On Privacy Calculus and Underlying Consumer Concerns influencing Mobile Banking Subscriptions

Kennedy Njenga
Department of Applied Information Systems
University of Johannesburg
Johannesburg, South Africa
e-mail: knjenga@uj.ac.za

Sifiso Ndlovu
Department of Applied Information Systems
University of Johannesburg
Johannesburg, South Africa
e-mail: sndlovu@pragmaticworks.com

Abstract—**The advancement of technology in mobile devices places South African (SA) banking institutions in unique positions to leverage these advancements into innovative value added services. Mobile banking is one such innovation that has afforded banking clients the ability to, amongst other services, view bank statements, pay bills, and transfer money. Despite a growing trend in mobile banking service offerings by SA banks, privacy and security issues are still considered a concern. The paper conceptualizes the underlying concerns by bank clients regarding the adoption of mobile banking services. Privacy Calculus Theory (PCT) has been used as a theoretical lens to explain the cognitive process involved when a potential mobile banking subscriber is presented with mobile banking technology solutions. The paper extends PCT by abstracting the risk/benefit trade-off *psyche* held by SA bank clients. The paper attempts to explain, using PCT, the bank clients' cognitive process and willingness to subscribe to mobile banking services. Quantitative research method has been used for this purpose. Purposeful sampling that targeted SA bank-account holders was applied. Empirical results show that the South African banked consumers' *psyche* is largely influenced by the utility of a technology (mobile banking service) and interestingly, privacy and security play a lesser role in this trade-off.**

Keywords-component; Mobile banking, Security, Information Privacy, Privacy Calculus Theory

I. Introduction

In the recent past, South Africa has witnessed diffusion of technologically advanced mobile devices in different economic segments. In business for instance, there has been acceptance and growing use of tablets and smartphones. Apple's *i-Pad* and Samsung's *Galaxy Note* phone for instance, are increasingly being embedded in business processes due to the unique features that these devices possess. Equipped with business-oriented applications (apps), such as spreadsheet apps, word processer apps, meeting reminder apps and meeting-minute drafting apps these devices expediently facilitate business.

There are several factors that have been attributed to the growing use of mobile devices. Factors such as affordability and convenience inherently make these devices attractive to consumers. The affordability factor invariably occurs as the price value of the mobile device decreases particularly when newer versions of the device become introduced to the market. For instance, the latest Apple's *i-Phone* model has led to the decrease in market prices of older *i-Phone* models, prompting more accessibility and affordability of the older models.

The advancement of technology in mobile devices places South African (SA) banking institutions in unique positions to leverage these advancements into innovative value added services. Various kinds of banking services that are device-centric are presently being marketed to bank clients. Convenience is a sound-bite used by banks to push mobile technology services to clients by allowing clients to view bank statements, pay bills, and transfer money.

While a growing number of South African banking clientele are beginning to slowly embrace mobile banking, anecdotal evidence suggests that many still prefer to conduct their banking via branch visits and occasionally by computer.

In an attempt to understand the underlying *psyche* and prevailing privacy and security perceptions that the South African banking clientele holds, we use and extend the Privacy Calculus Theory. The privacy calculus Theory (PCT) explains information privacy from a decision making perspective. In information systems, PCT posits that consumers constantly engage in an information privacy decision process (*the calculus*) wherein they compare the perceived risks against perceived benefits of using a technology [40]; [13]; [22]. The paper therefore extends PCT by abstracting the risk/benefit trade-off *psyche* held by the bank clients towards explaining their willingness to subscribe to mobile banking services. It follows then that the main research question is:

a) How does a bank client's perception regarding privacy/security and the inherent technology utility of a mobile device influence the decision to subscribe to a mobile banking service?

In trying to address and discuss the context and the question raised, this paper divides itself into eight sections. Section 1 has introduced and laid context for the key theme. Section 2 that follows this section unpacks terminology related to Information Privacy in greater detail. Section 3 introduces the conceptual framework while discussing Privacy Calculus Theory (PCT) in greater depth. Section 4 delineates the methodology while Section 5 provides a discourse on results. The penultimate sections 6 and 7 revisits the conceptual model and discusses what this means to theory and practice. Section 8 concludes the paper**.**

II. Information Privacy

Information privacy relates to the disclosure and use of personal information and is defined as the right of institutions, groups, or individuals to decide on the extent of disclosing their personal information [33];[7]. According to Barman [5] organizations should overtly inform consumers as to why personal information is collected and how it will be utilized. As Barman [5] notes, information disclosure rights are usually the preserve of consumers who must grant permission to organizations when these seek to use or to share personal information with third parties. Many countries have established regulatory bodies that oversee the functioning of financial institutions. In the United States for instance, the Financial Services Modernization Act (FSMA) forbids financial institutions from sharing clients' private personal information to non-affiliated third party organizations unless permission is granted by the client [32].

A. Information Privacy in South African Banks

The leading privacy concerns within South African banking institutions emanate from storage and use of clients' financial information [35]. South African banking institutions are presently guided by Acts of parliament, information security policies, standards and procedures that present the best ways to address the issue of disclosure of personal information. The Protection of Personal Information Bill, as introduced in the National Assembly (proposed section 75) has amplified this debate and concern in South Africa. The Bill published in Government Gazette No. 32495 of 14th August 2009 recognizes "*the right to privacy"* and "*includes a right to protection against the unlawful collection, retention, dissemination and use of personal information*" [28]. Moreover, most banking institutions abide by the stipulated codes of banking practice which are administered by the South African banking ombudsman. As part of the codes of banking practice, banks must assure their clients of confidentiality and privacy regardless of whether these clients maintain patronage with such banks or not [28].

