MEASURING MOBILE USERS' CONCERNS FOR INFORMATION PRIVACY

Completed Research Paper

Heng Xu
Pennsylvania State University
University Park, USA
hxu@ist.psu.edu

Sumeet Gupta
Indian Institute of Management
Raipur, India
sumeetguptadr@gmail.com

Mary Beth Rosson
Pennsylvania State University
University Park, USA
mrosson@ist.psu.edu

John M. Carroll
Pennsylvania State University
University Park, USA
jcarroll@ist.psu.edu

Abstract

The evolution of mobile network technologies and smartphones has provided mobile consumers with unprecedented access to Internet and value-added services while on the move. Privacy issues in such context become critically important because vendors may access a large volume of personal information. Although several pioneering studies have examined general privacy risks, few systematic attempts have been made to provide a theory-driven framework on the specific nature of privacy concerns among mobile consumers. To fill the gap in the literature, this article introduced a 9-item scale, which was shown to reasonably represent the dimensionality of mobile users' information privacy concerns (MUIPC), categorized as perceived surveillance, perceived intrusion, and secondary use of personal information. Through a survey study (n=310), the three-factor structure of MUIPC as revealed in exploratory factor analysis was further confirmed through confirmatory factor analysis. Further analysis revealed that the second-order model of MUIPC performed better than its first-order model.

Keywords: Information privacy, privacy concerns, mobile users, instrument development, survey

Introduction

The evolution of mobile network technologies and smartphones has provided mobile consumers with unprecedented access to Internet and value-added services while on the move. With the rapid diffusion of smartphones, the growth trajectory of mobile applications (apps) is striking. According to Gartner (2012), mobile apps will not only generate $15.9 billion in expected end-user spending in 2012, but also drive smartphone sales, advertising spending, and technology innovation. By offering context-aware features that cater to a user's mobile environment, mobile apps have redefined the user experience and have evolved into a highly competitive marketplace that attracts the interest of a number of stakeholders including device vendors, merchants, application developers and marketing firms (Gartner 2012).

However, the use of mobile apps often transmits a large amount of personal data in real time, rendering strong potential for privacy intrusion (FTC 2009). Recent headlines have highlighted this potential risk by reporting that vendors and app developers are indeed collecting personal data through users' smartphones and transmitting them to other entities. In an examination of 101 popular smartphone apps, the Wall Street Journal found that, 56 apps transmitted the phone's unique identifiers to other companies without users' awareness and 47 apps transmitted the phone's location to outsiders (Thurm and Kane

2010). It was further revealed that both Apple iOS and Google Android mobile operating systems regularly record and transmit location data without the consent of device owners (Angwin and Valentino-Devries 2011).

Such aggressive practices of data access and transmission employed by mobile apps and operating systems have aggravated privacy concerns among users. These concerns are related to the mobile devices' automatic collection and communication of users' real-time whereabouts information, and the confidentiality of gathered data such as location, personal identity, and daily behavior (FTC 2009). Unlike the conventional Internet, the mobile platform allows for real-time and always-on data communication and transmission, which poses salient privacy threats that are different from those online privacy issues discussed in earlier studies (e.g., Malhotra et al. 2004; Van Slyke et al. 2006; Xu et al. 2011). For this reason, Bélanger and Crossler (2011, p.1022) stated that "one area of future research that seems likely to gain importance is the balancing of information privacy concerns with the advantages of location-based services." To respond to this call, we aim to develop a theoretical framework on the specific nature of information privacy concerns among mobile consumers. Drawing on the Communication Privacy Management (CPM) theory (Petronio 2002), we propose that the privacy concerns of mobile users are centered on three major dimensions, namely, perceived surveillance, perceived intrusion, and secondary use of personal information. In this research, we define mobile users' information privacy concerns (MUIPC) as concerns about possible loss of privacy as a result of information disclosure to a specific external agent.

