides by rules set by the Islamic religion, Arab traditions and tribal norms that are influenced by the cultural norms for privacy. "Obviously, reducing exposure means more privacy and more boundary control" [26].

The study findings also show that, in Saudi Arabia, "Self-defense" explains around 23% of "Perceived privacy concerns". Self-defense is a function or motivator for keeping information private [26]. Self-defense can be seen when some people avoid engaging in self-disclosure due to their feeling that there is a great potential risk might be happened if they engage in such act. People may not want to reveal their personal information due to their belief that there is a great risk may

cause loss of face, relation, or role. Loss of face can be seen when disclose personal photos or private information leads to sort of embarrassment to individuals or to their relative or friends which also may pose a threat to the relationships. Due to face risks people in Saudi Arabia are more likely to anticipate the need for a defense if private information becomes public.

The results also show that "Perceived effectiveness of privacy policy" and "Perceived effectiveness of industry self-regulation" both are factors which have the ability to reduce individuals "Perceived privacy concerns" by 9% and 8% respectively. This show how Saudi individuals perceive the global regulations as a custodian who has responsibility for taking care of or protecting discloser personal information.

For the second part, "Perceived benefits" and "Perceived privacy concerns" are the antecedents of individuals "Attitude" towards using mobile apps, which explain the 71% of the variance. All of the hypotheses regarding "Attitude" are supported.

The Al-ghaith's equation [11] has been used again to calculate the participation of the antecedents of the "Attitude" on its explanatory power, the results have been summarized in Table 10. The result shows that "Perceived benefits" alone explains 73.75% of individuals "Attitude" towards using mobile apps, whereas, the findings show that "Perceived privacy concerns" reduce individuals "Attitude" by 2.75%.

Table 10: Participation of Attitude 's variables in its explanatory power

Antecedents	**Attitude**
Perceived benefits	73.75%
Perceived privacy concerns	-2.75%
Total	71%

The results show that Saudi people attitude toward using mobile apps is determined by perceived benefits and perceived privacy concerns, whereas the relative strengths of one of the two beliefs in a given context determine the individual's overall attitude within that context. The condition of very strong attitude toward using mobile apps is characterized by strength of perceived benefits and low perceived privacy concerns. Benefits of mobile apps such as convenience, accessibility, interactivity, socialization, expressive need, self-knowledge and personalized service are highly perceived by Saudi people rather than any risks might be occurred as a result of use of mobile apps such as privacy issues. As a result, number of mobile subscribers in 2013 reached 53 million, reflecting 181.6 percent of population diffusion rate [41].

For the third part, "Attitude", "Subjective norms" and "Perceived behavioural control" are the antecedents of individuals "Behavioral Intention" towards using apps on mobile, which explain the 89% of the variance. Whereas, "Behavioral Intention" with its antecedents and "Perceived behavioral control" are able to explain the 85% of the of individuals "Usage" behavior. All of the hypotheses regarding "Behavioral Intention" and individuals "Usage" behavior are supported.

The Al-ghaith's equation [11] has been used again to calculate the participation of the antecedents of the "Behavioral Intention" on its explanatory power, the results have been summarized in Table 11. The result shows that "Attitude" alone explains 74% of individuals "Behavioral Intention" towards using mobile apps, followed by "Subjective norms" which explains around 38% of "Behavioral Intention", and then "Perceived behavioural control" with 4%.

Table 11: Participation of Behavioral Intention 's variables in its explanatory power

Antecedents	Behavioral Intention
Attitude	47%
Subjective norms	38%
Perceived behavioural control	4%
Total	89%

6. IMPLICATIONS FOR THEORY AND PRACTICE

6.1. Implications for theory and research

The current research utilizes TPB model to examine the behaviour and intenion to berform behaviour, and CPM theory to understand determinates of privacy concerns. This study contributes to the body of the information systems literature by exploring the behavioural and social factors affecting users' decisions to adopt mobile apps as new technology. Importantly, the study shows that privacy concern is not the only factor that influences negatively on attitude, perceived benefits which represents the need for use should be considered also as a second factor however with a positive impact on individual's attitude.

