Check for updates

Article

Understanding antecedents to perceived information risks: An empirical study of the Korean telecommunications market

Information Development
2016, Vol. 32(1) 91–106
© The Author(s) 2014
Reprints and permission:
sagepub.co.uk/journalsPermissions.nav
DOI: 10.1177/0266666913516884
idv.sagepub.com
SAGE

Christian Fernando Libaque-Sáenz
Korea Advanced Institute of Science and Technology (KAIST)

Siew Fan Wong
Sunway University, Malaysia

Younghoon Chang
Korea Advanced Institute of Science and Technology (KAIST)

Young Wook Ha
Korea Advanced Institute of Science and Technology (KAIST)

Myeong-Cheol Park
Korea Advanced Institute of Science and Technology (KAIST)

Abstract

With increasing usage of electronic devices, people are creating digital footprints of their everyday actions. These footprints come in the form of big data, and can provide useful insights into customer preferences, thus enabling companies to gain business benefits. However, customers may perceive usage of their personal information as a threat. The telecommunications sector is facing this issue. It is capable of collecting huge amount of data due to wide usage of smartphones and mobile Internet. Yet, it is unable to capitalize on these data. To manage customer perception of information risks in giving telecommunications companies permission to use their personal information, this study examines factors that influence customers' risk perception. A survey of 512 Internet panel members in Korea shows that information practices play an important role in shaping information privacy concerns, trust, and perceived information risks. Information privacy concern is the strongest predictor of perceived information risks, followed by perceived data control, and trust. Perceived policy awareness and perceived information protection significantly influence perceived data control. The findings imply that telecommunications companies ought to increase the level of customer trust, improve their information practices, and reduce customers' information privacy concerns if they want to lower customer perception toward information risks.

Keywords

perceived information risk, information privacy concerns, information practices, trust, personal information, telecommunications market, Korea

Clear policies will assure consumers that companies are responsible in safeguarding their personal information.

Introduction

Information technologies (ITs) have changed how we communicate, interact with others, read, write, and in general, how we react to things. The Internet is a good example, where we use it for various purposes such as banking, searching, social networking, buying and

Corresponding author:
Younghoon Chang, Korea Advanced Institute of Science and Technology (KAIST) – Department of Management Science, #5108, N22 Alumni Building, Guseong-dong Yuseong Daejeon 305701, Republic of Korea. T: 0423506333 F: 0423506339.
Email: younghoonchang@kaist.ac.kr

selling products, and for entertainment. As we use the Internet, we are creating digital footprints of our everyday activities (Girardin et al., 2008). This trend is known as big data and it is characterized by three features: volume (i.e., huge amount of data), velocity (i.e., speed of data creation), and variety (i.e., variety of sources) (McAfee and Brynjolfsson, 2012).

The value of big data lies in the information that could be obtained from the analysis of individual information. For example, companies do not have to wait for months to obtain data from the field as they used to do. With IT, companies can obtain highly accurate data in real time, and thus improve decision-making through constant business experimentation, test of new products and business models, and innovation in customer experience (McAfee and Brynjolfsson, 2012; Davenport et al., 2010). Moreover, companies would be able to minimize costs, improve customer satisfaction, and create new products and services (Brown et al., 2011; McGuire et al., 2012).

However, the Internet and the associated data collection activities bring not only benefits to society but also concerns and threats. Topping the threat list is privacy concerns due to sensitivity of personal data (TRUSTe, 2011). Individuals are uncomfortable with their personal data being collected because of potential risks such as intrusion, public disclosure of embarrassing private facts, false light, and appropriation (Prosser, 1960). Governments have attempted to protect consumer privacy by enacting laws such as the Directive EC 95/461995 issued by the European Union, where it states that an unambiguous consent from consumers is needed for legitimate personal data usage (EC_95/461995, 1995).

The telecommunications sector represents well this phenomenon of consumer privacy concerns. First, the sector captures varieties of voluminous data at a very fast pace through customers' daily usage activities. Wide adoption of smartphones and mobile Internet further catalyzes significant increase in data traffic (Banerjee, 2011). If properly used, telecommunication companies (telcos) could leverage on consumer data for business benefits (Columbus, 2012; Sheina and Bali, 2012).While having the advantage of big data access, the telecommunications sector is a highly regulated industry where companies must follow established information privacy laws. This limits the usage of customer data without permission.

To obtain customer permission, telcos have to manage customer perception of risks associated with giving the companies permission to use personal data. Perception of risks is a prominent antecedent to privacy-related behavioral intentions (Jarvenpaa et al., 2000; Lee, 2009; Li et al., 2010; Malhotra et al., 2004; Pavlou, 2003; Van Slyke et al., 2006). Most existing studies in the privacy domain focus on the factors affecting intentions to carry out behaviors related to disclosure of personal information in various domains such as e-commerce, the Internet, online banking, and offline commerce (see Appendix A). To the best of our knowledge, no study has dissected perceived risks to understand the factors that contribute to increased perceived risks, and examined how information practices relate to perceived risks.

The objective of this study is, therefore, to explore relevant factors that could be managed to reduce the perception of risks in privacy situations within the telecommunications sector. It is expected that the results will shed light on the importance of information privacy concerns, trust, and information practices as antecedents to perceived information risks. Telcos could then manage these factors to reduce customer perception of risks in privacy-disclosure situations, and potentially leverage on their access to big customer data.

The paper proceeds as follows: the next section describes the context of the South Korean telecommunications market and provides a literature review on perceived information risks, trust, and information practices. The following section proposes the hypotheses and presents the research model. The next two sections present the research methodology and the results. The final section discusses the findings and implications, identifies the limitations, and proposes future research avenues.

Theoretical backgrounds

South Korean telecommunications market: Current situation and personal information protection

As stated before, the Korean telecommunications sector, more specifically its mobile telephone market, is selected for this study as it represents well an industry that holds large amounts of sensitive personal data in terms of volume, velocity, and variety. Currently, the Korean mobile telephone market has a penetration rate of 108%, representing around 53.8 million subscribers (KCC, 2013). These subscriptions are split among three operators: SK Telecom, KT, and LG U+ with 50.2%, 30.5%, and 19.2% of the market share respectively (KCC, 2013).

The Korean telecommunications market is very competitive. Its mobile telecommunications services had experienced a high growth rate until it attained maturity at the beginning of the present millennium (Kim et al., 2004). It took just four years, from 2009, for smartphone users to reach 64% of the total mobile users (KCC, 2013). LTE service, which started in 2011 has already reached one-third of the total mobile subscribers. Korean telcos are leading the market in terms of innovation. For instance, SKT and KT have started to adopt new communications convergence models by converging and developing new businesses. This change includes the development of services and platforms related to big data and content business (ET News, 2012a, 2012b, 2013).

To ensure successful deployment of these new business models, telcos need to overcome the challenges where the models require the processing of customers' personal information. Typically, Korean telcos collect information on their customers during the sign-up process and during the installation and usage of applications (Park, 2011). This information not only includes basic information to identify subscribers, but also information generated and collected through service processes, which could potentially touch on privacy laws. In other words, since Korean telcos are collecting huge amount and varieties of personal information, they are constrained by regulations such as the Korean Privacy Act, the Korean Data Communication Network Act, and the Korean Location Information Act (Park, 2011). In short, before using customers' personal information, Korean telcos must gain consent from their customers.