In what follows, we first provide a review of prior literature to introduce the theoretical background of studying information privacy, privacy concerns, and existing scales. Then we use the CPM theory as the overarching theory to guide our conceptual development on the specific nature of MUIPC. This is followed by a description of the research methodology and findings. The paper concludes with a discussion of the key results, directions for future research, and the practical implications of the findings.

Theoretical Background

Information Privacy, Information Privacy Concerns, and Existing Scales

Various approaches to conceptualize information privacy have been proposed in the literature across many disciplines or domains. To synthesize different theoretical perspectives from multiple disciplines, Smith et al. (2011) identified four definitional approaches of information privacy: privacy as a human right, privacy as a commodity, privacy as a state of limited access, and privacy as the ability to control information about oneself. Although there exist a number of conceptualizations of information privacy, there is little variance in operationalizing information privacy in the IS field. According to Xu et al. (2011), the variable of "information privacy concerns" has become the pivotal construct within IS research and has acted as proxy to operationalize the concept of "information privacy." Specifically, Smith et al. (1996) developed the scale of Concern for Information Privacy (CFIP), which regarded privacy concerns as "individuals' concerns about organizational information privacy practices" (p.169) with four data-related dimensions: collection of personal information, unauthorized secondary use of personal information, errors in personal information, and improper access to personal information. A later validation study of the CFIP scale empirically established the psychometric properties of this scale and demonstrated its second-order factor structure (Stewart and Segars 2002).

Malhotra et al. (2004) developed a multidimensional scale of Internet Users Information Privacy Concerns (IUIPC) which adapted the scale of CFIP from the original context of offline direct marketing into the Internet context. Focusing on "individuals' perceptions of fairness/justice in the context of information privacy" (p.340), IUIPC encompassed three dimensions of privacy concerns: collection of personal information, control over personal information, and awareness of organizational privacy practices. Malhotra et al. (2004) empirically demonstrated that IUIPC excelled CFIP as a predictor of consumers' reactions to online privacy threats. However, a recent literature review on information privacy (Bélanger and Crossler 2011) has revealed that the scale of IUIPC has been under-utilized in subsequent research. And most privacy studies including a few recent ones still adopt the CFIP scale (Bélanger and Crossler 2011). As one of their recommendations for future privacy research, Bélanger and Crossler (2011) stressed the need for more precise measurement of privacy concerns in varying contexts, and suggested

researchers to "create and utilize more validated instruments so that future privacy research can more readily build upon one another (p.1035)."

As a reliable instrument, the scale of CFIP has been widely applied in different contexts, ranging from direct marketing (Smith et al. 1996) to e-commerce (Van Slyke et al. 2006) and to healthcare (Angst and Agarwal 2009). However, when developing the CFIP scale, Smith et al. (1996) acknowledged that "the dimensionality is neither absolute nor static, since perceptions of advocates, consumers, and scholars could shift over time" (p. 190). Stewart and Segars (2002, p.37) also pointed out, "the theoretical and operational assumptions underlying the structure of constructs such as CFIP should be reinvestigated in light of emerging technology, practice, and research." This is particularly the case given current aggressive practices of data collection and transmission employed by mobile apps and operating systems. Thus it is vital to investigate the shifting dimensions of information privacy concerns because mobile users are likely to differ from online consumers and thus perceive privacy threats differently.

Communication Privacy Management (CPM) Theory

As revealed by the Wall Street Journal, popular mobile apps and major mobile operating systems regularly record and transmit personal information without the consent of device owners (Angwin and Valentino-Devries 2011; Thurm and Kane 2010). Such aggressive data collection and transmission practices imply that the information flow on a mobile device moves to a collective domain where both data subject (e.g., mobile users) and data recipient (e.g., vendors or app providers) become co-owners with joint responsibilities for keeping the information private. For this reason, mobile users' concerns for location information disclosure cannot be fully understood without knowing users' expectations about how their disclosed information will be used and who will have access to the information. CPM theory is especially useful for understanding the tension between data subjects and data recipients concerning privacy (Petronio 2002). One of the main contributions of CPM is that the theory "not only gives the option of examining personal privacy boundaries around an individual's information but also allows for the notion of multiple privacy boundaries or collectively held private information (Petronio 2010, p.180)."