B. Mobile Banking

Yoo [41:120] posits that mobile banking is "*a coalescence of mobile technology and financial services which surfaced after the dawn of the portable internet and smart-chip-embedded handsets*". Unlike internet banking which could mainly be established when one is exposed to a computer with an internet connection, mobile banking only requires subscribers to be in possession of a mobile phone with at least GPRS functionality. Consequently, a raising number of banking customers are opting to consider mobile banking services. This increasing growth in subscription to mobile banking services arises from the fact that statistically more people own mobile phones than they do fixed-line telephone [12].

Like other technological inventions, mobile banking suffers from security related issues. The security implications for mobile banking include non-repudiation, encryption, and transaction states. Furthermore, Deans [12] argues that issues such as lack of standards and security within devices as well as networks may be the stumbling block for the success of future of mobile banking services.

Hu [19: 211] asserts that "*mobile services such as mobile commerce can only be conducted if all parties believe that there is adequate security*". Accordingly, a viable security policy includes implementing effective security measures, identifying security risks, and educating users on the importance of security procedures.

C. Mobile Banking in South Africa

South African banking institutions continue to launch and re-launch mobile banking services that have mutual benefit both to the banks and the clients they serve. Amongst the services presently introduced include Nedbank's *M-PESA*TM, Standard Bank's *Instant Money*TM, FNB's *eWallet*TM and ABSA's *CashSend*TM.

The above mentioned "big four" South African banks use General Packet Radio Service protocol, (GPRS) the Short Message Service protocol (SMS) and Unstructured Supplementary Service Data (USSD) to make mobile banking applications accessible to banking clients [9]. The SMS and USSD technology rely on Wireless Internet Gateway (WIG). SMS Banking, which is based on Global System for Mobile Communications (GSM), allows subscribers to receive and request banking information on their mobile devices using the text-layout on the SMS platform [31];[2].

USSD is also part of GSM technology and it establishes a new secure session without any message trail. However, in terms of response times, USSD is much faster than SMS technology and as a result, the big four banks effectively use it. GPRS was an addition to the GSM network architecture and it allows bank users to access mobile applications via Wireless Application Protocol (WAP) [9].

The main requirement for subscribing to mobile banking services across four banks is that you should be an account holder within a given bank. Typical mobile banking services includes balance inquiry, viewing statements, transfers of money between accounts, making payments to beneficiaries, and purchases of pre-paid airtime and electricity [26];[34];[1];[16].

D. Mobile Banking Privacy and Security Issues

Mobile banking privacy cannot be removed from the wider aspects of general organizational security [15]. In fact some of the shortcomings of mobile banking privacy issues have become beneficial to white-collar perpetrators. White-collar crime can be defined as fraud and theft committed by mostly organization's personnel. There are two main reasons as to why the mobile environment can subject itself to, amongst other things, risks and white-collar crime. The first reason stems from the fact that the wireless platform used in mobile banking is shared and mainly an unrestrained medium. Secondly, wireless is a promiscuous technology in a sense that anyone can setup and connect given the necessary credentials [23].

In spite of the efforts made by banks towards curbing and detecting fraud, there are still incidents of fraud and theft on banking accounts reported by clients. Whilst the nature of the reported incidents ranges from trivial to significant, they are still of great concern, particularly because such incidents involve security. Security on mobile device technology continues to be a matter of research interest, especially when banking institutions continue to place strong emphasis and reliance on mobile technology as part of delivering efficient business service.

Three categories of threats exist in mobile banking security, namely, disclosure threats (that border on privacy issues), integrity threats, and denial-of-service threats. Disclosure threats or violations of confidentiality occur when the message or information considered to be private is disclosed to a third party [15]. Disclosure threats are further divided into eavesdropping, masquerading, traffic analysis, browsing, leakage, and inference. Integrity threats occur when the contents of a report, communication or message are copied, manipulated or altered by an interloper. Denial-of-service is established when right of entry to a base station or access point is deemed unfeasible by a hostile (possibly, intruder's) terminal overloading it with calls.

III. Conceptual Framework

Literature review portrays justifiable concern by consumers of traditional banking services technology as hesitant to embrace the more current and innovative mobile banking services. Such concerns are due to fear that banks and other financial institutions might not provide adequate assurance regarding use of their personal details in mobile platforms.

The uncertainty of privacy and security in mobile banking services, coupled with the innate attractiveness of mobile banking convenience results in situations where consumers engage in calculated trade-offs between the perceived benefits the underlying mobile technology may be deemed to offer (the utility) against perceived risks. It may not be surprising for consumers to forego privacy concerns at the expense of utilizing a mobile banking service if the utility derived by convenience is much higher. This latter idea possibly explains the diffusion rate and increasing uptake of mobile banking services. The Theory of Privacy Calculus explains such predicaments in insightful ways.

A. The Theory of Privacy Calculus

The Theory of Privacy Calculus argues that a consumer's ability to take risk (disclosure of personal information) is influenced by the consumer's perception of benefits against risks (the calculus). During *privacy calculus*, potential consumers are invariably willing to disclose personal information and forgo worrying about privacy and security whenever the perceived benefits (i.e. the utility of mobile banking's ease of use, high network availability etc.) outweigh the perceived potential privacy risk [40].

A related concept to Privacy Calculus Theory (PCT) is the Technology Acceptance Model (TAM). Whilst PCT attempts to *share insight on the psyche* of a potential consumer of technology, TAM provides insight on *external factors* that largely influences the potential subscriber's decision on whether or not to disclose personal information [30]. TAM is characterized by factors (variables) that are fundamental building blocks for PCT and which are commonly shared between these two frameworks. These two variables are '*Perceived Ease of Use'* (PEOU) and '*Perceived Usefulness'* (PU) of a technology [25];[29];[36]. PEOU refers to the amount of effort required on the consumer's side to utilize a system or service. TAM hypothesizes that the lesser the effort, taken to utilize a specific technology, the higher the utility and PEOU. The subsequent likelihood is that the consumer will perceive the proposed technological service as beneficial. This will in turn influence the consumer's *calculus* towards a specific technology or service [37].

The second TAM factor, PU, refers to whether or not the consumer believes that utilizing the mobile banking technology will increase the consumer's productivity. Similarly, the higher the belief that the technology will improve productivity, the greater the PU, which in turn increases the chances that the consumer will be willing to risk security (*privacy calculus*) and disclosure of private information as a trade-off towards utilizing the technology. However PU and PEOU are not the only determinants of PCT. Klein and Kleinman, [24] proved that there are other factors that influence consumer utility on technology, such as social factors that define status, meaning and usefulness of technological innovation within a given context.

This process was labeled as the social construction of technology (SCOT) [24]; [27]. SCOT is defined in four components, namely that of interpretive flexibility, closure and stabilization, wider context, and *relevant social groups* [24]. The latter component has been selected as an influencing variable in PCT and is of most concern to this study.

B. The Constructs

Based on the previous discussions, PCT identifies risks and benefits as independent variables that influence behavioral intentions. The framework also incorporates '*Perceived Ease of Use'* (PEOU) and '*Perceived Usefulness'* (PU) of a technology as other variables that influence behavioral intention (privacy calculus).

We extend PCT to include *relevant social groups* (RSG) [24] and *institutional privacy assurance* (IPA) as other variables that influence behavioral intention and therefor privacy calculus. In total we identified five prominent independent variables that would be tested against the extended PCT as follows;

- *Perceived Ease of Use* (PEOU)
- *Perceived Usefulness* (PU)
- *Relevant Social Groups* (RSG)
- *Institutional Privacy Assurance* (IPA)
- *Perceived Privacy Risks* (PPR)

For purposes on this study, we note that behavioral intention or *willingness to subscribe* (WtS) to the mobile banking technology is the dependent variable that is also used in our extended PCT. **Figure 1** illustrates the conceptual model.

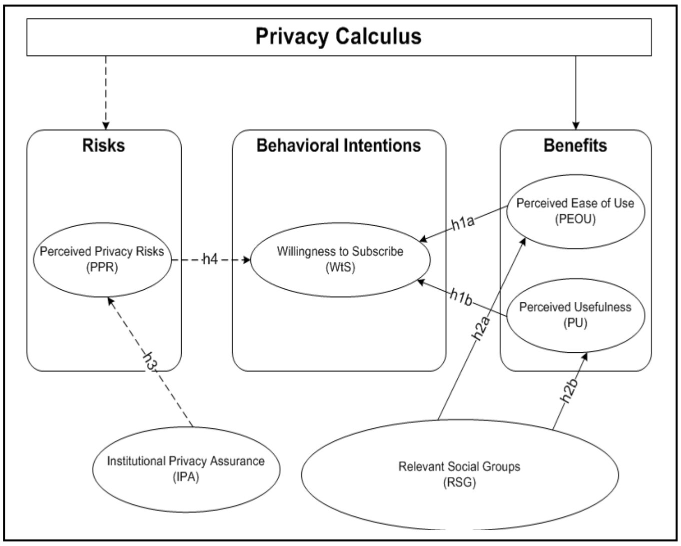
Privacy Calculus
Risks
Behavioral Intentions
Benefits
Perceived Ease of Use (PEOU)
h1a
Perceived Privacy Risks (PPR)
h4
Willingness to Subscribe (WtS)
h1b
Perceived Usefulness (PU)
h3
h2a
h2b
Institutional Privacy Assurance (IPA)
Relevant Social Groups (RSG)

Figure 1. **Extended Privacy Calculus Conceptual Model**

The model depicts privacy concerns as two-fold: perceived risks and perceived benefits. The behavioral intention component (*willingness to subscribe* -WtS) is a dependent variable of perceived risks and perceived benefits which are in turn influenced by PPR, IPA, RSG, PEOU and PU. Based on the framework above the following hypotheses can be deduced:

H1: PEOU and PU will positively influence WtS.

H2: RSG will positively influence PEOU and PU.

H3: PPR will negatively influence WtS.

H4: IPA will negatively influence WtS.

The research work therefore set out to test the above hypotheses regarding the *psyche* underlying *privacy calculus* for a South African mobile banking consumer. The next section outlines the methodology and methods used to test the above hypotheses.

IV. METHODOLOGY

According to Dawson, [10] a research method is the general principle that will guide the research. There exist two types of research methods, namely, qualitative, and quantitative. This research was quantitative in approach and sought an answer to the "how" question. The findings of this quantitative research are presented in an aggregated, summarized and statistical form [6];[20].

We surveyed respondents on a 5-point Likert scale questionnaire that was developed for the rigorousness understanding of inherent user *psyche*. We statistically scrutinized the *psyche* underlying *privacy calculus* and decision process of sampled South Africa mobile banking consumers. To achieve this purpose, we developed questionnaires that targeted a profile of potential mobile bank subscribers. Our quantitative research questions were relationship type questions.

The aim of relationship type research questions is to investigate groups, associations or causal relationships between two or more variables. This particular study was aimed at examining *privacy calculus* of a potential consumer of a mobile banking service and the *psyche* underlying willingness to actually subscribe to mobile banking.

A. Sampling and Non-Probability Sampling

Sampling is a way of identifying the unit of analysis (i.e. people, behavior, objects, events, or other elements) that can be used to conduct a research study. Sampling can be probability and non-probability sampling. During non-probability sampling, not every member of a target population is chosen as part of the sample. On the contrary, probability sampling requires that every research element (target population member) has equal opportunity of being chosen for a study as others.

For purposes of this research, purposive, non-probability sample was chosen as the appropriate sampling method that best fit our requirements [3];[4]. The sample comprises bank clients who belonged to the big four South African banks (i.e. FNB, ABSA, Nedbank, and Standard Bank). A filter question in the questionnaire was used to determine this. **Table 1** below illustrates this study's sampling process:

TABLE I. SAMPLING PROCESS

Sampling	**Examples**
Non-Probability Sampling	General Profile of South Africans
Purposive Sampling	Banking clients of South Africa

B. Data Analysis

Data analysis is a process that involves making sense of data that has been collected [39]. Data analysis should be confined within the constraints of a given research problem and objectives [38]. We analyzed our data using SPSS, a statistical software that utilizes syntax of mathematical processes to help researchers make sense of collected data. We employed and adhered to the requirements and procedures of parametric statistics due to interval scale of measurement used [17].

C. Reliability Analysis

According to Foster, [17] whenever data analysis is conducted, it is imperative that reliability and validity of the measurement instrument is evaluated. There are various ways of assessing reliability of a scale such as *internal consistency* methods. Internal consistency methods focus on measuring the consistency of respondents' answer to questions that relate to an underlying construct or scale. The internal consistency method is further divided into average inter-item correlation, average inter-total correlation, split-half correlations, Cronbach's alpha, and the Kuder-Richardson coefficient [11]. This study utilized internal consistency prescribed by the Cronbach's alpha method. The rules of Cronbach's alpha dictate that the measurement instrument can only be reliable with positive values of 0.7 or more. **Table II** presents summarized results for the reliability analysis of all 5 constructs.

TABLE II. RELIABILITY

Reliability Statistics		
Construct	**Cronbach's Alpha**	**Number of Items**
Perceived Ease of Use (PEOU)	.796	15
Perceived Usefulness (PU)	.825	15
Perceived Privacy Risks (PPR)	.900	18
Relevant Social Groups (RSG)	.881	21
Institutional Privacy Assurance (IPA)	.930	20

The analysis was conducted by grouping all variables pertaining to constructs. The Cronbach's alpha for all constructs was greater than 0.7 which indicates that the instrument used to measure these constructs was consistent. It must be noted, however, that initially the reliability analysis of the PEOU construct was based on 16 items but variable PEOU11 was later eliminated as it had negative correlations against other variables which could have indicated that it might have been measuring something different. Consequently, with the elimination of variable PEOU11, the Cronbach's alpha for the overall PEOU improved from **.791** to **.796.**

D. Test of Validity

Validity on the other hand refers to examining whether the research's measurement instrument is actually measuring what it supposed to measure [21]. This means that it is possible that the measurement instrument is reliable but it could be measuring different underlying concepts than the research's initial objectives. Thus, a valid measurement instrument is "one that truly measures the construct of interest" [14]. Similarly to research reliability, there are various aspects to validity such as criterion, convergent and discrimination, construct, and content validity [11].

For the purposes of this study, construct validity was further scrutinised. Construct validity involved estimating existence of inferred underlying characteristics (i.e. intelligence, love, curiosity etc.) based on behaviour [18]. Construct validation is often a lengthy process because "no criterion or universe of content is accepted as completely sufficient in defining the construct to be measured" [18]. In other words, as postulated by De Vaus [11], a construct becomes validated when relationships within items of measurement instrument are established in line with theoretical understanding about the construct.

V. RESULTS AND DISCUSSION

There were a total of 350 questionnaires distributed across 7 cities within South Africa's 5 provinces. As it has been explained in methodology section, these cities were chosen because of the diversity in banking clients' cultural, demographic and biographic characteristics. These provinces were *Kwa-Zulu Natal*, *Gauteng*, *Mpumalanga*, *North West* and *Limpopo*. Each of these provinces was allocated 50 questionnaires. There were 209 questionnaires successfully captured out of the 350 that were distributed (a success rate of 59.7%).

Table III below provides a summary of the provinces that had the most responses to the questionnaires. The *Zululand* District of Kwa-Zulu Natal province had the highest response rate, followed by Gauteng's *Sandton* and again Kwa-Zulu Natal's *Durban* at a tie. Mpumalanga's *White River* came in fourth. Gauteng's *Auckland Park* came fifth while North West's *Kimberly* and Limpopo's *Polokwane* came sixth and seventh respectively.

TABLE III. LOCATION

	Where was the questionnaire filled?			
	Location	***Frequency***	***Valid%***	***Cumulative %***
Valid	*Sandton*	39	18.7	18.7
	Durban	39	18.7	37.3
	Polokwane	10	4.8	42.1
	Kimberly	14	6.7	48.8
	Zululand	46	22.0	70.8
	White River	38	18.2	89.0
	Auckland Park	23	11.0	100.0
	Total	**209**	**100.0**	

A. Prerequisite Questions

It was imperative that the correct respondents were identified and that is why a set of prerequisite questions were provided. **Table IV** provides a summary of the responses to the prerequisite questions which shows that the data collected was from the intended respondent as they all answered accordingly.

TABLE IV. SA BANK HOLDER

	Have you been an account holder of a South African bank?			
		Frequency	***Valid%***	***Cumulative %***
Valid	*Yes, I had in the past five years*	55	26.3	26.3
	Yes, I currently do	154	73.7	100.0
	Total	**209**	**100.0**	

B. Age Group

The questionnaire identified 6 levels of age groups that respondent could be classified into. **Table V** provides a summary of which age group had the most respondents. As noted by **Table V**, the age group (21-29) had the highest response rates with the age group (60 or older) having the lowest response rates.

TABLE V. AGE GROUP

	Age Group			
	Age Group	***Frequency***	***Valid%***	***Cumulative %***
Valid	20 or younger	36	17.2	17.2
	21 – 29	81	38.8	56.0
	30 – 39	56	26.8	82.8
	40 – 49	23	11.0	93.8
	50 – 59	11	5.3	99.0
	60 or older	2	1.0	100.0
	Total	209	100.0	

C. *Ethnicity*

According to **Table VI** below, there were more people of black ethnicity who respondent to the questionnaire than any other race groups.

TABLE VI. ETHNICITY

	Ethnicity			
	Ethnicity	***Frequency***	***Valid%***	***Cumulative %***
	Black	141	67.5	67.5
	Colored	22	10.5	78.0
	Indian or Asian	17	8.1	86.1
	White	29	13.9	100.0
	Total	209	100.0	

D. *Employment Status*

According to **Table VII** below there were significantly more self-employed people who responded to the questionnaire.

TABLE VII. EMPLOYMENT STATUS

	Age Group			
	Age Group	***Frequency***	***Valid%***	***Cumulative %***
Valid	*Employed*	36	64.1	64.1
	Self-employed/ Independent Consultant	81	7.7	71.8
	Unemployed	56	5.3	77.0
	Student	23	22.0	99.0
	Retired/Pensioner	11	1.0	100.0
	Total	209	100.0	

VI. TESTING OF THE HYPOTHESES

Perceived Ease of Use and Perceived Usefulness

This section revisits the hypothesis stipulated previously and tests these respectively as follows: **H1**: PEOU and PU will positively influence WtS. We conducted a correlation test in order to establish the relationship between the independent variables PEOU/PU *Perceived Ease of Use/ Perceived Usefulness*) and the dependent variable WtS (*Willingness to Subscribe*). The purpose was to determine the *Pearson correlation coefficient* (two-tailed test) using SPSS. The SPSS output provided a matrix shown as **Table VIII** below.

TABLE VIII. CORRELATION BETWEEN WTS AND PEOU/PU

		WtS	**PEOU**	**PU**
		Banking And File Sharing	I have never experienced timeouts	Always operational .
Banking And File Sharing	Pearson Correlation	1		
	Sig. (2-tailed)			
I have never experienced timeouts	Pearson Correlation	.269**	1	
	Sig. (2-tailed)	.000		
Always operational.	Pearson Correlation	.144*	.614**	1
	Sig. (2-tailed)	.038	.000	
**. Correlation is significant at the 0.01 level (2-tailed).				
b. Listwise N=209				

Data analysis show that PEOU and PU are positively related to WtS with a Person correlation coefficient of ***r*** = .**269** and **.144** respectively. The Significant Value for PEOU is less that **.001** (as indicated by the double asterix (**) after the coefficient). The significance value shows that the probability of getting a correlation coefficient this big in a sample of 209 respondents if the null hypothesis were true is very low. Although we can state with certainty that PEOU will positively influence WtS, since the significance is less than .001 we cannot state the same (with any certainty) with the variable PU which has a significance of **.038** that PU is related to willingness to subscribe. We may reject the null hypothesis..

Relevant Social Groupings

This section revisits the hypothesis: **H2-** RSG (*Relevant Social Groups*) will positively influence PEOU and PU. The SPSS output provided a matrix shown as **Table IX** below. Data analysis show that PEOU and PU are positively related to RSG (weak relationship) with a Person correlation coefficient of ***r*** = .**181**** and **.039** respectively. This can be interpreted to mean that family and friends have an influence, although a weak one, on a consumer’s choice to subscribe to mobile banking services.

TABLE IX. CORRELATION BETWEEN RSG AND PEOU/PU

		PEOU	PU	RSG
		Mobile banking applications' default screen lists types of banking transactions available.	Mobile banking applications allow for the purchases of prepaid airtime, electricity etc.	Somebody influenced my adoption of mobile banking applications.
Mobile banking applications' default screen lists types of banking transactions available.	Pearson Correlation	1		
	Sig. (2-tailed)			
Mobile banking applications allow for the purchases of prepaid airtime, electricity etc.	Pearson Correlation	.181**	1	
	Sig. (2-tailed)	.009		
Somebody influenced my adoption of mobile banking applications.	Pearson Correlation	.039	.193**	1
	Sig. (2-tailed)	.573	.005	
**. Correlation is significant at the 0.01 level (2-tailed).				
b. Listwise N=209				

Perceived Privacy Risk

This section revisits the hypothesis: **H3**- PPR (Perceived Privacy Risk) will negatively influence WtS. The SPSS output provided a matrix shown as **Table VIII** below. The SPSS output provided a matrix shown as **Table IX** below. Data analysis show that two constructs used for PPR are both negatively related to WtS (weak relationship) with a Person correlation coefficient of ***r*** = **-.204**** and **-.048** respectively.

TABLE X. CORRELATION BETWEEN PPR AND WTS

		WtS	PPR	PPR
		Banking And File Sharing	Mobile banking applications informs subscriber about ways of reinforcing security.	Mobile banking applications provide tips on security mechanisms' best practice.
Banking And File Sharing	Pearson Correlation	1		
	Sig. (2-tailed)			
Mobile banking applications informs subscriber about ways of reinforcing security.	Pearson Correlation	-.204**	1	
	Sig. (2-tailed)	.003		
Mobile banking applications provide tips on security mechanisms' best practice.	Pearson Correlation	-.048	.622**	1
	Sig. (2-tailed)	.490	.000	
**. Correlation is significant at the 0.01 level (2-tailed).				
b. Listwise N=209				

In light of South African consumers' perceived privacy threats the data can be interpreted to mean that that South Africa banking institutions constantly intervene with the aim of re-assuring consumers hence altering the consumer's privacy calculus. That is why the data shows very weak relationships. (***r*** = **-.048**, significant at **p = .490**). This means that we cannot be conclusive that risk has an influence on a consumer's willingness to subscribe to a mobile banking service even though they are aware. This is because the **p value** is not significant (**p =.490**).

Institutional Privacy Assurance

This section revisits the hypothesis: **H4**: IPA *(Institutional Privacy Assurance*) will negatively influence WtS. The SPSS output provided a matrix shown as **Table IX** below. Data analysis show that two constructs used for IPA are both negatively related to WtS with a Person correlation coefficient of ***r*** = **-.056** and **-.007** respectively. The data shows weak relationships and that Institutional privacy assurance (IPA) likely affect the subscriber's privacy calculus, but not as strongly as originally envisaged. According to data, the role of banks (or lack thereof) of assurance and obligations towards the privacy of client's personal information has not been significant.

TABLE XI. CORRELATION BETWEEN WTS AND IPA

		WtS	IPA	IPA
		Banking And File Sharing	I am satisfied with my bank's mobile banking application privacy policy	My banks provides explanations for the collection of my personal information
Banking And File Sharing	Pearson Correlation	1		
	Sig. (2-tailed)			
I am satisfied with my bank's mobile banking application privacy policy	Pearson Correlation	-.056	1	
	Sig. (2-tailed)	.421		
My banks provides explanations for the collection of my personal information	Pearson Correlation	-.007	.463**	1
	Sig. (2-tailed)	.914	.000	
**. Correlation is significant at the 0.01 level (2-tailed).				
b. Listwise N=209				

In summary and on the basis of the above empirical findings, it seems that empirical data analysis *confirms* (although a weak confirmation of) *all our prior hypotheses*.

VII. PRIVACY CALCULUS AND CONSUMER AND BANKING CONSUMER PSYCHE

A. Revisiting the Conceptual Model

Based on empirical data we revisit and populate the model Figure 2 below as follows:

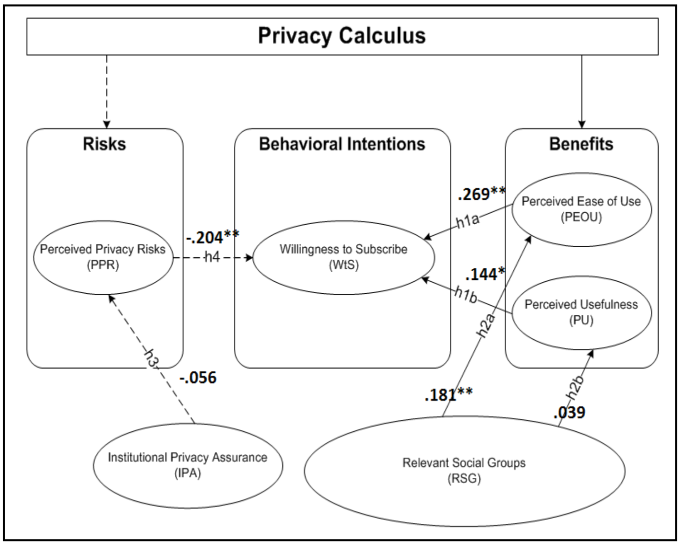
Privacy Calculus
Risks
Behavioral Intentions
Benefits
Perceived Privacy Risks (PPR)
Willingness to Subscribe (WtS)
Perceived Ease of Use (PEOU)
Perceived Usefulness (PU)
Institutional Privacy Assurance (IPA)
Relevant Social Groups (RSG)
-.204**
h4
.269**
h1a
.144*
h1b
h2a
h2b
h3
-.056
.181**
.039

Figure 2. **Privacy Calculus Conceptual Model Showing Empirical Relationships**

It can be shown from **Figure 2** above that South African banked consumer *psyche* is largely influenced more by the perceived ease of use (PEOU) of a technology (***r*** = **.269****) than perceived risk (r = **-.204****). ***According to this study this variable has the most significant influence over all other variables when determining whether or not to subscribe to mobile banking service.*** In South Africa, this is significant particularly because it shows how technology is presently perceived. Empirical data shows that privacy and security is not as predominant in the *psyche* of the consumer as expected. This is especially so when banks do not disclose any specific breaches to public. The 'discerning' South African consumer will therefore forgo concerns about privacy and security. In South African banking contexts, this is a potential huge benefit for bankers particularly if consumers exhibit or display this sort of psyche.

Another factor that can be deduced from the model is that relevant social groups (RSG) **(*r* = .181**)** have the potential to influence a consumer's psyche. Empirical data however shows this as a very weak or insignificant influence. Research has shown that South Africans rely of close friends and family to influence their purchase decisions. For example, if there is a general positive groupthink towards a proposed technological service emanating from social interactions, then willingness to subscribe to the particular technological service follows.

B. Implication for Practice

Drawing on the insights from Privacy Calculus Theory, (PCT) the work provides empirical evidence of a weak relationship between consumers' perceived privacy risk (PPR) and their willingness to subscribe (WtS). This is an interesting finding because it shows that consumers' conscientious understanding of privacy and security might not dampen their willingness to use internet banking if there is perceived technological utility. The theory of privacy calculus argues that in order for a consumer to risk disclosure of privacy, the said consumer constantly compares the perceived benefits against the perceived risks. ***Empirical data shows that PEOU has a much stronger relationship with WtS than all other variables. It follows then that this is the privacy calculus for this study.***

To practice this means that as long as a consumer's willingness to subscribe (WtS) is derived from the perceived usefulness of the technology, this might mitigate their worry towards privacy and security. The results are only strengthened only when there is an element of institutional privacy assurance.

C. Implication for Theory

The current study contributed toward the construction of a broader knowledge base towards understanding the *psyche* of South African banking consumers. The theoretical advances made in the study as espoused by the conceptual model advances the study of Privacy (and Security risk). From a consumer perspective, the use of Privacy Calculus Theory offers a new way of conceptualizing the psyche of a banked South African consumer in light of other existing theories. The study highlights the fact that Privacy (and Security risk) should not be looked at in isolation of other variables such as utility of technology. Significantly and most interesting, according to this study, utility may at times override privacy and security concerns. This should be worrying to practitioners of security particularly if dynamics of utility variables keep changing in contexts.

VIII. CONCLUSION

The article explored the psyche around South African banked consumers' willingness to subscribe to mobile banking services. The article introduced Privacy Calculus Theory which is characterized by two important variables, namely risk and benefits and how these two influence consumer psyche. The empirical results from this study reveal that while practice may emphasize and place significant interest in privacy and security, this perception significantly differs from consumers. Empirical data in this study reveals that the higher the perceived utility that a consumer derives from a technology service and in this case mobile banking service, the more this may override privacy and security concerns. ***This is the inherent calculus revealed in this study***. Based on empirical data, it is worrying to note that perceived benefits of mobile banking services had a much stronger influence on South African banked consumer psyche than perceived risks. While the study has shown this inherent calculus, this does not in any way dilute the importance of security. Essentially a lot needs to be done to ***raise awareness*** of security concerns.

REFERENCES

[1] ABSA. [2011]. Cellphone Banking. Available from: http://www.absa.co.za/Absacoza/Individual/Ways-to-Bank/Anytime,-Anywhere/Cellphone-Banking (Accessed 13 July 2011).

[2] Adagunodo, E. R., Awodele, O. & Ajayi, O. B. (2007). SMS Banking Services: A 21st Century Innovation in Banking Technology. Issues in Informing Science and Information Technology, 4:227-234.

[3] Adler, E. S. & Clark, R. (2008). How it's done: An Invitation to Social Research, 3rd edition. California: Thomson.

[4] Agarwal, B. L. (2005). Programmed Statistics: Question-Answers, 3rd edition. New Delhi: New Age International.

[5] Barman, S. (2002). Writing Information Security Policies. New Riders: Indiana.

[6] Britten, N. (2011). Qualitative Research on Health Communication: What Can it Contribute? Patient Education and Counseling, 82: 384–388.

[7] Cate, F. H. (1997). Privacy in the Information Age. The Brookings Institution: Washington.

[8] Charmaz, K. (2006). Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis. London: SAGE Publications.

[9] Chikomo, K., Chong, K. M., Arnab, A. & Hutchison, A. (2006). Security of Mobile Banking. Available from: http:// pubs.cs.uct.ac.za/archive/00000347/01/Security_of_Mobile_Banking_paper.pdf (Accessed 13 July 2011).

[10] Dawson, C. (2006). A Practical Guide to Research Methods: A User-Friendly Manual for Mastering Research Techniques and Projects, 2nd edition. Oxford: How to Books Ltd.

[11] De Vaus, D. (2002). Analyzing Social Science Data: 50 Key Problems in Data Analysis. SAGE: London

[12] Deans, P., C. (2005). E-Commerce and M-Commerce Technologies. Hershey: IRM Press.

[13] Dinev, T., Hart, P. & Mullen, M. R. (2008). Internet Privacy Concerns and Beliefs about Government Surveillance – An Empirical Investigation. Journal of Strategic Information Systems, 17: 214-233.

[14] Dunn, D. S. (2010). The Practical Researcher: A Student Guide to Conducting Psychological Research, 2nd edition. Wiley-Blackwell: West Sussex

[15] Elliot, G. & Phillips, N. (2004). Mobile Commerce and Wireless Computing Systems. Harlow: Pearson.

[16] FNB. [2011]. Mobile Banking. Available from: https://www.fnb.co.za/cellphone-banking/mobile-banking.html (Accessed 13 July 2011).

[17] Foster, J. J. (1998). Data Analysis Using SPSS for Windows: A Beginner's Guide. SAGE: London

[18] Gregory, R. J. (1996). Psychological Testing: History, Principles, and Applications, 2nd edition. Boston: Allyn & Bacon.

[19] Hu, W., Lee, C. & Kou, W. (2005). Advances in Security and Payment Methods for Mobile Commerce. Hershey: Idea Group Publishing.

[20] Jacobs, J.K., Kawanaka, T., & Stigler, J. W. (1999). Integrating Qualitative and Quantitative Approaches to the Analysis of Video Data on Classroom Teaching. International Journal of Educational Research, 31: 717–724.

[21] Kaplan, R., M. & Saccuzzo, D., P. (2009). Psychological Testing: Principles, Applications and Issues, 7th edition. California: Wadsworth

[22] Kim, E. & Lee, B. (2009). E-Service Quality Competition Through Personalization Under Consumer Privacy Concerns. Electronic Commerce Research and Applications, 8: 182-190.

[23] Kipper, G. (2007). Wireless Crime and Forensic Investigation. London: Auerbach Publications.

[24] Klein, H. K. & Kleinman, D. L. (2002). The Social Construction of Technology: Structural Considerations. Science, Technology, & Human Values, Vol. 27(1): 28-52.

[25] Legris, P., Ingham, J. & Collerette, P. (2003). Why Do People Use Information Technology? A Critical Review of the Technology Acceptance Model. Information & Management, 40: 191-204.

[26] Nedbank. [2011]. Cellphone Banking. Available from: http://www.nedbank.co.za/website/content/Products/ product_detail.asp?SubSubcatid=1865&Subcatid=501&ProductID=102 (Accessed 13 July 2011).

[27] Nessiaprincess. (2009). Technological Determinism vs Social Construction of Technology. Available from: http://communicationista.wordpress.com/2009/12/16/technological-determinism-vs-social-construction-of-technology/ (Accessed 13 July 2011).

[28] On Protection Of Personal Information Bill [2009]. Minister of Justice and Constitutional Development- Republic Of South Africa: As introduced in the National Assembly (proposed section 75); explanatory summary of Bill published in Government Gazette No. 32495 of 14 August 2009 Available from: http://www.justice.gov.za/legislation/bills/B9-2009_ProtectionOfPersonalInformation.pdf (Accessed 13 July 2011).

[29] Pai, F. & Huang, K. (2011). Applying the Technology Acceptance Model to the Introduction of Healthcare Information Systems. Technological Forecasting & Social Change, 78: 650-660.

[30] Park, S. Y. (2009). An Analysis of the Technology Acceptance Model in Understanding University Students' Behavioral Intention to Use e-Learning. Educational Technology & Society, 12(3): 150-162.

[31] Peevers, G., Douglas, G., & Jack, M., A. (2008). A Usability Comparison of Three Alternative Message Formats for an SMS Banking Service. International Journal of Human-Computer Studies, 66:113-123.

[32] Shaw, P. (2001). E-Business Privacy and Trust: Planning and Management Strategies. John Wiley & Sons: New York.

[33] Solovo, D. J., Rotenberg, M. & Schwartz, P. M. (2006). Privacy, Information, and Technology. Aspen Publishers: New York.

[34] Standard Bank. [2011]. Banking on your Cellphone. Available from: http://standardbank.co.sz/SBIC/Frontdoor_02_02/ 0,2454,3447_27200558_0,00.html (Accessed 13 July 2011).

[35] Szewczak, E. & Snodgrass, C. (2002). Managing the Human Side of Information Technology: Challenges and Solutions. Idea Group Publishing: Hershey.

[36] Turner, M., Kitchenham, B., Brereton, P., Charters, S. & Budgen, D. (2010). Does The Technology Acceptance Model Predict Actual Use? A Systematic Literature Review. Information and Software Technology, 52: 463-479.

[37] Venkatesh, V. (2000). Determinants of Perceived Ease of Use: Integration Control, Intrinsic Motivation, and Emotion into the Technology Acceptance Model. Information Systems Research, 11(4): 342-365.

[38] Walliman, N. (2011). Your Research Project: Designing and Planning Your Work, 3rd edition. SAGE: London

[39] Wilkinson, D. (ed.) (2000). The Researcher's Toolkit: The Complete Guide to Practitioner Research. Routledge: London

[40] Xu, H., Luo, X. R., Carrolll, J. M., Rosson, M. B. (2011). The Personalization Privacy Paradox: An Exploratory Study of Decision Making Process for Location-Aware Marketing. Decision Support Systems, 51: 42-52.

[41] Yoo, Y., Lee, J. & Rowley, C. (2008). Trends in Mobile Technology and Business in the Asia-Pacific Region. Oxford: Chandos Publishing.