Perceived information risks

Perceived information risk is individuals' beliefs regarding potential loss associated with giving third parties permission to use their personal information (Dowling and Staelin, 1994; Malhotra et al., 2004). Prior studies in the privacy domain mostly focused on the factors affecting privacy-related behavioral intentions. The results showed that perception of risks is an important antecedent to intention. For example, Jarvenpaa et al. (2000) conducted a research on intention to purchase from Internet stores and found that risk beliefs have both a direct and an indirect significant effect on willingness to buy. In studying intentions to use online banking, Lee (2009) found that different types of risks such as performance, social, time, financial, and security risks significantly affect behavioral intention. Additionally, both Li et al. (2010) and Malhotra et al. (2004) conducted research on intention to disclose personal information through the Internet and found support for a significant effect of risk perceptions on behavioral intention. Pavlou (2003) and Van Slyke et al. (2006) studied the antecedents to intention to transact on the Internet. Both studies found that risk belief has a significant effect on privacy-related behavioral intention. Therefore, given the importance of risk perceptions in the privacy domain, and considering that no study has examined this construct in the context of the telecommunications industry, this study attempts to focus on identifying factors that contribute to perceived information risks.

Trust

According to Pavlou and Fygenson (2006), trust is individuals' beliefs that a company (i.e., a third party) will act according to their expectations without exploiting their vulnerabilities. According to Gefen et al. (2003), trust is made of three dimensions: competence, which refers to individuals' perceptions that the trustee has the ability to perform up to their expectations; integrity, which refers to individuals' perceptions that the trustee will be honest; and benevolence, which refers to the individuals' perceptions that the trustee will not act in an opportunistic manner. Trust is important because it reduces one's perception of risks associated with opportunistic behaviors by the trustee (Ganesan, 1994).

Many studies have examined the relationship between trust and risk beliefs and found support for the relationship (Dinev and Hart, 2006; Jarvenpaa et al., 2000; Malhotra et al., 2004; Norberg et al., 2007; Pavlou, 2003). For example, Dinev and Hart's (2006) work on individuals' intention to provide personal information to complete transactions on the Internet highlighted a direct negative effect of perceived Internet privacy risks on Internet trust. Similarly, Malhotra et al.'s (2004) study on individuals' intention to give personal information through the Internet found a direct negative effect of trusting beliefs on risk beliefs. On the other hand, in examining offline disclosure of personal information, Norberg et al. (2007) found the existence of a paradox between behavioral intention and actual behavior, where risk perception is the main antecedent to the former while trust is the main antecedent to the latter.

Although the relationship between trust and risk beliefs has been widely studied in the e-commerce

and Internet domains (see Appendix A), we are not aware of any other studies that have addressed this relationship in the mobile communication context within the telecommunications sector. Furthermore, as evident from previous research, the strength of this relationship may vary according to the contexts (Xu et al., 2011). Hence, this study will treat trust as one of the main antecedents to our dependent variable (i.e., perceived information risks) in an attempt to shed light on this relationship in a new context – the telecommunications sector.

Information privacy concerns

Another widely studied relationship is the one between privacy concerns and risk perceptions (see Appendix A). Privacy concern refers to individuals' level of anxiety regarding a third party's information practices (Smith et al., 1996). Prior research provides support for a strong link between privacy concerns and risk perceptions (Dinev and Hart, 2006; Malhotra et al., 2004; Van Slyke et al., 2006; Xu et al., 2011). Xu et al. (2011) examined the effect of institutional privacy assurances on privacy concerns in four domains: e-commerce, social networking, finance, and healthcare. They found that each context differs significantly from the others in terms of the information type, and the strength of relationship between privacy concerns and risk beliefs. Therefore, there is the need to examine the nature of the relationship within the telecommunications sector.

Information practices

Information practices refer to the strategies for collecting and using personal information by data holders (Culnan and Armstrong, 1999). Information practices have four dimensions: access, choice, notice, and security (Liu et al., 2004). Access refers to the possibility of accessing stored personal information by customers; choice refers to customer decision on which information can be used by data holders; notice is the disclosure of information practices to customers; and security refers to the assurances for keeping personal information secure (Liu et al., 2004).

When further examining the four dimensions, it is clear that access is related to choice. In fact, it is a precondition to choice. In other words, we cannot make a choice on which personal information could be used by data holders if we do not have access to the data they store. Previous research has combined both access and choice into one construct. For example, Westin (1967: page 7) defined privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." Clearly, Westin's definition includes both access and choice.

As for the dimension of notice, Malhotra et al. (2004) operationalized it through awareness of privacy practices. Awareness of privacy practices refers to the level to which consumers are informed about the company's intended use of personal information. In terms of security, the literature (Li et al., 2010; Pavlou and Fygenson, 2006) operationalized it using perception of information protection. Putting together the constructs, perceived policy awareness and perceived information protection, we have the concept of proxy control. Proxy control is defined as individuals' attempt to align themselves with a powerful force or powerful others to gain control (Yamaguchi, 2001). Control agency theory postulates that, depending on the control agent, control could be divided into two categories: self agency, where the control is exerted by one's own self; and proxy agency, where the control is exerted by powerful others (Xu et al., 2012). In addition, control literature also posits that, in environments where people lack skills, resources or power to achieve desired outcomes, they are motivated to rely on proxy control (Yamaguchi, 2001). Bandura (2001) and Yamaguchi (2001) claimed that having proxy control could increase the perception of self-control.

A few studies have addressed perception of information practices as antecedent to trust and privacy concerns. Culnan and Armstrong (1999) examined the role of fair information practices in reducing customers' privacy concerns using an experimental approach with discriminant analysis technique and secondary data with items measuring proxy privacy concerns. Although their work provided useful insights into the importance of using fair information practices, it failed to support causality. Furthermore, their usage of only secondary data is another limitation of the study. Liu et al. (2004) employed a laboratory experiment methodology to research on factors affecting individuals' intention to disclose personal information in e-commerce transactions and found a significant correlation between the perception of each dimension of information practices – notice, access, choice, and security – and trust. However, causality could not be established with certainty (Liu et al., 2004). Chellappa and Pavlou (2002) and Suh and Han (2003) found the existence of a relationship between perceived security

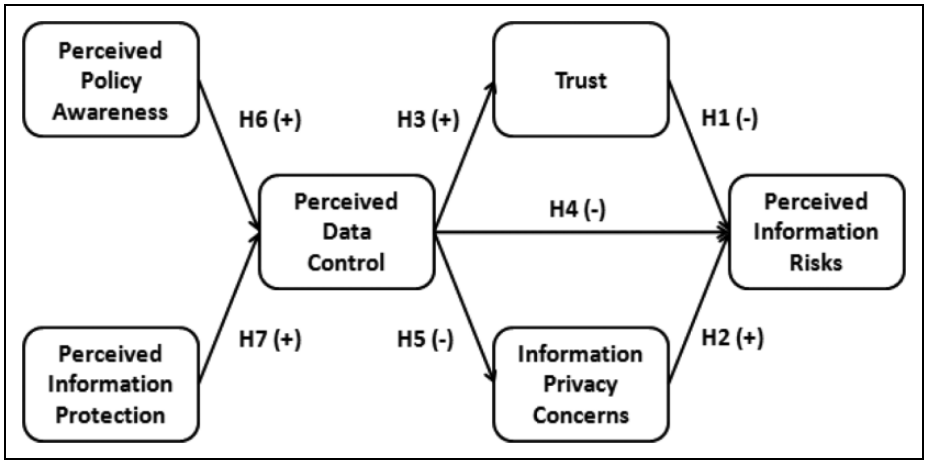


Figure 1. Research Model.

and trust when investigating e-commerce and online banking transactions respectively.

In short, prior research has empirically validated the effect of perceived information practices on privacy concerns and trust, and the relationship between these last two variables and perceived information risks. However, these studies have not examined all dimensions of information practices when studying perceived information risks. Furthermore, we know of no studies that address the effect of perceived information practices on information privacy concerns and trust simultaneously. This present research attempts to fill these gaps.

Research model and hypotheses

We argue that risk beliefs could be affected by privacy concerns, trust, and information practices. We define our dependent variable, perceived information risks (PIR) as individual's beliefs regarding potential loss associated with giving telcos permission to use personal information. Our research model is illustrated in Figure 1 while the following discusses the hypotheses.

Trust (TRU)

Using Pavlou and Fygenson (2006)'s definition of trust, we define this variable as individuals' beliefs that telcos will act according to their expectations without exploiting their vulnerabilities. To gain consumer confidence, telcos need gain trust of their consumers that if consumers were to allow telcos to access their personal information, these information will be safe and will not be exploited. Once such trust is being developed, consumers will have lower level of risk perception toward telcos. Accordingly, we hypothesize a direct negative relationship between trust and perceived information risks. This hypothesis is supported by trust-risk literature (Gefen, 2000; Gefen et al., 2003) and by prior empirical findings (Jarvenpaa et al., 2000; Malhotra et al., 2004; Siegrist et al., 2005; Van Slyke et al., 2006).

> **H1:** Trust negatively influences perceived information risks

Information privacy concerns (CON)

Following Smith et al. (1996)'s definition of privacy concerns, we define this variable as individuals' level of anxiety regarding telcos' information practices. Anxiety is a mood (Segerstrom et al., 2000). According to mood congruency effect described in psychology literature, the perception of anxious people is often distorted toward greater negativity (Raghunathan and Pham, 1999). In this context, since perceived information risk is a potential loss, i.e., a negative outcome, we postulate that anxious people will tend to perceive higher potential risks compared to non-anxious people (Mathews, 1990). Thus, we hypothesize that information privacy concerns has a direct positive effect on perceived information risks. This argument is consistent with previous findings (Malhotra et al., 2004; Van Slyke et al., 2006).

> **H2:** Information privacy concerns positively influences perceived information risks

Information practices: Perceived data control (PDC), perceived policy awareness (PPA), and perceived information protection (PIP)

Following existing research (Malhotra et al., 2004; Phelps et al., 2000; Xu et al., 2011), we treat access and choice as one latent construct and use subjective privacy as a proxy measurement of the construct. We operationalize it through perceived data control (PDC) which is defined as individuals' perceptions of their ability to control the usage of their personal information by telcos (Xu et al., 2011; Westin, 1967).

Control-risk literature posits a positive relationship between control perceptions and optimistic bias (for a review, see Harris, 1996), that is, the greater the perception of control over the outcome, the more positive will be the expectation about the event (Klein and Helweg-Larsen, 2002). Accordingly, control perception is an important antecedent to risk-taking and risk perception. When people feel in control, they are more willing to take risks and tend to assess those risks as less serious (Brandimarte et al., 2012). Mayer et al. (1995) defined trust as the willingness to take risks, which perfectly matches the risk-taking concept. Furthermore, risk perception refers to the judgment of the risks associated with the event (i.e., PIR). On the other hand, psychology literature suggests that low perceptions of control may lead people to have high levels of anxiety (i.e., CON) and vice versa for high subjective control (for detailed review, see Rapee et al., 1996). In short, consistent with prior research, we hypothesize that perceived data control positively affects trust (Das and Teng, 2001; Joinson et al., 2010), while it negatively influences perceived information risks (Das and Teng, 2001) and information privacy concerns (Culnan and Armstrong, 1999; Malhotra et al., 2004).

H3: Perceived data control positively influences trust
H4: Perceived data control negatively influences perceived information risks
H5: Perceived data control negatively influences information privacy concerns

Following the literature, we defined perceived policy awareness (PPA) as individuals' perceptions of the degree to which they understand telcos' information practices and perceived information protection (PIP) as individuals' perceptions that their telcos have the ability to safeguard their personal information from security breaches (Pavlou and Fygenson, 2006).

Bandura (2001) and Yamaguchi (2001) claimed that having proxy control could increase the perception of self-control. In the case of perceived policy awareness, literature on institutional privacy assurances claims that in disclosure situations, individuals may attempt to align themselves with privacy policies as a powerful force. This means privacy policies may load individuals with proxy control (Xu, 2007; Xu et al., 2012). Indeed, individuals exert control to avoid their personal information from being misused by companies (Hoffman et al., 1999), and privacy policies are the assurances loading them with beliefs that companies will behave appropriately (Xu, 2007). As for perceived information protection, by definition, it matches the concept of proxy control, i.e., individuals' beliefs that powerful others have the ability to achieve their desired outcomes (Xu, 2007). When it comes to information protection, individuals need both controls to avoid threats related to data holders and threats related to environmental factors (Hoffman et al., 1999). When they believe that data holders are capable of safeguarding their personal information from security breach, they will have higher perception toward their ability to control usage of personal information by telcos.

H6: Perceived policy awareness positively influences perceived data control
H7: Perceived information protection positively influences perceived data control

Research methodology

Measurement of variables

Previously validated measurement items from the literature were adapted to fit our research context and objectives. All items were measured on seven-point Likert scales. Before implementing the full scale study, we conducted a pilot test to verify the reliability and validity of our measurement model. We collected 30 samples from mobile users of a local university in Korea. All results for internal consistency, discriminant validity, and confirmatory factor analysis were within acceptable range and thus satisfied the criteria of reliability and validity. Table 1 shows the total number of items for each construct and the source of the items while Appendix B presents the measurement items.

Data collection and analysis

We used a survey method to collect the data. We engaged Macromill Embrain research company (http://

Table 1. Measurement items.