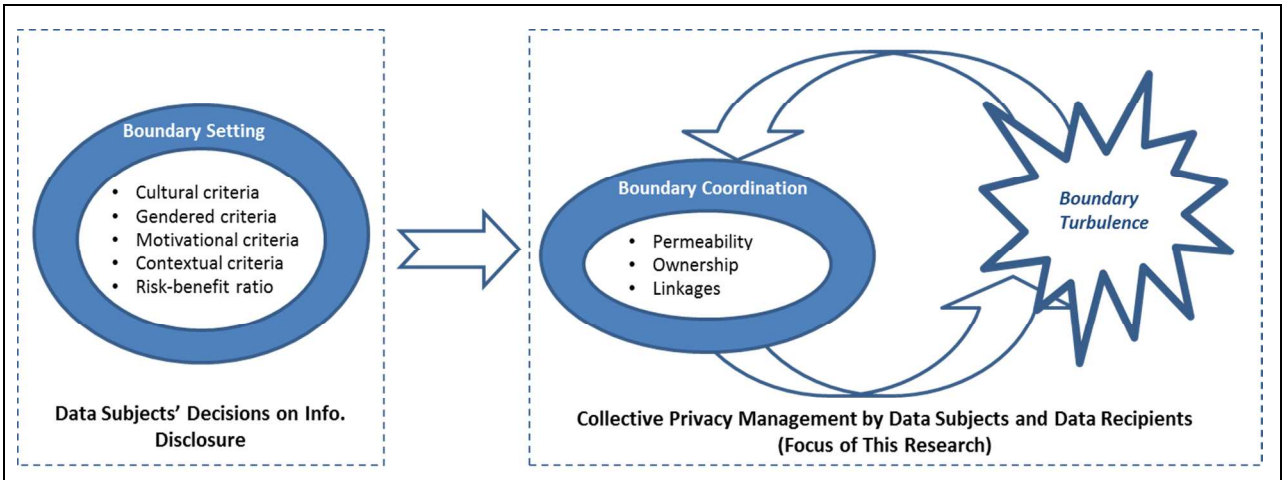


Figure 1. Communication Privacy Management (CPM) Theory (Adapted from Petronio 2002)

CPM is a rule-based theory which proposes that individuals develop rules to form cognitive information spaces based on five criteria they perceive as salient at the time of the information disclosure (Petronio 2002): (1) cost-benefit ratio, (2) context, (3) motivations, (4) gender, and (5) culture. After individuals disclose their personal information, the information moves to a collective domain where collectives (i.e., data subjects and data recipients) manage mutually held privacy boundaries (see Figure 1). CPM makes a compelling case for the notion of co-management of private information, which calls for the boundary coordination process through collective control over revealed information by both data subjects and data recipients (Petronio 2010). Three boundary coordination rules are identified by the CPM theory (Petronio 2002), including (a) coordinating permeability rules, (b) coordinating ownership rules, and (c)

coordinating linkage rules. As a whole, these coordination rules "illustrate the modes of change for the dialectic of privacy-disclosure as managed in a collective manner" (Petronio 2002, p.127).

Boundary turbulence occurs when data subjects and data recipients are unable to collectively execute or enact coordination rules guiding information permeability, ownership, and linkages (Petronio 2002). The recent public privacy outcry that ensued after Apple violated its own privacy policy by allowing its iPhone applications to transmit a user's data (including age, gender, unique phone ID and location) to third parties is one recent example of boundary turbulence (Thurm and Kane 2010). When boundary turbulence (e.g., privacy breach) occurs, individuals' privacy concerns increase. Consequently, they attempt to re-coordinate their boundary rules guiding information permeability, ownership, and linkages.

Mobile Users' Information Privacy Concerns (MUIPC)

As shown in Figure 1, we apply the boundary coordination rules to theoretically explore the interplay between mobiles users and service providers where privacy is concerned; while the boundary setting rules focusing on individuals' decisions on information disclosure are not examined in this study. Specifically, we develop three dimensions of MUIPC, corresponding to the three boundary coordination rules in the CPM theory. First, we argue that users' perceptions of *surveillance* can be very salient due to aggressive data collection activities by mobile apps, which leads to the open boundary structure with high degree of information permeability. Second, the perceptions of *intrusion* could be triggered when ownership rules are violated, i.e., when mobile apps are able to make independent decisions about possessing or soliciting users' personal information. Third, mobile users' privacy concerns over *secondary use of information* can be very salient when linkage coordination rules are violated, i.e., when a new linkage to personal data occurs without users' awareness or consent.

Perceived Surveillance

Malhotra et al. (2004) suggest that the practice of data collection, whether legitimate or illegitimate, "is the starting point of various information privacy concerns (p.338)." Reflecting on the origin of privacy concerns, collection refers to individuals' concerns about the amount of personal information demanded by others (Malhotra et al. 2004). The act of data collection triggers the coordination of permeability rules which refer to the parameters for how much others should know about the private information within the co-owned privacy boundary (Petronio 2010). Typically, when individuals are provided with a significant amount of control over information disclosure, they create boundary structures that reduce the amount of information collection by others or they establish boundaries with low permeability (Child et al. 2009; Petronio 2010).

However, the rapid advancement of mobile technologies has provided a more encompassing and powerful means of surveillance, which creates an open boundary structure with high degree of information permeability. Increasingly, the aggressive data collection activities by mobile apps and operating systems induce the perception of intensive data logging, as well as the impression that vendors are constantly monitoring user behavior through smartphones. Because smart phones contain various functions such as web browsers, emails, photo albums, games, calendars, and contact lists, apps can collect far more personally invasive data than was previously conceivable in conventional use of personal computers, e.g., identity, upcoming schedule, time spent on different apps, contact lists, real-time location, etc.

Solove (2006) has defined surveillance as "the watching, listening to, or recording of an individual's activities (p.490)." In today's mobile environment, vendors take advantage of the powerful surveillance technologies to track and profile mobile consumers. Mobile users may resist mobile apps for the fear that their activities may be watched, recorded, and transmitted to various entities. Accordingly, we posit surveillance, rooted from the dimension of collection from CFIP and IUIPC, as an important factor characterizing MUIPC.

Perceived Intrusion

In CPM, ownership rules capture the extent to which the original owner of private information (i.e., data subjects) assumes that co-owners (i.e., data recipients) are able to make independent decisions about further possessing or soliciting information (Child et al. 2009; Petronio 2010). According to Child et al.

(2009), "[r]ules governing ownership are easily observed when they are violated," and "when the individuals involved discover they must change or readjust their privacy rules to guard against unwelcome intrusions (p.2081)." In other words, data subjects' perceptions of intrusion would be triggered when data recipients are able to make independent decisions about their personal information.

The notion of intrusion has often been connected to the concept of personal space (Solove 2006), which is consistent with the notion of boundary in CPM. In today's mobile environment, due to the powerful technological surveillance means to track and profile a mobile user, the notion of personal space has expanded to incorporate realms of both physical and informational space. Solove (2006) defines intrusion as "invasive acts that disturb one's tranquility or solitude" (p.491) and "involves the unwanted general incursion of another's presence or activities" (p.555). It has been argued that intrusion interrupts the victim's activities or routines, destroys his or her solitude, and often makes the victim feel uncomfortable (Solove 2006).

Malware is an especially growing problem for smartphones (Dignan 2011). A plethora of data is accessible by malware developers, including browser history, usage patterns of apps, keyboard keystroke cache, phone numbers, contacts, current and past geographic location, and etc. Because it is highly possible to have malware even from mobile app stores (Dignan 2011), users may resist mobile apps for the fear that the malicious apps may interrupt their activities through the unwanted presence. The major point that emerges is that intrusion can create discomfort and harm and therefore, the flow of personal information across boundaries requires users' efforts to restore their comfort levels. Indeed, the intrusion dimension is somehow implied through such CFIP dimensions as improper access and errors, as well as the dimension of control in IUIPC. However, we believe that the intrusion dimension based on CPM will succinctly convey mobile users' concerns over both physical and informational space.

Secondary Use of Information

According to Smith et al. (1996), secondary use of personal information refers to the situations where information is collected from individuals for one purpose but is used for another (e.g., profiling individuals and sending marketing messages), without authorization from the individuals. The activity of secondary use of information by an organization, can "potentially threaten an individual's ability to maintain a condition of limited access to his/her personal information, harm individuals, and subsequently threaten the organization's legitimacy in its interactions with consumers, shareholders, and regulators (Culnan and Williams 2009, p.675)."

The practice of secondary use of personal information triggers the coordination of linkage rules which refer to "the establishment of mutually agreed-upon privacy rules used to choose others who may be privy to the collectively held information (Jin 2012, p.70)." In CPM, establishing a linkage means data access is granted to another entity to become a co-owner of private information. Users' privacy concerns over secondary use of information would be triggered when a new linkage occurs without users' (i.e., data subjects') awareness or consent. The linkage coordination rules are often considered breached if the vendor reveals the gathered personal information to unauthorized entities, or if the vendor uses personal information for secondary purposes without consumers' awareness and consent. According to Solove (2006, p.520), "[t]he potential for secondary use generates fear and uncertainty over how one's information will be used in the future, creating a sense of powerlessness and vulnerability." Therefore, we posit secondary use of personal information, which is also a dimension of CFIP, as a key dimension characterizing MUIPC.

Research Method

Scale Development

All research constructs are measured using seven-point Likert scale items (see the Appendix). Validated existing instruments were adapted for use as far as possible. *Secondary use of personal information* was measured by items adapted from Smith et al. (1996). *Perceived intrusion* was measured by items adapted from Xu et al. (2008). In our search for validated scales for *perceived surveillance*, we explored the literature but we were not able to find any rigorously validated instrument that captured perceived surveillance as a separate construct. Consistent with the best practices in instrument development, we

relied on our theoretical foundation to operationalize this construct. As we discussed earlier, surveillance was rooted from the dimension of collection from CFIP. Accordingly, existing scales from Smith et al. (1996) and Malhotra et al. (2004) were reviewed and modified to reflect the theoretical meaning of surveillance. This was followed by the construction of an initial set of items. These items were discussed with three fellow researchers with survey research background, and four active users of smartphones through face to face interviews. The initial set of items was modestly modified as a result of the comments we received from these interviews.

Following Stewart and Segars (2002)'s procedure to validate the higher-order factor structure of CFIP, we also measured *behavioral intention* using the items taken from Malhotra et al. (2004), and *prior privacy experience* using items taken from Smith et al. (1996). A pilot study was conducted among 76 graduate and undergraduate students to assess the clarity and conciseness of the survey instructions and questions, and evaluate the measurement model. A sub-group of these respondents (n=15) were contacted for a face-to-face interview so that their opinions and comments on the survey instructions and questions could be collected.

The final instrument of MUIPC used in this work consisted of three items for perceived surveillance, three items for perceived intrusion, and three items for secondary use of personal information. The final items of MUIPC and sources are presented in the Appendix. Throughout the scale development process, we invested significant amount of efforts to make sure that the wording of each item captured precisely, without confusion, the intended theoretical meaning of a specific dimension of MUIPC.

Survey Design

Data for instrument validation were obtained through an online survey that was administered to undergraduate and graduate students at a large university in the United States. The recruitment materials provided some background information about this study without disclosing too many details, and required that participants must own mobile phones to participate in the survey. There were total 346 participants. The responses from those participants who never owned a mobile phone or used any mobile app were dropped from the data analysis. Since participation of the study was completely voluntary, some respondents submitted empty or only partially filled questionnaires that were subsequently eliminated. A total of 310 responses were usable. Most of our participants had used mobile devices for at least one year (90%). In the mobile environment, college students are naturally a part of the population of interest, and they are avid users of various mobile apps (PEW-Internet 2010). Thus we assert that the use of college students as mobile consumers is appropriate.

Data Analysis and Results

The data analysis was divided into two stages: Stage I consisted of identifying the factor structure of MUIPC, and Stage II consisted of establishing the nomological validity of MUIPC.

Stage I: Identifying the Factor Structure of MUIPC

Since the construct of MUIPC was made of factors collected from existing scales as well as new items developed based on theory and prior literature, it was important to establish a proper factor structure of the MUIPC construct. Following the procedure presented in previous studies of establishing privacy measurement (Malhotra et al. 2004), we first conducted an exploratory factor analysis of the various factors of MUIPC, followed by confirmatory factor analysis.

The exploratory factor analysis (EFA) was conducted using the technique of Principal Components Analysis with VARIMAX rotation. As shown in Table 1, all items loaded cleanly on their respective constructs and there were no cross loadings. In EFA, the assessments of convergent validity were carried out by examining Cronbach Alpha, a reliability measure, for each factor (Bagozzi 1980). As shown in Table 1, the Cronbach Alpha was more than 0.7 for all the three constructs, which satisfied Nunnally's (1978) criteria for adequate convergent validity. Thus, these nine items were clearly divided across three dimensions (i.e., secondary use of personal information, perceived surveillance, and perceived intrusion), which represented a nine-item scale of MUIPC.

To further confirm the factor structure, we conducted confirmatory factor analysis (CFA) to confirm the factor structure derived from EFA (Smith et al. 1996). In this work, we followed the procedures of Stewart and Segars (2002) to conduct CFA that compares covariance matrices based on observed data and the hypothesized models. The observed covariance matrix in our case is a 9 x 9 matrix of the measures adopted to measure MUIPC. In CFA, this observed covariance matrix is compared with the implied matrix which is a set of covariances (9 x 9) generated through maximum likelihood estimation as a result of the hypothesized model (Stewart and Segars 2002). The results of the comparison between observed and implied matrix are then presented as the goodness of fit indices. The closer are the two models, the better is the model fit (the evidence demonstrating that the hypothesized model is indicative of the observed data). In line with prior literature (Bentler and Bonett 1980; Jöreskog and Sörbom 1993; Marsh and Hocevar 1988), the various fit indices were used for assessing the fit between the observed and the implied model.

Table 1: Results of Principal Component Analysis using Varimax Rotation

Factor	Items	Component			Cronbach's Alpha
		1	2	3	
Secondary Use of Personal Information	SUSE1	**.874**	.108	.128	0.891
	SUSE2	**.920**	.107	.118	
	SUSE3	**.888**	.119	.134	
Perceived Surveillance	SURV1	.159	.191	**.762**	0.801
	SURV2	.128	.147	**.840**	
	SURV3	.085	.226	**.844**	
Perceived Intrusion	INTR1	.125	**.863**	.160	0.860
	INTR2	.122	**.872**	.217	
	INTR3	.092	**.831**	.205	
Rotation Sum of Squared Loadings	Total	2.487	2.342	2.161	
	% Variance	27.630	26.025	24.007	
	Cumulative Variance	27.630	53.655	77.662	

Next, we used LISREL 8.54 for conducting CFA and tested four hypothesized models:

- ✓ Model 1 hypothesizes that all items of MUIPC form into a single factor, which accounts for all the common variance among the 9 items. