ON RATIONAL CHOICE, RISK AND UTILITY IN MOBILE BANKING

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

Sifiso Ndlovu,
Department of Applied Information Systems, University of Johannesburg, South Africa, SifisoN@karabina.co.za

ABSTRACT: The diffusion of mobile banking technology offers an opportunity for analysis of the risk associated with the protection of information of banking clientele. There is emerging discourse with regard to clientele awareness of privacy issues. This article conceptualises banking clientele awareness of specific issues such as risk, security and information privacy policies. The key concern is the impact such awareness has on subscribers choosing to continue their use of mobile banking services. The article attempts to explain the utility/risk trade-off and how this affects the clients' willingness to continue subscribing to mobile banking services, using quantitative analysis and rational choice theory (RCT). Purposeful sampling targeted South African bank account-holders. Empirical results show that consumer willingness to continue to use mobile banking services is largely driven by the perceived utility of the service, while privacy risk is not a significant deterrent. This is an important finding in the context of banks encouraging consumers to use mobile banking systems, for the banks to achieve retail growth. This creates a greater responsibility for banks to manage consumer risk. The findings may be more broadly pertinent in the SADC region and on the African continent, where telecoms firms engaged in mobile banking services must also attend to issues of consumer risk; and where R&D investment in the field of information security is highly desirable.

KEYWORDS:
Mobile banking, privacy, risk, utility, rational choice theory

INTRODUCTION: THE PROBLEM OF RISK AND UTILITY IN MOBILE BANKING

Countries on the African continent have witnessed diffusion of advanced mobile devices such as smart phones and tablets in diverse economic segments, with mobile banking users being predicated as drivers for present and future retail banking revenues in South Africa (SouthAfrica.info, 2012) and elsewhere, such as Ghana (Essegbey & Frempong, 2011) and Kenya (Mishra & Bisht, 2013). This has come as a result of convergence between smart phones and banking technology. Notably, smart phones are increasingly becoming as powerful as laptops and desktops (Husted, Saidi & Gehani, 2011). Smart phones also have robust sensor platforms containing technologies such as global positioning systems (GPS), near field communications (NFC), wireless fidelity (Wi-Fi), Bluetooth and cellular capabilities (Husted et al, 2011). Because of their storage and transactional capabilities, smart phones and tablets have been vaults for large amounts of personal information, thereby exposing their owners to risk. The use of smart phones and tablets in mobile banking has attracted researchers and practitioners to understand the information security risk and to address concerns of privacy and the protection of banking clientele information. Of primary concern to researchers has been the goal of information protection and the discourse that addresses issues such as privacy, trust and information risk, because consumers are exposed to risk of third party information access during transactions (Shen, Huang, Chu & Hsu, 2010). Banks, financial service providers and banked clientele have all become aware of the reputational risk associated with breaches in personal information. It has therefore become imperative that banks put in place mechanisms to protect personal information from security breaches or improper access.

While banking clientele continue to derive and expect increased utility in mobile banking options, banks are increasingly concerned with information governance and issues such as security and privacy that address information risk. In an attempt to understand the underlying utility/risk tradeoff that banking clientele engage in, the authors use and extend the rational choice theory (RCT). In the information systems field of enquiry, RCT posits that consumers constantly engage in *making choices*, in which they compare the perceived utility against perceived risks of using a technology. The paper extends RCT by analysing the utility/risk trade-off *choice* of the banking clients in order to explain their willingness to continue subscribing to mobile banking services. The main research question therefore is: How does a bank client's rational perception regarding inherent utility and risk of mobile banking influence the choice to continue subscribing to a mobile banking service?

In exploring the question, the authors studied responses from mobile banking users in five provinces in South Africa. The findings and analysis may have broader applicability to mobile banking on the African continent, as the respondents come from a variety of income levels, genders, urban and peri-urban environments. In addressing the context and the question raised, the article is presented as follows: introduction of main theme and context; discussion of terminology related to information privacy and conceptual framework discussing rational choice theory (RCT); methodology and results. The penultimate sections revisit the conceptual model on the basis of the results obtained; followed by a discussion of what this means to theory and practice.

MOBILE BANKING, INFORMATION GOVERNANCE AND PRIVACY

Yoo, Lee and Rowley (2008) posit that mobile banking is "a coalescence of mobile technology and financial services, that surfaced after the dawn of the portable Internet and smart-chip-embedded handsets" (p. 120). Unlike Internet banking, which can mainly be established via a computer with an Internet connection, mobile banking only requires subscribers to be in possession of a mobile phone with at least GPRS functionality. Hu, Lee and Kou (2005) assert that "mobile services such as mobile commerce can only be conducted if all parties believe that there is adequate security" (p. 211). Accordingly, a viable security policy includes implementing effective security measures, identifying security risks, and educating users on the importance of security procedures.

Information governance is a methodology for providing controlled access to sensitive information while privacy relates to the disclosure and use of personal information. According to Huang, Shen, Yen and Chou (2011), factors such as privacy may impact a consumer's mobile banking utility. In practice, privacy is a key issue that affects the building of trust in mobile banking services. It is defined as the right of institutions, groups, or individuals to decide on the extent of disclosing their personal information (Solovo, Rotenberg & Schwartz, 2006; Cate, 1997).

GOVERNANCE AND PRIVACY IN DEVELOPED COUNTRIES

According to Giordano, (2010) governance and privacy have been converging, particularly in aspects such as regulatory frameworks. As an illustration, in the late 1990s the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) jointly announced the formulation of an information governance framework for *web trust*. Web trust provided assurance in four primary areas, namely: (1) business practices and disclosure, (2) transaction integrity, (3) information protection and (4) information privacy (Huang et al, 2011). Another regulatory framework formulated in the United States, known as the Financial Services Modernization Act (FSMA), forbids financial institutions from sharing clients' personal information to non-affiliated third-party organisations unless permission is granted by the client (Shaw, 2001). Other assurance models, such as *Verisign*, focus on transaction integrity and information protection, while *TrustE* focuses only on information privacy. In addition to the *web trust* information governance framework, Table 1 below summarises examples of regulatory frameworks discussed that have had an impact on mobile banking practices in the US (Giordano, 2010).

TABLE 1: GOVERNANCE AND PRIVACY FRAMEWORKS

Assurance	Governance framework	Privacy frameworks
Business practices and disclosure, transaction integrity, protection and privacy	Web trust, Financial Services Modernization Act (FSMA), Sarbanes Oxley Act (SOX 404 and 409), Verisign	TrustE, HIPAA Security Rule, HIPAA Privacy Rule

According to Barman (2002) organisations should explicitly inform consumers why personal information is collected and how it will be utilised. As Barman (2002) notes, information disclosure rights are usually the preserve of consumers who must grant permission to organisations when these seek to use or to share personal information with third parties.

GOVERNANCE AND PRIVACY OF MOBILE BANKING IN AFRICA

Mobile banking governance and privacy cannot be removed from the wider aspects of general organisational risk and security (Elliot & Phillips, 2004). In fact, some of the shortcomings of mobile banking privacy issues have become beneficial to white-collar perpetrators of crime. Against the backdrop of white-collar crime, the continent through its banks and telecoms companies continues to provide mobile banking and mobile money transfer services that have increased utility for the clients they serve.

In South Africa, among the services currently in operation are Nedbank's *M-PESA*™, Standard Bank's *Instant Money*™, FNB's *eWallet*™ and ABSA's *CashSend*™. While the mobile banking model in South Africa is primarily bank-led, telecom companies have generally been drivers on the African continent for mobile banking services such as Kenya Safaricom's ground-breaking *M-pesa*™. Celpay is another telecom company driving mobile banking initiatives in Zambia, Democratic Republic of Congo and soon in Tanzania (Mishra & Bisht, 2013).

Besides Safaricom's *M-pesa*™, Chege & Wepukhulu (2013) allude to mobile banking services in Kenya that are third-party-led. These include Airtel's *Zap*™ (now Airtel money), and *yuCash*™. Banks in Kenya have also teamed up with telecom companies to offer mobile banking services. Orange Telkom has partnered with Equity bank to offer *Iko Pesa*™ and Family bank has teamed up with Safaricom to offer *Pesa Pap*™.

While developed countries have adopted governance and regulatory mechanisms for mobile banking initiatives, the situation is quite different in African countries. Mobile banking initiatives on the continent have been marked by differences in approach towards governance, security and privacy. In South Africa, for instance, the Protection of Personal Information (POPI) Act (passed by the National Assembly in 2013), has amplified this debate and concern. The Act sets out conditions on how information should be processed by institutions that handle personal information. The POPI Act also recognises "the right to privacy" and "includes a right to protection against the unlawful collection, retention, dissemination and use of personal information" (Korb, 2013). Moreover, most banking institutions abide by the stipulated codes of banking practice 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 or not these clients maintain patronage with such banks (Korb, 2013).

In Kenya, Safaricom's entry into mobile banking through *M-pesa*™ was undertaken in the absence of legislation governing mobile payment systems, e-money, bank agents, consumer protection and anti-money laundering (CGAP, 2010). What followed from Kenya's *M-pesa*™ initiative was for legislators to initiate legislative changes that would accommodate regulatory requirements pertinent to mobile banking. These legislative initiatives included the 2009 amendment to the Banking Act 1991 to permit deposit-taking institutions to use agents. In addition, parliament passed the Anti-Money Laundering and Counter-Terrorism Financing Act 2009 (AML/CTF) (CGAP, 2010). At present, Kenya has no specific law or regulation that deals directly with issues of governance and privacy regarding e-money. As noted by CGAP (2010), the absence of any legal framework and the issuing of e-money by a licensed financial institution does not appear to raise issues with the Central Bank of Kenya (CBK).

In 2009, the Central Bank of Nigeria published its regulatory framework for mobile payment services that covered three specified models: bank focused, bank-led and third-party-led (Ayo & Ukpere, 2010). In sub-Saharan Africa, excluding South Africa, Nigeria is a leading light regarding mobile banking regulation (Ayo & Ukpere, 2010). Because of privacy and security concerns, analysts and stakeholders in Africa agree that there is a critical need to ensure that the mobile banking sector is well regulated (Ayo & Ukpere, 2010).

Across the continent, banks and governments must therefore address the potential threats to mobile banking, because of the need to protect the personal details and financial information of African consumers, which is critical to the success of mobile banking (McKnight, Choudhury & Kacmar, 2002). The playing field for mobile banking on the continent has not been comparable to South Africa's, where the country's tougher regulations have meant greater adherence to consumer protection against information security risks. In the absence of sound and clear regulatory frameworks that address privacy, security threats for African consumers are likely to be exacerbated.

There are three categories of security threats in mobile banking that are likely to affect mobile banking consumers on the African continent. These include 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 (Elliot & Phillips, 2004). 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 there are attempts to make mobile resources unavailable to intended users. It is usually perpetrated by hostile computers overloading the target mobile resources with unsolicited requests. Scholarly literature portrays justifiable concern by consumers of traditional banking services as hesitant to embrace the more current and innovative mobile banking services (McKnight, Choudhury & Kacmar 2002).

Such concerns may be due to fear that banks and other financial institutions may not provide adequate assurance regarding protection of their personal details on mobile platforms. The uncertainty associated with privacy and security risk in mobile banking services, coupled with the innate attractiveness (utility) of mobile banking convenience results in situations where consumers engage in calculated trade-offs between the perceived utility and perceived risks of mobile technology.

APPLYING THE THEORY OF RATIONAL CHOICE

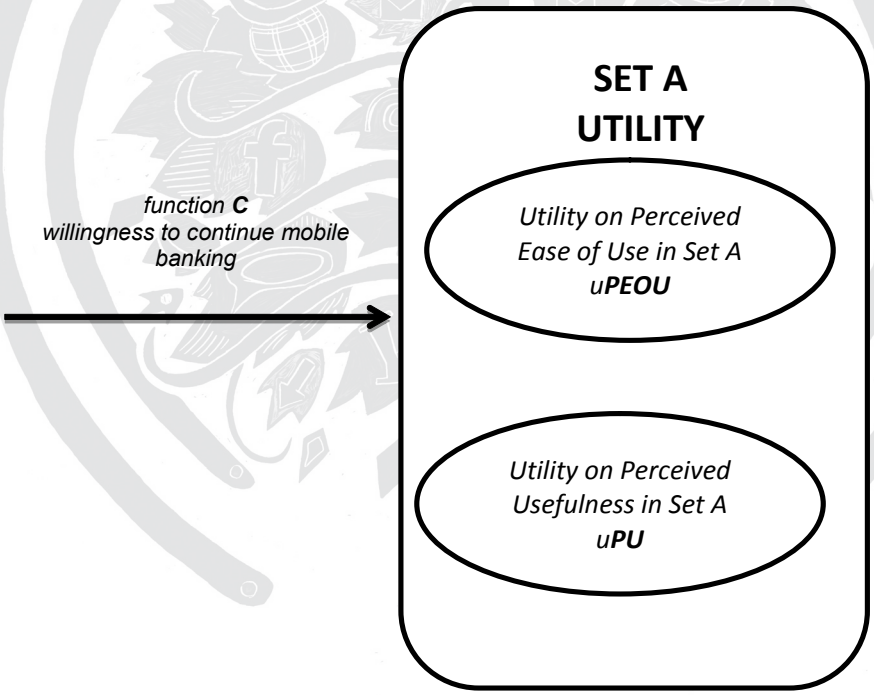
Rational choice theory (RCT) is an approach that seeks to explain choice by making certain assumptions about what motivates individual action (Bridge, 2009). RCT describes the choices (optimise/maximise utility) made by individuals as an optimisation and maximisation process. The assumption in the case of banked clientele deciding to subscribe to mobile banking services is that those individuals have certain preferences towards mobile services (utility) and that they act in a consistent way to get the most of what they require from those services (optimise/maximise utility). The hypothesis for this study is that in the process of maximising utility from mobile banking services, banking consumers are invariably willing to disclose personal information and forgo concerns regarding privacy and security whenever the perceived benefits (ie utility of ease of use, high network availability, etc) outweigh the perceived potential privacy risk.

A related concept to rational choice theory (RCT) is the technology acceptance model (TAM). While RCT attempts to share insights on the process of optimising and maximising utility of a technology, TAM provides insight on external variables that largely influence clientele's decision on whether or not personal information is at risk (Park, 2009). TAM is characterised by variables that are fundamental building blocks for RCT. These two variables are utility derived from *"Perceived Ease of Use"* **(uPEOU)** and *"Perceived Usefulness"* **(uPU)** of a technology (Legris, Ingham, & Collerette, 2003; Pai & Huang, 2011; Turner, Kitchenham, Brereton, Charters & Budgen, 2010). The utility of PEOU refers to the satisfaction a consumer gets by spending the least amount of effort to utilise a system or service. TAM hypothesises that the less effort taken to utilise a specific technology, the higher the utility and PEOU. The likelihood then is that the consumer will perceive the proposed technological service as beneficial. This will in turn influence the consumer's choice towards a specific technology or service (Venkatesh, 2000).

The second TAM factor, utility on PU, refers to whether or not the consumer believes that utilising mobile banking technology will increase the consumer's productivity. 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 (*rational choice*) and disclosure of private information as a trade-off towards utilising the technology.

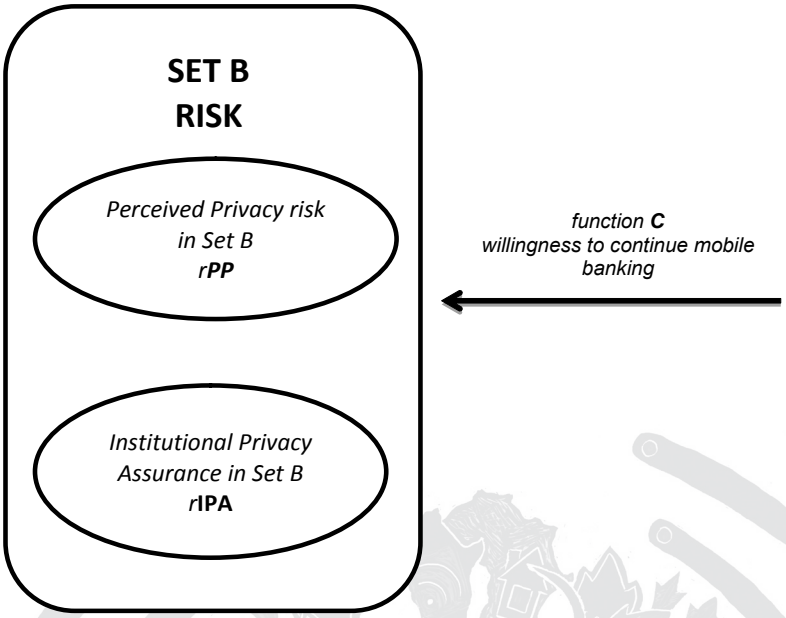
A key property of *rational choice* as explained in the previous discourse is attributed to what Miljkovic (2005) calls *consistency* of reason and is explained as follows: Consider a bank client's behaviour regarding what influences mobile banking *choice* (in Set A) by analysing subsets of the set A (influencing variables uPEOU and uPU), as described by a function C whose domain is the set of all subsets of A and whose range is the set A. This can be denoted by Figure 1 below.

FIGURE 1: UTILITY SET AND SUB-SET



From Figure 1, the element *choice* for Set A, *utility*, denoted as $C(A_1)$, is interpreted as the bank client's choice whenever she/he confronts the decision problem A. For every A, $C(A_1) \in A$. It is said that the (rational) client's behaviour function C satisfies the consistency condition if for all A1 u***PEOU*** $\subseteq A_2$ u***PU*** $\subseteq A$, if $C(A_2) \in A_1$ then $C(A_1$,u***PEOU***$) = C(A_2$, u***PU***$)$. In other words, if the element chosen from the large set (A) is a member of the smaller set (A_1), then the decisionmaker chooses this element from the smaller set as well. The same reasoning can be applied on the choice regarding risk, with the element choice for Set B risk, denoted as $C(B_1)$ and is interpreted as the client's choice to take risk whenever confronted by a decision problem B. For every B, $C(B_1) \in B$. The set B could include sub-set B_1 *Perceived Privacy risk* (r**PP**) and B2, *Institutional Privacy Assurance* (r***IPA***) as other variables that influence choice C such that B_1 r**PP** $\subseteq B_2$ r**IPA** $\subseteq B$, if $C(B_2) \in B_1$ then $C(B_1$,r**PP**$) = C(B_2$, r**IPA**$)$.This can be denoted by Figure 2 below.

FIGURE 2: RISK SET AND SUB SET



THE CONSTRUCTS

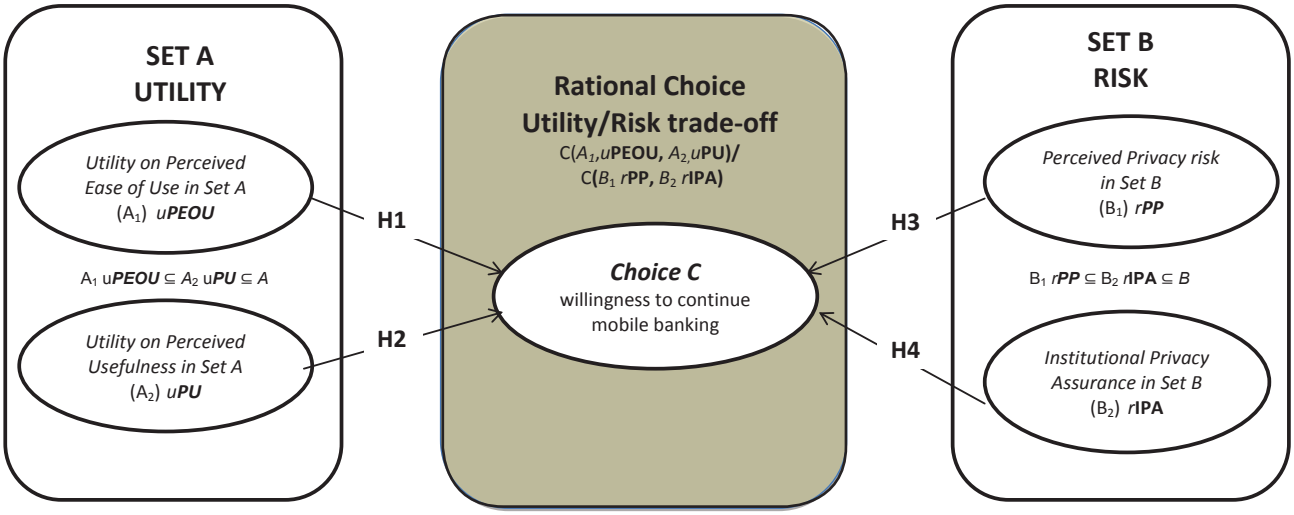
Based on the previous discussions, RCT identifies the choice C that a bank client makes regarding the utility/risk tradeoff, C(A_1,*u***PEOU**, A_2, *u***PU**)/ C(B_1 *r***PP**, B_2 *r***IPA**). The following constructs have been used to examine the risk/ utility tradeoff as follows;

- *Utility on Perceived Ease of Use* (*u***PEOU**)
- *Utility on Perceived Usefulness* (*u***PU**)
- *Institutional Privacy Assurance Risks* (*r***IPA**)
- *Perceived Privacy Risks* (*r***PP**)

On the basis of the above four variables, a framework for testing the utility/risk tradeoff can be developed using the following hypotheses:

H1: uPEOU will positively influence trusting intention, C.
H2: uPU will positively influence trusting intention, C.
H3: rPP will negatively influence trusting intention, C.
H4: rIPA will negatively influence trusting intention, C.

FIGURE 3: RATIONAL CHOICE CONCEPTUAL MODEL FOR UTILITY/ RISK TRADEOFF



The research work therefore set out to test the above framework regarding the *choice* C underlying C(A_1,*u***PEOU**, A_2, *u***PU**)/ C(B_1 *r***PP**, B_2 *r***IPA**) for a South African mobile banking consumer. The next section outlines the methodology and methods used to test the above hypotheses.

METHODOLOGY

This research was quantitative in approach as it sought to understand "how", not "why", consumers respond to choice. This enquiry is useful because it enables an understanding of why firms and governments should address issues of risk in mobile banking.

South Africa is appropriate as a study country because a survey of five provinces offers an opportunity to understand the choices of consumers in highly urbanised "city" environments and in more provincial environments. Thus the survey results reveal insights into a cross-section of mobile banking consumers. Three hundred and fifty questionnaires were distributed across seven cities in five provinces of South Africa. These cities were selected because of diversity in the banking clients' cultural, demographic and biographic characteristics. The provinces were KwaZulu-Natal, Gauteng, Mpumalanga, North West Province and Limpopo. Each province was allocated 50 questionnaires. Two hundred and nine questionnaires were completed successfully, a success rate of 59.7%.

Table 2 below provides a summary of the provinces that had the highest response rates to the questionnaire. The Zululand District of KwaZulu-Natal had the highest response rate (peri-urban), followed jointly by Gauteng's Sandton (city) and KwaZulu-Natal's Durban (city). Mpumalanga's White River is fourth (peri-urban), Gauteng's Auckland Park fifth (city), while North West's Kimberley (large town) and Limpopo's Polokwane (large town) are sixth and seventh respectively.

TABLE 2: SURVEY LOCATIONS

	Response rates from provinces			
	Location	Frequency	Valid %	Cumulative %
Valid	Zululand	46	22.0	22.0
	Sandton	39	18.7	40.7
	Durban	39	18.7	59.4
	White River	38	18.2	77.6
	Auckland Park	23	11.0	88.6
	Kimberley	14	6.7	95.3
	Polokwane	10	4.7	100.0
	Total	**209**	**100.0**	

The study surveyed respondents using a questionnaire based on a five-point Likert scale (see Appendix) that was developed to enable a rigorous understanding of consumer choice. The researcher statistically scrutinised *choice* and the decision process of a sample of mobile consumers who were already using basic features of smart phone applications such as online streaming of media content, social media and email and had started using mobile banking applications. To achieve this purpose, the questionnaires targeted users who had started using mobile banking applications. The quantitative research questions were relationship type questions, the aim being to investigate groups, associations or causal relationships between two or more variables. This particular study was aimed at examining the *choice* of actual consumers of a mobile banking service and its influence on their *willingness to continue* using mobile banking services.

For purposes of this research, purposive, non-probability sampling was chosen as the appropriate sampling method that best fits the requirements (Adler & Clark, 2008; Agarwal, 2005), see Table 3 below. The sample comprises bank clients of the four largest South African banks (FNB, ABSA, Nedbank, and Standard Bank). A filter question in the questionnaire was used to determine this.

TABLE 3. SAMPLING PROCESS

Sampling	Examples
Non-probability sampling	General profile of South Africans
Purposive sampling	Banking clients of South Africa

TABLE 4. RELIABILITY

Reliability statistics		
Construct	Cronbach's Alpha	Number of items
Perceived Ease of Use (uPEOU)	.796	15
Perceived Usefulness (uPU)	.825	15
Perceived Privacy Risks (rPP)	.900	18
Institutional Privacy Assurance (rIPA)	.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.

RESULTS AND DISCUSSION

It was imperative that the correct respondents were identified, hence a set of prerequisite questions were provided. 26.3% of respondents had been bank account holders in the previous five years, while the majority or 73.7% were bank account holders at the time of the survey. The composition of the study population of 209 was mainly in the age groups 21-49 years (76.6%), generically black[1] (86.1%), employed or self-employed (71.6%)

Hypothesis testing revealed the following:

UTILITY: PERCEIVED EASE OF USE AND PERCEIVED USEFULNESS

This section revisits the hypothesis **H1:** *u*PEOU and *u*PU will positively influence *choice C*. A correlation test was conducted in order to establish the relationship between the independent variables uPEOU/uPU *Perceived Ease of Use/ Perceived Usefulness*) and the dependent variable C (*Willingness to Continue Subscribing*). The purpose was to determine the *Pearson correlation coefficient* (two-tailed test) using SPSS. The SPSS output provided a matrix shown as Table 5 below.

TABLE 5: CORRELATION BETWEEN C AND UPEOU/UPU

		C	uPEOU	uPU
		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				

1 In South Africa, generically black means Black, Coloured and Indian/Asian

Data analysis shows that *u*PEOU and *u*PU positively influence C with a Pearson correlation coefficient of *r* = **.269** and **.144** respectively. The Significance Value for *u*PEOU is less than **.001** (as indicated by the double asterisk (**) 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 *u*PEOU will positively influence C, 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 *u*PU is related to willingness to subscribe C.

We may reject the null hypothesis.

PERCEIVED PRIVACY RISK

This section revisits the hypothesis: **H3**- *r*PP (Perceived Privacy Risk) will negatively influence C. The SPSS output provided a matrix shown as **Table 6** below. Data analysis show that two constructs used for *r*PP are both negatively related to C (weak relationship) with a Person correlation coefficient of *r* = -.**204**** and **-.048** respectively.

TABLE 6: CORRELATION BETWEEN RPP AND C

		C	rPP	rPP
		Banking and file sharing	Mobile banking applications inform subscribers 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 inform subscribers 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 variable, consumer choice C, is dependent on South African banking institutions intervening by providing reassurance to consumers regarding security risk. There is a very weak relationship (*r* = **-.048**, significant at **p = .490**), meaning that we cannot conclusively state that risk has an influence on a consumer's choice on continued use of mobile banking services even though they could be aware of such risk. This is because the **p** value is not significant (**p =.490**).

INSTITUTIONAL PRIVACY ASSURANCE

This section revisits the hypothesis: **H4:** *r*IPA (*Institutional Privacy Assurance*) will negatively influence C. The SPSS output provided a matrix shown as **Table 7** below. Data analysis shows that two constructs used for rIPA are both negatively related to C with a Person correlation coefficient of r = **-.056** and **-.007** respectively.

TABLE 7: CORRELATION BETWEEN C AND RIPA

		C	rIPA	rIPA
		Banking and file sharing	I am satisfied with my bank's mobile banking application privacy policy	My bank 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 bank 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				

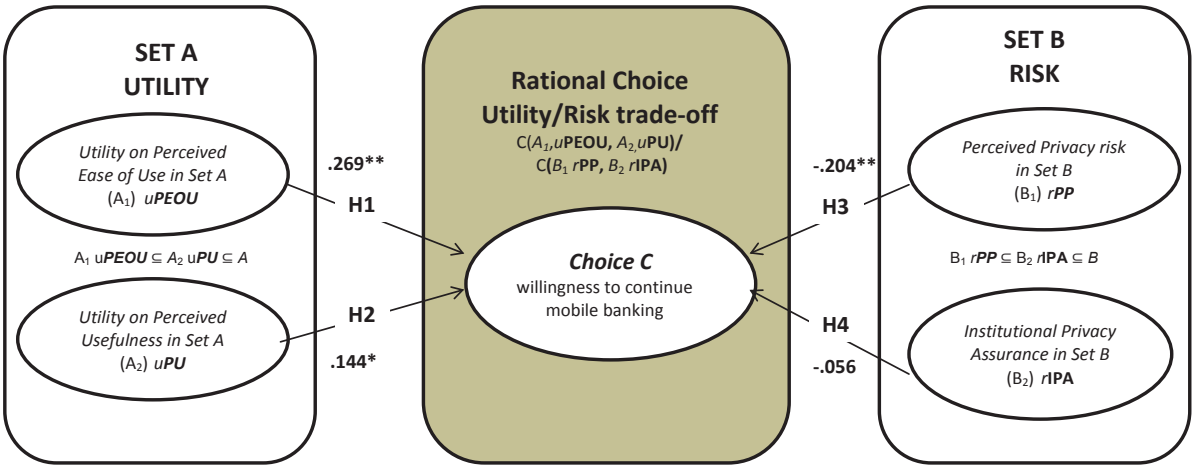
The data shows weak relationships and that institutional privacy assurance (rIPA) most likely affects the consumer's choice, but not as strongly as originally envisaged. According to data, the role of banks in providing assurance and maintaining obligations (or lack thereof) towards the privacy of client's personal information has not been significant.

REVISITING THE RATIONAL CHOICE MODEL FOR MOBILE BANKING UTILITY AND RISK

Based on empirical data we revisit and populate the model Figure 2, now shown as Figure 4: South African mobile banking consumer choice is influenced more by the perceived ease of use (u*PEOU*) of a technology (r = .**269****) than by perceived risk (r*PP*) (r = -.**204****). According to this study, the u*PEOU* variable has the most significant influence over all other variables when determining whether or not a consumer would continue subscribing to mobile banking services.

This is significant because it shows how mobile banking technology and services are currently perceived. The South African consumer (21-49, generically black, employed or self-employed) will forgo concerns about privacy and security in favour of utility. In banking contexts, this is a potentially significant insight for banking institutions, particularly if consumers exhibit this behaviour *after they start using mobile banking services*. The results can be interpreted to mean that once mobile banking is initiated, risk would not constitute a significant deterrent.

FIGURE 4: RATIONAL CHOICE CONCEPTUAL MODEL SHOWING EMPIRICAL RELATIONSHIPS



Drawing on the insights from rational choice theory this work provides empirical evidence of a weak relationship between consumers' perceived privacy risk (*r*PP) and their willingness to continue to subscribe (C). This is an interesting finding because it shows that consumers' understanding of privacy and security may not dampen their willingness to use Internet banking when there is perceived technological utility. Empirical data shows that uPEOU has a much stronger relationship with C than all other variables. It follows then that this is the rational choice explicated in this study. While South Africa was the study country, the results may have broader applicability, as the sample included a cross-section of the population according to geo-economic context (city, peri-urban, town), age, race and employment status.

IMPLICATIONS OF STUDY FOR INDUSTRY

Financial institutions should be aware that consumers of mobile banking will make choices that are not static. Dynamism in choices will depend on the following variables that are likely to shape perception of utility for mobile banking depending on whether consumers will gain or not at any point in time. These variables will include how utility (as opposed to risk) is framed, anchored, endowed and fair (Yang & Lester, 2008).

At present, the study has shown that the average consumer is willing to continue to subscribe (*choice* C) as long as there is perceived usefulness of the technology. A strong mobile banking brand must effectively portray utility and trust, while addressing risk, thus strengthening choice. Banks and the mobile telecommunications industry must build a clear brand that aims towards consolidating risk assurance and utility for consumers. Strong branding should be supported by continuous innovation in security standards and analysis of emergent security risks.

IMPLICATIONS FOR THEORY

This limited study contributed toward the construction of a broader knowledge base for understanding the choice of banking consumers to continue to use mobile banking. From a consumer perspective, the use of rational choice theory offers a way of conceptualising the choice made by a banked consumer. The study highlights the idea that privacy (and security risk) should not be looked at in isolation from other variables such as utility of technology. Significantly, according to the findings of this study, utility may at times override privacy and security concerns. This should be of concern to practitioners of data and information security, particularly if dynamics of utility variables keep changing in the context of transition to a digital banking and financial system. Greater investment is required in research and development (R&D) for information security products and services as the digital era advances, including on the African continent where R&D investment is meagre.

LIMITATIONS OF STUDY

One of the main limitations of this study is the notion that decisions are always rational. Other studies that show that this is not always the case include work by Yang & Lester (2008), who have philosophised about the existence of irrational behavior and argue that decisionmakers may not always optimise computational power in pursuit of maximising expected utility. Furthermore, in order to understand the decisionmaking process and choice of decisionmakers, qualitative approaches would be more appropriate to extract the reasons behind consumer choice.

CONCLUSION

The article examined consumer choice and the willingness of consumers to continue subscribing to mobile banking services. Indeed, increased mobile banking and mobile money transfer revenues across the continent (Toyama, 2009; Mishra & Bisht, 2013) suggest that these are common choices. The empirical results reveal that while theory may emphasise risk, perceived utility was noted as the overriding factor that influenced willingness to continue using mobile banking. At this stage it may be difficult to tell whether experience and familiarity with applications similar to mobile banking service applications played a catalysing role in influencing choice. Future research can consider the plausibility of other factors that influence choice in subscribing to mobile banking services.

Finally, as discussed above, it is disturbing that mobile banking consumers are paying less attention to risk. More needs to be done to raise awareness of security concerns and to build innovation capability in the field of information security for mobile banking and mobile money.

REFERENCES

Adler, E. & Clark, R. (2008). How it's done: *An invitation to social research*, 3rd edition. Thomson, California.

Agarwal, B. (2005). *Programmed statistics: Question-answers*, 3rd edition. New Age International, New Delhi.

Ayo C. & Ukpere W. (2010). Design of a secure unified e-payment system in Nigeria: A case study. *African Journal of Business Management* 4(9) pp. 1753-1760.

Barman, S. (2002). *Writing Information Security Policies*. New Riders, Indiana.

Bridge G. (2009). Rational choice theory and rational choice Marxism, *International Encyclopedia of Human Geography,* pp. 100-106.

Cate, F. (1997). Privacy in the information age. The Brookings Institution, Washington.

CGAP (2010). Update on Regulation of Branchless Banking in Kenya. CGAP.org. Retrieved 16 November 2013 from http://www.cgap.org/sites/default/files/CGAP-Regulation-of-Branchless-Banking-in-Kenya-Jan-2010.pdf.

Chege, F. & Wepukhulu, J. (2013). The effect of mobile money transfer on working capital management: A case of debt collection at NAWASSCO. *Research Journal of Finance and Accounting*, 4(14) pp 66-71.

De Vaus, D. (2002). *Analyzing social science data: 50 key problems in data analysis*. Sage, London.

Elliot, G. & Phillips, N. (2004). Mobile commerce and wireless computing systems. Pearson, Harlow.

Essegbey, G. & Frempong G. (2011). Creating space for innovation: The case of mobile telephony in MSEs in Ghana, *Technovation*, 31 pp. 679-688.

Foster, J. (1998). Data analysis using SPSS for Windows: A beginner's guide. Sage, London.

Giordano, S. (2010). Applying information security and privacy principles to governance, risk management and compliance, SANS Institute InfoSec Reading Room, pp.1-32.

Gregory, R. (1996). *Psychological testing: History, principles and applications*, 2nd edition. Allyn & Bacon, Boston.

Huang, S., Shen, W., Yen, D. & Chou, L. (2011). IT governance: Objectives and assurances in Internet banking, *Advances in Accounting, incorporating Advances in International Accounting*, 27 pp.406-414.

Hu, W., Lee, C. & Kou, W. (2005). Advances in security and payment methods for mobile commerce. Idea Group Publishing, Hershey.

Husted, N., Saidi, H. & Gehani, A. (2011). Smartphone security limitations: Conflicting traditions, Proceedings of the 2011 Workshop on governance of technology, information and policies, ACM, New York.

Korb, B. (2013). Implementation of POPI Act means companies must secure their information. IT Governance and Risk Management, ITWeb, Retrieved 10 October 2013 from http://www.itweb.co.za/index.php?option=com_content&view=article&id=63461.

Legris, P., Ingham, J. & Collerette, P. (2003). Why do people use information technology? A critical review of the technology acceptance model. *Information & Management,* 40 pp. 191-204.

McKnight, D., Choudhury V. & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology, *Information Systems Research*, 13(3) pp. 334-359.

Miljkovic, D. (2005). Rational choice and irrational individuals or simply an irrational theory: A critical review of the hypothesis of perfect rationality. Journal of Socio-Economics, 34(5) pp. 621-634.

Mishra, V. & Bisht, S. (2013). Mobile banking in a developing economy: A customer-centric model for policy formulation. *Telecommunications Policy,* 37(6-7) pp. 503-514.

Pai, F. & Huang, K. (2011). Applying the technology acceptance model to the introduction of healthcare information systems. *Technological Forecasting & Social Change*, 78 pp. 650-660.

Park, S. (2009). An analysis of the technology acceptance model in understanding university students' behavioral intention to use e-learning. *Educational Technology & Society,* 12(3) pp. 150-162.

Shaw, P. (2001). *e-Business privacy and trust: Planning and management strategies*. John Wiley & Sons, New York.

Shen, Y., Huang C., Chu, C. & Hsu, C. (2010). A benefit-cost perspective of the consumer adoption of the mobile banking system. *Behavior & Information Technology*, 29(5) pp. 497-511.

Solovo, D., Rotenberg, M. & Schwartz, P. (2006). *Privacy, information, and technology*. Aspen Publishers, New York.

SouthAfrica.info (2012) South Africa banks go mobile. SouthAfrica.info, retrieved 10 Oct 2013 from http://www.southafrica.info/business/trends/newbusiness/mobile-banking-050412.htm.

Toyama, K. (2009). Mobile banking adoption and usage by low-literate, low income users in the developing world. *Journal of Internalization, Design and Global Development*, pp. 485-494.

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 pp. 463-479.

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) pp. 342-365.

Yang, B. & Lester, D. (2008). Reflections on rational choice: The existence of systematic irrationality. *The Journal of Socio-Economics*, 37(3) pp. 1218-1233.

Yoo, Y., Lee, J. & Rowley, C. (2008). *Trends in mobile technology and business in the Asia-Pacific region*. Chandos Publishing, Oxford.

APPENDIX: Survey Questionnaire

Section 1: Background Information

Location .....

1.1. Have you been an account holder of a South African bank?

Yes, I have been in the past five years	1
Yes, I currently am	2
No, I haven't been in the past five years	3

If you marked 1 or 2, then proceed to the questions below, or your participation in this questionnaire ends here. Thank you for participating.

1.2. Do you own a cellphone?

Yes	1
No	2

If you marked 1, then proceed to the questions below, or your participation in this questionnaire ends here. Thank you for participating.

1.3. Can your cellphone launch an Internet browser?

Yes	1
No	2
Not sure	3

If you marked 1 or 3, then proceed to the questions below, or your participation in this questionnaire ends here. Thank you for participating.

1.4. Have you used your cellphone's Internet to receive and perform any of the activities below? (Please indicate with an X where applicable)

RSS feeds	
Mobile banking	
Online streaming (ie audio, TV, Film, etc.)	
Downloads (ie Games, Music, etc.)	
Social networks (ie Facebook, Twitter, BBM, etc.)	
Email	
Modem & hotspot	
Content subscriptions (ie magazines, news, etc.)	
File sharing	
Other, please specify:	

Section 2: Biographic Information

This section of the questionnaire refers to background (biographical) information. Although we are aware of the sensitivity of the questions in this section, the information will allow us to compare groups of respondents. Once again, we assure you that your response will remain confidential and anonymous. Your cooperation is appreciated.

2.1. Gender

Male	1
Female	2

2.2. Age group

20 or younger	1
21 – 29	2
30 – 39	3
40 – 49	4
50 – 59	5
60 or older	6

2.3. Ethnicity

Black	1
Coloured	2
Indian or Asian	3
White	4

2.4. Marital status

Single	1
Married	2
Divorced	3
Living with partner	4
Widowed	5
Other, please specify:	6

2.5. Highest educational qualification achieved

Grade 11 or lower (Std 9 or lower)	1
Grade 12 (Matric, Std 10)	2
Post-matric diploma or certificate	3
Baccalaureate degree(s)	4
Post-Graduate degree(s)	5

2.6. How would you describe the area in which you are residing?

Urban	1
Rural	2

2.7. Size of your household, ie the number of people, including yourself, who live in your house/dwellings for at least three months of the year?

Live alone	1
2	2
3	3
4	4
5	5
6 or more	6

2.8. Employment status

Employed	1
Self-employed /independent consultant	2
Unemployed	3
Student	4
Other, please specify:	5

If you marked 1, 2 or 5, then proceed to the question below (2.9.), otherwise proceed to Section C.

2.9. Employment industry

Construction, trades & mining	1
Education and teaching	2
Banking & finance	3
Media	4
Automotive	5
Telecommunications	6
IT	7
Government	8
Non-governmental organisation	9
Consulting	10
Safety and security	11
Manufacturing & production	12
Legal	13
Property	14
Recruitment	15
Science & research	16
Sports & lifestyle	17
Travel, leisure & tourism	18
Aerospace & aviation	19
Customer service & call centre	20
Insurance	21
Retail & wholesale	22
Agriculture, fishing & forestry	23
Catering & hospitality	24

Fashion, art & design	25
Health, medicine & nursing	26
Marketing, advertising & PR	27
Oil, gas & alternative energy	28
Purchasing & supply chain	29
Sales	30
Social services	31
Transport & logistics	32
Installation, maintenance & repair	33
Warehousing & distribution	34
Other, please specify:	35

Section 3: Perceptions

Please note that every question in this section and sections to follow is associated with two scales: the first part seeks your level of agreement or disagreement towards the given statement; the second part aims to identify your level of importance towards the given statement.

3.1 Choice (please indicate by making an X in the relevant column)

Item code	Question	Current					Level of importance				
		Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Not important	Somewhat important	Neutral	Very important	Essential
C01	Mobile banking is important to my life	1	2	3	4	5	1	2	3	4	5
C02	I conduct and share personal banking information/files across my mobile device	1	2	3	4	5	1	2	3	4	5

Please note that every question in this section and sections to follow is associated with two scales: the first part seeks your level of agreement or disagreement towards the given statement; the second part aims to identify your level of importance towards the given statement.

4.1 Perceived ease of use (please indicate by making an X in the relevant column) (extract of actual)

Item code	Question	Current					Level of importance				
		Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Not important	Somewhat important	Neutral	Very important	Essential
PEOU01	Mobile banking applications are easy to install	1	2	3	4	5	1	2	3	4	5
PEOU02	I have never experienced timeouts with mobile banking applications.	1	2	3	4	5	1	2	3	4	5
PEOU03	Mobile banking applications allow conducting of banking at any time of the day.	1	2	3	4	5	1	2	3	4	5
PEOU04	Waiting period for authentication into mobile banking applications is short.	1	2	3	4	5	1	2	3	4	5
PEOU05	Doing banking using mobile banking applications is error-free.	1	2	3	4	5	1	2	3	4	5
PEOU06	Mobile banking applications' default screen lists types of banking transactions available.	1	2	3	4	5	1	2	3	4	5
PEOU07	Mobile banking applications offer helpful tips on banking using a mobile device.	1	2	3	4	5	1	2	3	4	5

4.2 Perceived usefulness (please indicate by making an X in the relevant column) (extract of actual)

Item code	Question	Current					Level of importance				
		Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Not important	Somewhat important	Neutral	Very important	Essential
PU01	Mobile banking applications allow for viewing of bank account statements.	1	2	3	4	5	1	2	3	4	5
PU02	Mobile banking applications help me avoid standing in long queues at the bank's branch.	1	2	3	4	5	1	2	3	4	5
PU03	Mobile banking applications allow for the purchases of prepaid airtime, electricity etc.	1	2	3	4	5	1	2	3	4	5
PU04	Mobile banking applications permits the making of payments.	1	2	3	4	5	1	2	3	4	5
PU05	Mobile banking applications are always operational.	1	2	3	4	5	1	2	3	4	5
PU06	Mobile banking applications permits the making cash transfers.	1	2	3	4	5	1	2	3	4	5

4.3 Perceived privacy risks (please indicate by making an X in the relevant column) (extract of actual)

Item Code	Question	Current					Level of importance				
		Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Not important	Somewhat important	Neutral	Very important	Essential
PP01	Mobile banking applications conceal subscriber's personal information.	1	2	3	4	5	1	2	3	4	5
PP02	Mobile banking applications do not store usage history without subscriber's knowing.	1	2	3	4	5	1	2	3	4	5
PP03	Mobile banking applications remove subscriber's browsing history upon log-out.	1	2	3	4	5	1	2	3	4	5
PP04	Mobile banking applications inform subscriber about ways of reinforcing security.	1	2	3	4	5	1	2	3	4	5
PP05	Mobile banking applications prevent the use of cookies to track subscriber's usage history.	1	2	3	4	5	1	2	3	4	5
PP06	Mobile banking applications prevent installation of add-on software that could compromise privacy information.	1	2	3	4	5	1	2	3	4	5
PP07	Mobile banking applications block installation of third party software that could compromise privacy information.	1	2	3	4	5	1	2	3	4	5
PP08	Mobile banking applications provide tips on security mechanisms' best practice.	1	2	3	4	5	1	2	3	4	5
PP09	Mobile banking applications suggest to the subscriber about necessary software upgrades.	1	2	3	4	5	1	2	3	4	5

4.4 Institutional privacy assurance (please indicate by making an X in the relevant column) (extract of actual)

Item code	Question	Current					Level of importance				
		Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Not important	Somewhat important	Neutral	Very important	Essential
IPA01	Mobile banking application protects the integrity of subscriber's personal information.	1	2	3	4	5	1	2	3	4	5
IPA02	I am aware of my bank's mobile banking applications privacy policy.	1	2	3	4	5	1	2	3	4	5
IPA03	My bank's mobile banking applications privacy policy is understandable.	1	2	3	4	5	1	2	3	4	5
IPA04	I am satisfied with my bank's mobile banking application privacy policy.	1	2	3	4	5	1	2	3	4	5
IPA05	I am pleased with my bank's mobile banking application information privacy assurance.	1	2	3	4	5	1	2	3	4	5
IPA06	My bank provides explanations for the collection of my personal information.	1	2	3	4	5	1	2	3	4	5
IPA07	I understand reasons behind collection of personal information by my bank.	1	2	3	4	5	1	2	3	4	5