Variable	No. Items	Adapted from
Information privacy concerns (CON)	4	Xu et al. (2011)
Perceived data control (PDC)	4	Xu et al. (2011)
Perceived information protection (PIP)	2	Pavlou and Fygenson (2006)
Perceived information risks (PIR)	4	Xu et al. (2011)
Perceived policy awareness (PPA)	3	Malhotra et al. (2004)
Trust (TRU)	3	Pavlou and Fygenson (2006)

embrain.com), an online research panel company, to collect the data via an online survey system. Previous studies (e.g., Li et al., 1999) have engaged similar services for their data collection. For this study, an online survey was conducted on a special survey website administrated by the company. A sample was invited randomly by the email server. The sample was drawn from the company's Internet panel members to participate in the 15-minute online survey. Incentive was paid to all members who participated in the survey. A total of 512 responses were obtained. To analyze the data, we used Partial Least Square structural equation modeling (SEM) method. PLS is robust in handling complex model and in theory testing especially during early stage of a study such as that in this paper (Chin, 1998). The tool used was SmartPLS 2.0 (Ringle et al., 2005).

Sample

The sample consists of 53.8% men and 46.5% women (see Table 2). More than 60% of the respondents are between the age of 20 to 39 years old and about 68% of them have earned a bachelor's degree. The majority of the respondents (61.1%) are working adults. Half of them subscribe to SK Telecom, the dominant player in the Korean mobile communication market. This representation closely resembles the market share of mobile operators in Korea.

Results

Measurement model

We evaluated the measurement model by assessing the item reliability, convergent reliability, and discriminant validity. All item loadings for respective constructs (Table 3) exceed the recommended threshold of 0.7, thus signifying good reliability (Barclay et al., 1995). The composite reliability scores for all constructs are above 0.9 (Table 4) which exceeds the requirement of 0.70 by a comfortable margin (Numally, 1978). The AVEs of the constructs (Table 4) meet the minimum cutoff of 0.50 (Hu et al., 2004) and the square root of the AVEs are larger than the correlation between any two constructs (Table 4). In addition, item loadings are larger on the intended construct than on any other constructs (Table 3). All these provide evidence for adequate convergent validity and discriminant validity (Chin, 1998).

Structural model

Figure 2 shows the PLS results. Forty five percent of the variance in perceived information risks, 27 percent of the variance in trusting beliefs, 7 percent of the variance in privacy concerns, and 46 percent of the variance in perceived data control are accounted for by the model. All of the hypotheses are significant at $p<0.05$. The results show that perceived information risks are determined by the individuals' privacy concerns, trusting beliefs, and perceived data control. Privacy concerns have the strongest effect on perceived information risks ($\beta = 0.534$), followed by perceived data control ($\beta = -0.164$), and trust ($\beta = -0.132$). Besides exerting direct effect on perceived information risks, perceived data control also has an indirect impact on perceived information risks via privacy concerns and trust. Perceived data control is in turn determined by perceived policy awareness and perceived information protection with the former having stronger effect than the latter.

Discussion and implications

This study aims to examine the factors that influence perceived information risks. Specifically, it validated the influence of information practices on information privacy concerns, trust, and perceived information risks. It also dissected information practices into perceived policy awareness, perceived information protection, and perceived data control and examined the interrelationships among the three variables. By doing so, this study overcomes the limitations of prior studies by using primary data, providing theoretical background to support the research model,

Table 2. Respondents' demographics.

Demographic Category		N = 512 Frequency	Percentage (%)
Gender	Male	274	53.8
	Female	238	46.5
Age	20–29	178	34.8
	30–39	140	27.3
	40–49	111	21.7
	50–older	83	16.2
Education Level	High school	116	22.7
	Bachelor	350	68.4
	Master	41	8.0
	Doctorate	5	1.0
Occupation	Student	42	8.2
	Worker	313	61.1
	Researcher	6	1.2
	Professional	27	5.3
	Other	124	24.2
Income (KRW)	500,000 or less	22	4.3
	500,000 – 1,000,000	23	4.5
	1,000,000 – 1,500,000	46	9.0
	1,500,000 – 2,000,000	59	11.5
	2,000,000 – 3,000,000	102	19.9
	3,000,000 – 4,000,000	81	15.8
	4,000,000 – 5,000,000	65	12.7
	5,000,000 – 6,000,000	48	9.4
	6,000,000 – more	38	7.4
	None	28	5.5
Telco	SK Telecom	256	50.0
	KT	154	30.1
	LG U+	102	19.9

and including all dimensions of information practices into the research model.

For telcos, the results imply that the factors identified in the model validated in this study can be manipulated to reduce the amount of risks customers perceive in allowing companies to use their personal information. Such reduction is favorable to telcos as previous studies have established a significant link between reduction of risk perception and intention to carry out a behavior such as performing transactions online (Dinev and Hart, 2006; Jarvenpaa et al., 2000; Malhotra et al., 2004). Extending the findings to the context of telcos, we expect customers who perceive lower potential loss associated with giving telcos permission to use personal information to also have higher likelihood of allowing telcos to use their information. Once telcos obtain legal rights to customer information, they will be able to mine the data and customize services to optimize customer experience and improve customer retention rate. This is a competitive advantage that many companies are yearning for especially in the era of big data where infrastructure and information are all readily available. Yet, the biggest roadblock is customer consent. Hence, one of the novelties of this study is the validation of the factors that lead to perceived information risks among telcos customers.

There is strong evidence that in order to lower customers' perception of risks, telcos ought to increase the confidence customers have toward their companies by reducing the anxiety level customers have toward their information practices (i.e., information privacy concern). This can be done by improving customer perception toward their ability to control how telcos will use their personal information (i.e., perceived data control). In fact, improving this perception is valuable as the results show that perceived data control not only has a direct significant effect on perceived information risks, but also an indirect effect on perceived information risks via trust and information privacy concerns. The impact on trust is much stronger compared to that of perceived information risks and information privacy concerns.

Although the relationships between perceived data control and information privacy concerns are found to be significant, we observe from Figure 2 that the variance explained in information privacy concerns is small. This suggests there are other factors beyond perceived data control that influence information privacy concerns. For instance, demographic factors such as gender, age, education level, and income might affect one's privacy concerns (O'Neil, 2001), indeed, as privacy concerns are subjective measures (Introna and Pouloudi, 1999; Kate, 1998; O'Neil, 2001; Singer et al., 1993).

As established in the literature on disclosure of personal information (Dinev and Hart, 2006; Jarvenpaa et al., 2000; Kim et al., 2008), there is a significant relationship between trust and perceived information risks. Therefore, if telcos instill higher levels of trust in customers, then customers will feel more comfortable and perceive lesser risks in giving telcos permission to use their personal information.

The investigation of information practices in the telecommunications industry is another novel contribution of this study. Particularly, the strength of the relationship between perceived policy awareness and perceived data control is worth noting. This indicates that the more an individual thinks he or she understands telcos' information practices, the stronger the individual perceives

Table 3. Confirmatory factor analysis.