Theoretically, drawing on CPM theory, this research is important because it developed a research model suggesting that "Cultural values", "Context of the situation", "Self-defense", "Perceived effectiveness of privacy policy" and "Perceived effectiveness of industry self-regulation" are the antecedents of individuals "Perceived privacy concerns" towards using apps on mobile, which explain the 81% of the "Perceived privacy concerns" variance. Whereas, "Expressive need" and "Self-knowledge" are able to explain the 82% of individuals "Perceived benefits".

6.2. Implications for Practice

For mobile apps developers who face growing pressure to determine information privacy issues [2], this research offers practical recommendations on developing mobile apps. Mobile apps can be personalized through asking individuals to provide their favorites rather than gathering their personal information.

This study also suggests the need to invent a new operating systems and mobile hardware which ensure strong protection of individuals' information and prevent unauthorized access to the users' information. Moreover, the new operating systems and mobile hardware must also prevent mobile apps from accessing to the users' information.

REFERENCES

[1] CISCO. (2020). Cisco Annual Internet Report (2018–2023). Retrieved from CISCO Website https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf.

[2] Sutanto, J., Palme, E., Chuan-Hoo, T., & Chee Wei, P. (2013). ADDRESSING THE PERSONALIZATION-PRIVACY PARADOX: AN EMPIRICAL ASSESSMENT FROM A FIELD EXPERIMENT ON SMARTPHONE USERS. MIS Quarterly, 37(4), 1141-A5.

[3] Angwin, J., & Valentino-DeVries, J. (2011, April 22). Apple, Google Collect User Data. The Wall Street Journal, U.S. Edition. Retrieved from http://www.wsj.com/articles/SB10001424052748703983704576277101723453610

[4] Hutchinson, R. (2011, January 26). 50 Percent of iPhone Apps Can Track User Data. Applie News. Retrieved from http://www.geeky-gadgets.com/50-percent-of-iphone-apps-can-track-user-data-26-01-2011/

[5] Federal Trade Commission. (2015). Internet of things: Privacy & Security in a Connected World. Preliminary FTC Staff Report. Retrieved from Federal Trade Commission Website: (https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf).
[6] Banisar, D. (2014, December 8). National Comprehensive Data Protection/Privacy Laws and Bills 2014 Map. Retrieved from SSRN Website: http://ssrn.com/abstract=1951416
[7] Conger, S., Pratt, J. H. & Loch, K. D. (2013). Personal information privacy and emerging technologies. Info Systems J, 23, 401–417.
[8] DLA Piper. (2015). DLA Piper's Data Protection Laws of the World Handbook. Retrieved from DLA Piper Website: http://dlapiperdataprotection.com/#handbook/world-map-section
[9] Arab Social Media Report. (2014). Citizen Engagement and Public Services in the Arab World: The Potential of Social Media. Mohammed bin Rashid School of government, 1(6). Retrieved from Arab Social Media Report Website: http://www.arabsocialmediareport.com/
[10] Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. Journal of Public Policy and Marketing, 19(1), 27-41.
[11] Al-ghaith, W. (2015). Understanding Social Network Usage: impact of co-presence, intimacy, and immediacy. International Journal of Advanced Computer Science and Applications (IJACSA), 6(8), 99-111.
[12] RFID World Canada. (2015). Billion Dollar Mobile Payment Industry Using Secure NFC Technology Projected to Continue Strong Growth. Retrieved from RFID World Canada Website: http://www.rfidworld.ca/billion-dollar-mobile-payment-industry-using-secure-nfc-technology-projected-to-continue-strong-growth/2418
[13] Giorgia, G., Teunissena, P., Verhagena, S. & Buista, P. (2010). GNSS remote sensing: testing a new multivariate GNSS carrier phase attitude determination method for remote sensing platforms. Advances in Space Research, 46, 118–129.
[14] Daniel, O. (2007). Security and privacy on the semantic web. In Milan Petkovic and Willem Jonker, editors, Security, Privacy and Trust in Modern Data Management, Data-Centric Systems and Applications. Berlin Heidelberg: Springer.
[15] Ajzen, I., & Fishbein, M. (1980). Understanding Attitudes and Predicting Social Behaviour. Englewood Cliffs, NJ: Prentice-Hall.
[16] Ajzen, I. (1991). The theory of planned behaviour. Organizational Behaviour and Human Decision Processes, 50(2), 179-211.
[17] Pavlou, P. & Fygenson, M. (2006). Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior. MIS Quarterly, 30(1), 115-143.
[18] Hernandez M., & Mazzon J. (2007). Adoption of internet banking: proposition and implementation of an integrated methodology approach. The International Journal of Bank Marketing, 25(2), 72-88.
[19] Marler, Janet H., Fisher, Sandra L., & Ke, Weiling. (2009). employee self-service technology acceptance: a comparison of pre-implementation and post-implementation relationships. Personnel Psychology, 62(2), 327-358.
[20] Warren, S., & Brandeis, L. (1890). The Right to Privacy. Harvard Law Review. IV (5).
[21] Li, Y. (2014). The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. Decision Support Systems, 57(1), 343–354.
[22] Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. The Journal of Computer Information Systems, 62–71.
[23] Koohikamali, M., Gerhart, N. & Mousavizadeh, M. (2015). Location disclosure on LB-SNAs: The role of incentives on sharing behavior. Decision Support Systems, 71(1), 78–87.
[24] Alghaith, W., Sanzogni, L., & Sandhu, K. (2010). Factors Influencing the Adoption and Usage of Online Services in Saudi Arabia. Electronic Journal of Information Systems in Developing Countries (EJISDC), 40(1), 1-32.
[25] Petronio, S. (1991). Communication boundary management: a theoretical model of managing disclosure of private information between marital couples. Communication Theory, 311-335.
[26] Petronio, S. (2002). Boundaries of privacy: Dialectics of disclosure (xix,pp. 268). Albany, NY: State University of New York Press.
[27] Chen, J., Ping, W., Xu, Y., & Tan, B.C.Y. (2009). Am i afraid of my peers? Understanding the antecedents of information privacy concerns in the online social context. In: Proceedings of the Thirtieth International Conference on Information Systems.

[28] Metzger, M.J. (2007). Communication privacy management in electronic commerce. Journal of Computer-Mediated Communication, 12(2), 335–361.
[29] Ji, P. & Lieber, P. S. (2010). Am I safe? Exploring relationships between primary territories and online privacy. Journal of Internet Commerce, 9(1), 3–22.
[30] Zikmund, W. G. (2003). Business research methods (7th ed.). Cincinnati, OH: Thomson.
[31] Xu, C., Ryan, S., Prybutok, V., & Wen, C. (2012). It is not for fun: An examination of social network site usage. Information and Management, 49(5), 210–217.
[32] Taylor, S., & Todd, P.A. (1995). Understanding information technology usage: A test of competing models. Information Systems Research, 6(2), 144-176.
[33] Moore, C., & Benbasat, I. (2001). Development of an instrument to measure the perception of adopting an information technology innovation. Information Systems Research, 2, 192-222.
[34] Al-Debei, M., Al-Lozi, E., & Papazafeiropoulou, A. (2013). Why people keep coming back to Facebook: Explaining and predicting continuance participation from an extended theory of planned behaviour perspective. Decision Support Systems, 55(1), 43-54.
[35] Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. Information Technology and Management, 6(2-3), 181-202.
[36] Premkumar, G., & Ramamurthy, K. (1995). The role of Interorganizational and organizational factors of the decision mode for adoption of interorganizational systems. Decision Science, 26(3), 303-336.
[37] Comrey, A.L., & Lee, H.B. (1992). A first course in factor analysis. N.J.: L. Erlbaum Associates.
[38] Asher, H.B. (1983). Causal modeling. Newbury Park: Sage University Press.
[39] Lee, M. (2009). Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. Electronic Commerce Research and Applications, 8(3), 130-141.
[40] Alsharif, A. (2014). Teaching the customs, traditions and culture of Saudi Arabia through the arts in high school to promote cultural understanding and appreciation (Order No. 1589365). Available from ProQuest Dissertations & Theses Global. (1691800000).
[41] Alotaibi, M. (2015). Mobile Computing Trends in Saudi Arabia: An Exploratory Study. I.J. Information Technology and Computer Science, 01, 21-32.