Construct	1	2	3	4	5	6	t-value
1. CON							
CON1	**0.949**	−0.248	−0.270	0.586	−0.302	−0.340	157.11
CON2	**0.954**	−0.261	−0.282	0.594	−0.294	−0.342	153.24
CON3	**0.948**	−0.240	−0.299	0.588	−0.300	−0.349	120.28
CON4	**0.954**	−0.231	−0.311	0.606	−0.318	−0.355	132.45
2. PDC							
PDC1	−0.202	**0.939**	0.522	−0.328	0.645	0.501	81.50
PDC2	−0.249	**0.971**	0.536	−0.350	0.648	0.509	305.36
PDC3	−0.275	**0.966**	0.505	−0.374	0.618	0.473	213.49
PDC4	−0.259	**0.946**	0.513	−0.361	0.643	0.486	133.34
3. PIP							
PIP1	−0.281	0.516	**0.978**	−0.351	0.685	0.741	371.36
PIP2	−0.316	0.547	**0.981**	−0.387	0.705	0.767	441.09
4. PIR							
PIR1	0.597	−0.340	−0.345	**0.940**	−0.336	−0.377	143.99
PIR2	0.564	−0.361	−0.326	**0.928**	−0.334	−0.369	95.64
PIR3	0.599	−0.340	−0.384	**0.946**	−0.341	−0.405	117.01
PIR4	0.584	−0.348	−0.361	**0.942**	−0.341	−0.390	137.90
5. PPA							
PPA1	−0.286	0.607	0.666	−0.302	**0.937**	0.667	91.21
PPA2	−0.318	0.646	0.702	−0.351	**0.952**	0.684	141.16
PPA3	−0.288	0.616	0.617	−0.354	**0.909**	0.611	52.44
6. TRU							
TRU1	−0.353	0.428	0.727	−0.365	0.630	**0.922**	75.30
TRU2	−0.347	0.485	0.746	−0.403	0.658	**0.953**	189.84
TRU3	−0.312	0.511	0.666	−0.369	0.656	**0.899**	72.89

Table 4. Internal consistency and discriminant validity of the constructs

Construct	Mean	Standard deviation	AVE	Composite Reliability	CON	PDC	PIP	PIR	PPA	TRU
CON	5.25	1.18	0.905	0.974	**0.95**					
PDC	3.14	1.22	0.913	0.977	*−0.26*	**0.96**				
PIP	3.47	1.28	0.959	0.979	*−0.31*	*0.54*	**0.98**			
PIR	5.78	1.02	0.882	0.968	*0.62*	*−0.37*	*−0.38*	**0.94**		
PPA	3.36	1.18	0.870	0.953	*−0.32*	*0.67*	*0.71*	*−0.36*	**0.93**	
TRU	3.47	1.19	0.856	0.947	*−0.36*	*0.52*	*0.77*	*−0.41*	*0.70*	**0.93**

**Numbers in bold represent the square root of the AVE while numbers in italics represent the correlations.*

himself or herself as having better ability to control the usage of their personal information by telcos. The finding adds support to the role of informed customers in a company's business decisions (Culnan and Armstrong, 1999). For example, telcos could disclose and publicize their practices and make these practices transparent to customers. Alternatively, they could launch campaigns to educate and raise awareness among customers on their information practices. Increasing the awareness of telcos' practices clearly improves customers' perceived data control, and therefore reduces perception toward information risks. Of course, publication of practices requires approval from organizational stakeholders and implementation of educational campaigns requires time and cost and may not directly contribute to the bottom line. However, to gauge the benefit of having the ability to mine customer data for better market positioning and penetration, the importance of these strategies should not be overlooked. The actions of publicizing information practices and educating customers appear to be a good mechanism to increase their awareness.

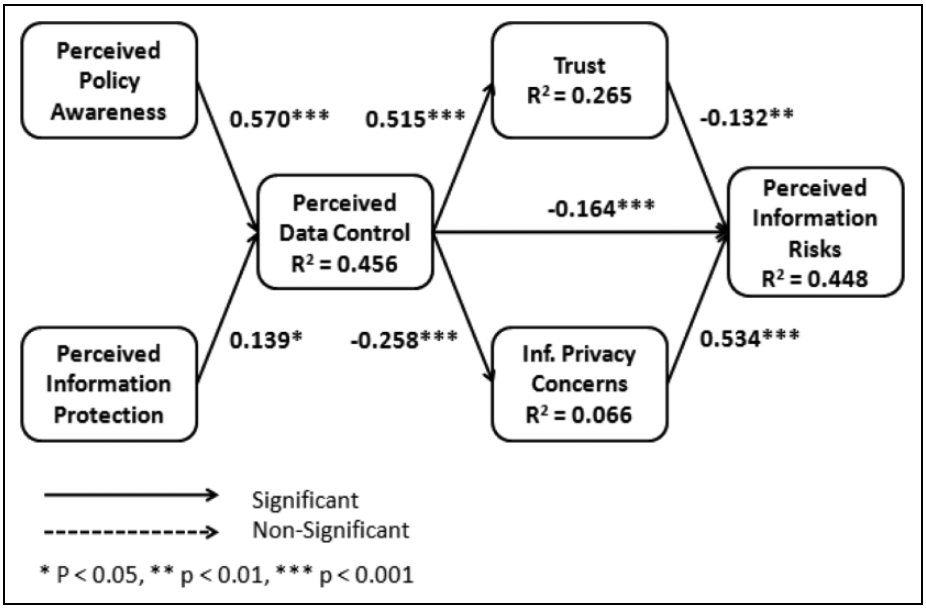


Figure 2. Results of the path analysis (N=512).

The strength of the relationship between perceived policy awareness and perceived data control also has implications for government policies. Specifically, enactment of regulations such as that of Fair Information Practices (Culnan and Armstrong, 1999) will help to instill consumer confidence that their information will not be exploited by commercial organizations. As argued in the literature on institutional privacy assurances (Xu et al., 2012), in disclosure situations, individuals may attempt to align themselves with privacy policies as a powerful force. Therefore, having clear policies in place will assure consumers that companies are and should be responsible in safeguarding their personal information from security breaches.

Theoretical implications

The analysis shows that all of the hypotheses were supported with significant variance explained, indicating that the proposed model is a useful tool to understand how customers perceive the potential risks they may encounter should they give telcos permission to use their personal information. Since the importance of the factors predicting perceived information risks may vary across industries and contexts (Xu et al., 2011), this study makes a valuable contribution by identifying factors that are specific to the context of telecommunication industry.

In particular, information practices are an important part of the model serving as critical antecedents to perceived information risks. As one of the premier studies to support the potential role of information practices in reducing risk beliefs, the findings contribute theoretically to privacy literature. They establishe that passive dimensions such as policy awareness and information protection are important antecedents to active dimensional control (i.e., perceived data control). The findings also highlight the importance of privacy policies because policy awareness, information protection, and control could be captured by privacy policies if they are clearly written to specify how data holders will use customer information and protect this information, and how customers can exert their rights to control their information.

Furthermore, this study establishes the relationship between information practices and trust as well as between information practices and information privacy concerns. It reemphasizes the role of information practices when it comes to consumer perception toward the sharing of personal information with organizations. This opens an avenue of future research to focus on information practices as applicable to different industries and information type.

Limitations and future research

This study provides empirical support for the proposed model. However, the results should be interpreted within its limitations. First, the data was collected only from mobile device users within the telecommunications sector. Therefore, care should be taken when generalizing the interpretations to other contexts such as

different sectors with potentially different information types. For example, consumers may be more sensitive to medical records stored in the health industry compared to shopping transactions stored in the retail industry. As such, they will be much more careful when they consider sharing their medical information with services providers. However, we believe our model is general enough to serve as the basic perceived risks framework for other research contexts. Second, this study focuses only on the antecedents to risks beliefs. However, we believe this is an important first step toward understanding the issues of risks belief within telecommunications industry.

There are potential avenues for future research. First, future research can examine information practices and perceived information risks in different industries and investigate how information practices differ based on the types of consumer information, and the level of sensitivity to these information. Second, different cultures may have different attitude toward information sharing and different level of sensitivity toward information types. A piece of information that is well-guarded in one culture may be seen as simply public information in another culture. Future studies could therefore explore how different cultures vary on their sensitiveness toward personal information and how such level of sensitivity affects their perceived information risks and ultimately their willingness to share the information with services providers. Third, future research can compare and contrast the effect of different types of regulations on customer perception of information risks. Such insights are valuable as consumers often align themselves with privacy policies in disclosure situations. Fourth, since perceived data control only explains a small variance in information privacy concerns, future research could explore other factors that may contribute to perceived data control.

Conclusion

This study builds on existing literature to develop a model of perceived information risks and validated the model with data from the telecommunications sector. It tested all four dimensions of information practices and their interrelations as well as the effect of information practices on trust, information privacy concerns, and perceived information risks. With all hypotheses found to be significant and satisfactory variance explained by the model, it serves as a good framework for telcos to start formulating effective strategies to manage customer risk perception. Only when customers see lesser risks associated with allowing companies to use their personal information will companies be able to gauge benefits from the voluminous amount of data that are sitting in company servers waiting to be mined.

Appendix A

Literature Review

Source	Topic (Domain)	Important concepts	Major findings
Bellman et al. (2004)	Explore possible explanations for differences in privacy concerns (Internet)	Internet privacy concerns, culture, internet experience, government involvement in regulation	Privacy concerns varied across cultural values and Internet experience.
Culnan and Armstrong (1999)	Willingness to have personal information to be used for profiling (Interactive Marketing)	Fair information practices, privacy concerns, direct marketing frequency	Companies may reduce customers' privacy concerns by using fair information practices.
Dinev and Hart (2004)	Factors affecting privacy concerns (e-Commerce)	Privacy concerns, perceived vulnerability (risk), perceived ability to control	Development and validation of three measurement instruments for privacy concerns, perceived vulnerability, and perceived ability to control.
Dinev and Hart (2006)	Factors affecting intention to provide personal information to complete transactions (e-Commerce)	Internet privacy concerns, Internet trust, perceived Internet privacy risk, personal Internet interest	Privacy concerns and perceived risks played important roles as inhibitors for e-commerce transactions. However, the role of trust and personal interest may outweigh this negative effect.

(continued)

Appendix A. (continued)

Source	Topic (Domain)	Important concepts	Major findings
Häkkilä and Chatfield (2005)	Perceived privacy in short message service (Telecommunications)	Privacy	Individuals felt mobile phones are personal devices. Also, they perceived SMS as more private than voice calls.
Jarvenpaa et al. (2000)	Factors affecting intention to purchase from Internet stores (e-Commerce)	Risk perception, trust in store, perceived size, perceived reputation	Differences in size and reputation among online stores shaped their trust on vendors and their perception of risks.
Jensen and Potts (2004)	Usability of online privacy policies (e-Commerce)	Accessibility, writing, content	Form, location, and legal context of policies were very important for customers' decision-making.
Lee and Kim (2006)	Privacy threats in mobile Radio Frequency Identification (RFID)	Privacy threats (risks), privacy protecting measures	Mobility of reader device may cause privacy threats, thus becoming a barrier for the development of this service model.
Lee (2009)	Factors affecting intention to use online banking (Online Banking)	Perceived benefit, perceived usefulness, perceived ease of use, perceived risks	Financial and security (information) risks were the main factors negatively affecting behavioral intention while perceived benefits were found to have a positive significant effect on intention.
Li et al. (2010)	Factors affecting intention to disclose personal information (e-Commerce)	Perceived usefulness, monetary rewards, privacy protection belief, privacy risk belief, perceived relevance of information	Monetary rewards could undermine personal information disclosure when information has low relevance to the transaction. In addition, risks perception was the strongest predictor of intention
Malhotra et al. (2004)	Factors affecting intention to give personal information (Internet)	Trusting beliefs, risk beliefs, privacy concerns, type of information	Risk beliefs were found to be the strongest predictor of intention and this path outweighed the effect of trusting beliefs and privacy concerns.
Norberg et al. (2007)	Factors affecting intention to disclose personal information (Offline)	Trust, risk	A paradox between intention and actual behavior may exist. Risks were the strongest predictor for intention, while trust was the strongest predictor for actual behavior.
Pavlou (2003)	Factors affecting intention to transact on internet (e-Commerce)	Perceived risk, perceived usefulness, perceived ease of use, trust, reputation, satisfaction with past transactions	Perceived risk was the strongest antecedent to intention. Trust has direct and indirect effect onto intention.
Sheehan (2002)	Development of Internet users typology (Internet)	Privacy concerns, awareness, information sensitivity	Four distinct groups of Internet users were found: Unconcerned, circumspect, wary, and alarmed.
Slyke et al. (2006)	Factors affecting intention to transact on internet (e-Commerce)	Familiarity, trust, privacy concerns, risk perception	Privacy concerns affected risks perceptions, trust, and intention to transact for a well-known store, but not for a less well-known store. Risks were the strongest predictors of intention.

Appendix B

Measurement Items

Information Privacy Concerns (CON)

CON1[a]	I am concerned that if I give permission to my Network Operator to use my personal information they have stored, this information could be misused
CON2[a]	I am concerned that others can find private information about me if I give permission to my Network Operator to use my personal information they have stored
CON3[a]	I am concerned about giving permission to my Network Operator to use my personal information they have stored because of what others might do with it
CON4[a]	I am concerned about giving permission to my Network Operator to use my personal information they have stored because it could be used in a way I do not foresee

Trust (TRU)

TRU1[b]	My Network Operator will be competent in using my personal information
TRU2[b]	My Network Operator will be honest in the ways it will use my personal information
TRU3[b]	My Network Operator will not seek to take advantage of me if I give permission to use my personal information

Perceived Information Risks (PIR)

PIR1[a]	It would be risky to give permission to my Network Operator to use my personal information they have stored
PIR2[b]	If I give permission to my Network Operator to use my personal information they have stored, there would be high potential for privacy loss
PIR3[b]	If I give permission to my Network Operator to use my personal information they have stored, my personal information could be inappropriately used
PIR4[b]	If I give permission to my Network Operator to use my personal information they have stored, it would involve many unexpected problems

Perceived Data Control (PDC)

PDC1[b]	If I give permission to my Network Operator to use my personal information they have stored, I will have control over who can get access to it
PDC2[b]	If I give permission to my Network Operator to use my personal information they have stored, I will have control over what personal information is used
PDC3[b]	If I give permission to my Network Operator to use my personal information they have stored, I will have control over how it is used
PDC4[b]	If I give permission to my Network Operator to use my personal information they have stored, I will have control over it

Perceived Information Protection (PIP)

PIP1[a]	I expect my personal information to be adequately protected if I give permission to my Network Operator to use it
PIP2[a]	I feel secure that my personal information will be kept private if I give permission to my Network Operator to use it

Policy Awareness (PPA)

PPA1[a]	I believe my Network Operator will disclose the way my personal information will be collected, processed, and used
PPA2[a]	I am confident that my Network Operator's privacy policy will have a clear and conspicuous disclosure
PPA3[a]	I am confident that I will be aware and knowledgeable about how my personal information will be used

[a] Scale: Strongly disagree / strongly agree.

[b] Scale: Extremely unlikely / extremely likely.

References

Bandura A (2001) Social cognitive theory: An agentic perspective. *Annual Review of Psychology* 52(1): 1–26.

Banerjee A (2011) Addressing "Big Data" telecom requirements for real-time analytics. *Heavy Reading*.

Barclay D, Higgins C and Thompson R (1995) The partial least squares (PLS) approach to causal modeling: Personal computer adoption and use as an illustration. *Technology Studies* 2(2): 285–309.

Bellman S, Lohse GL and Johnson EJ (1999) Predictors of online buying behavior. *Communications of the ACM* 42(12): 32–38.

Brandimarte L, Acquisti A and Loewenstein G (2012) Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science* 0(0): 1–8.

Brown B, Chui M and Manyika J (2011) Are you ready for the era of 'Big Data'? *MacKinsey Global Institute*.

Chellappa RK and Pavlou PA (2002) Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management* 15(5/6): 358–368.

Chin WW (1998) The partial least squares approach for structural equation modeling. In: Marcoulides GA (ed) *Modern methods for business research*. Mahwah, NJ: Lawrence Erlbaum Associates, pp. 295–336.

Columbus L (2012) Roundup of Big Data forecasts and market estimates, 2012. *Forbes*, 16 August.

Culnan MJ and Armstrong PK (1999) Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science* 10(1): 104–115.

Das TK and Teng B-S (2001) Trust, control, and risk in strategic alliances: An integrated framework. *Organization Studies* 22(2): 251–283.

Davenport TH, Harris JG and Morison R (2010) *Analytics at work: Smarter decisions, better results*. Boston, MA: Harvard Business Press.

Dinev T and Hart P (2004) Internet privacy concerns and their antecedents–measurement validity and a regression model. *Behaviour & Information Technology* 23(6): 413–422.

Dinev T and Hart P (2006) An extended privacy calculus model for e-commerce transactions. *Information Systems Research* 17(1): 61–80.

Dowling GR and Staelin R (1994) A model of perceived risk and intended risk-handling activity. *Journal of Consumer Research* 21(1): 119–134.

EC_95/461995 (1995) Directive 95/46/ec of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

ET News (2012a) Decline of telcos' revenue. Will telcos recover it in the second quarter. *ET News*, 5 August.

ET News (2012b) Why KT invest KRW 100bn in contents fund. *ET News*, 17 September.

ET News (2013) SKT invest KRW 1,200bn to ICT convergence business. *ET News*, 9 May.

Ganesan S (1994) Determinants of long-term orientation in buyer-seller relationships. *Journal of Marketing* 58(2): 1–19.

Gefen D (2000) E-commerce: The role of familiarity and trust. *Omega* 28(6): 725–737.

Gefen D, Karahanna E and Straub DW (2003) Trust and TAM in online shopping: An integrated model. *MIS Quarterly* 27(1): 51–90.

Girardin F, Calabrese F, Fiore FD, et al. (2008) Digital footprinting: Uncovering tourists with user-generated content. *Pervasive Computing, IEEE* 7(4): 36–43.

Häkkilä J and Chatfield C (2005) 'It's like if you opened someone else's letter': User perceived privacy and social practices with SMS communication. In: *7th International Conference on Human Computer Interaction with Mobile Devices & Services (MobileHCI 2005)*, Salzburg, Austria.

Harris P (1996) Sufficient grounds for optimism? The relationship between perceived controllability and optimistic bias. *Journal of Social and Clinical Psychology* 15(1): 9–52.

Hoffman DL, Novak TP and Peralta M (1999) Building consumer trust online. *Communications of the ACM* 42(4): 80–85.

Hu X, Lin Z, Whinston AB, et al. (2004) Hope or hype: On the viability of escrow services as trusted third parties in online auction environments. *Information Systems Research* 15(3): 236–249.

Introna L and Pouloudi A (1999) Privacy in the information age: Stakeholders, interests and values. *Journal of Business Ethics* 22(1): 27–38.

Jarvenpaa SL, Tractinsky N and Vitale M (2000) Consumer trust in an Internet store. *Information Technology and Management* 1(1–2): 45–71.

Jensen C and Potts C (2004) Privacy policies as decision-making tools: An evaluation of online privacy notices. In: *SIGCHI Conference on Human Factors in Computing Systems (CHI 2004)*, Vienna, Austria.

Joinson AN, Reips U-D, Buchanan T, et al. (2010) Privacy, trust, and self-disclosure online. *Human-Computer Interaction* 25(1): 1–24.

Kate N (1998) Women want privacy. *American Demographics* 20(1): 37.

KCC (2013) ICT Statistics. Available at: http://kcc.go.kr/user.do?boardId=1030&page=A02060400&dc=K02060400 (accessed 10 June 2013).

Kim DJ, Ferrin DL and Rao HR (2008) A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems* 44(2): 544–564.

Kim M-K, Park M-C and Jeong D-H (2004) The effects of customer satisfaction and switching barrier on customer loyalty in Korean mobile telecommunication services. *Telecommunications Policy* 28(2): 145–159.

Klein CT and Helweg-Larsen M (2002) Perceived control and the optimistic bias: A meta-analytic review. *Psychology and Health* 17(4): 437–446.

Lee H and Kim J (2006) Privacy threats and issues in mobile RFID. In: *1st International Conference on Availability, Reliability, and Security (ARES 2006)*, Vienna, Austria.

Lee M-C (2009) Factors influencing the adoption of Internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. *Electronic Commerce Research and Applications* 8(3): 130–141.

Li H, Kuo C and Rusell MG (1999) The impact of perceived channel utilities, shopping orientations, and demographics on the consumer's online buying behavior. *Journal of Computer-Mediated Communication* 5(2): 0–0.

Li H, Sarathy R and Xu H (2010) Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems* 51(1): 62–71.

Liu C, Marchewka JT, Lu J, et al. (2004) Beyond concern: A privacy-trust-behavioral intention model of electronic commerce. *Information & Management* 42(1): 127–142.

McAfee A and Brynjolfsson E (2012) Big data: The management revolution. *Harvard Business Review* 90(10): 60–66.

McGuire T, Manyika J and Chui M (2012) Why Big Data is the new competitive advantage. *Ivey Business Journal* July / August.

Malhotra NK, Kim SS and Agarwal J (2004) Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research* 15(4): 336–355.

Mathews A (1990) Why worry? The cognitive function of anxiety. *Behaviour Research and Therapy* 28(6): 455–468.

Mayer RC, Davis JH and Schoorman FD (1995) An integrative model of organizational trust. *Academy of Management Review* 20(3): 709–734.

Norberg PA, Horne DR and Horne DA (2007) The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs* 41(1): 100–126.

Numally JC (1978) *Psychometric theory*. New York, NY: McGraw-Hill.

O'Neil D (2001) Analysis of Internet users' level of online privacy concerns. *Social Science Computer Review* 19(1): 17–31.

Park N (2011) A study on mobile data protection. *Korea Communications Commission*.

Pavlou PA (2003) Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce* 7(3): 101–134.

Pavlou PA and Fygenson M (2006) Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *MIS Quarterly* 30(1): 115–143.

Phelps J, Nowak G and Ferrell E (2000) Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing* 19(1): 27–41.

Prosser WL (1960) Privacy. *California Law Review* 48(3): 383–423.

Raghunathan R and Pham MT (1999) All negative moods are not equal: Motivational influences of anxiety and sadness on decision making. *Organizational Behavior and Human Decision Processes* 79(1): 56–77.

Rapee RM, Craske MG, Brown TA, et al. (1996) Measurement of perceived control over anxiety-related events. *Behavior Therapy* 27(2): 279–293.

Ringle CM, Wende S and Will A (2005) SmartPLS 2.0 (M3) Beta, Hamburg. Available in http://www.smartpls.de.

Segerstrom SC, Tsao JC, Alden LE, et al. (2000) Worry and rumination: Repetitive thought as a concomitant and predictor of negative mood. *Cognitive Therapy and Research* 24(6): 671–688.

Sheehan KB (2002) Toward a typology of Internet users and online privacy concerns. *The Information Society* 18(1): 21–32.

Sheina M and Bali S (2012) Dialing into telco data. Reliable data management drives smarter telco business. *OVUM*.

Siegrist M, Gutscher H and Earle TC (2005) Perception of risk: The influence of general trust and general confidence. *Journal of Risk Research* 8(2): 145–156.

Singer E, Mathiowetz NA and Couper MP (1993) The impact of privacy and confidentiality concerns on survey participation: The case of the 1990 US census. *Public Opinion Quarterly* 57(4): 465–482.

Smith HJ, Milberg SJ and Burke SJ (1996) Information privacy: Measuring individuals' concerns about organizational practices. *MIS quarterly* 20(2): 167–196.

Suh B and Han I (2003) The impact of customer trust and perception of security control on the acceptance of electronic commerce. *International Journal of Electronic Commerce* 7(3): 135–161.

TRUSTe (2011) Smart privacy for smartphones. Understanding and delivering the protection consumers want. *TRUSTe*.

Van Slyke C, Shim J, Johnson R, et al. (2006) Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems* 7(6): 415–444.

Westin AF (1967) *Privacy and freedom*. New York, NY: Atheneum.

Xu H (2007) The effects of self-construal and perceived control on privacy concerns. In: *28th Annual International Conference on Information Systems (ICIS 2007)*, Montréal, Canada.

Xu H, Dinev T, Smith J, et al. (2011) Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems* 12(12): 798–824.

Xu H, Teo H-H, Tan BC, et al. (2012) Research note–Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. *Information Systems Research* 23(4): 1342–1363.

Yamaguchi S (2001) Culture and control orientations. In: Matsumoto D (ed.) *The handbook of culture and psychology*. New York: Oxford University Press, pp.223–243.

About the authors

Christian Fernando Libaque-Sáenz is a PhD candidate at the Department of Business & Technology Management at Korea Advanced Institute of Science and Technology (KAIST). He received his bachelor degree in Telecommunications Engineering from National University of Engineering (Universidad Nacional de Ingeniería, Peru), and MA degree in Information and Telecommunication Technology from KAIST. Before joining the PhD program at KAIST, he worked for the Peruvian Ministry of Transport and Communications. Christian's research interests include digital divide, privacy issues, ICT strategy, and spectrum management. Contact: Korea Advanced Institute of Science and Technology (KAIST) – Department of Business and Technology Management, Yuseong, Daejeon, Republic of Korea. Email: christianlibaque@kaist.ac.kr

Siew Fan Wong is a senior lecturer in the Department of Information Systems at Sunway University, Malaysia. She received her PhD degree in MIS from the University of Houston, Texas. Her research includes IT outsourcing and organizational IT strategy. Recently, she started working on projects that look at the impacts of social media usage and the digital divide. Contact: Sunway University – Department of Information Systems, No 5, Jalan Universiti, Bandar Sunway, Petaling Jaya, Selangor 46150, Malaysia. Email: siewfanw@sunway.edu.my, siewfan@gmail.com

Younghoon Chang is a PhD candidate in the Department of Business & Technology Management at Korea Advanced Institute of Science and Technology (KAIST). He received his bachelor's degree in business administration from Korea University. Younghoon's research interests include digital divide, e-business, ICT strategy, and cross-cultural IT marketing. His articles have appeared in *Information Development. Entrue Journal of Information Technology*, and *Telecommunications Review* as well as in the proceedings of international conferences and domestic conferences. Contact: Korea Advanced Institute of Science and Technology (KAIST) – Department of Management Science, #5108, N22 Alumni Building, Guseong-dong Yuseong Daejeon 305701, Republic of Korea, T: 0423506333 F: 042350 6339. Email: younghoonchang@kaist.ac.kr

Young Wook Ha is a PhD candidate in the Department of Business & Technology Management at Korea Advanced Institute of Science and Technology (KAIST) and a senior researcher in the Creative Future Research Laboratory at Electronics and Telecommunications Research Institute (ETRI). He received his master's degree in the Department of IT Management at Korea Advanced Institute of Science and Technology (KAIST). His research interests include new media marketing, mobile SNS advertising, and IT behavior. His articles have appeared in *Psychology & Marketing* and *ETRI Journal*. Contact: Korea Advanced Institute of Science and Technology (KAIST) – Department of Business and Technology Management, Yuseong, Daejeon, Republic of Korea. Email: top3@kaist.ac.kr

Myeong-Cheol Park is a professor in the Department of Business & Technology Management at Korea Advanced Institute of Science and Technology (KAIST). He is a board member of CPRsouth (Communication Policy Research South) and former President of Korea Technology Innovation Society. He has published numerous papers in the areas of telecommunications management strategy and economics in *Telecommunications Policy, Information Economics and Policy, Internet Research, Journal of Global Information and Management, Scientometrics, Information Technology and Management, Information Systems and e-Business Management, Management Decision,* and *ETRI Journal*. One of his papers published in *Telecommunications Policy* is now honored as the most-cited paper since his publication from 2004. Before joining KAIST, he worked for Electronics and Telecommunication Research Institute (ETRI), one of the largest Korean government research institutes. He received his BS and MA degrees from Seoul National University, and his PhD degree in business administration from the University of Iowa (USA). Contact: Korea Advanced Institute of Science and Technology (KAIST) – Department of Business and Technology Management, Yuseong, Daejeon, Republic of Korea. Email: imcpark@kaist.ac.kr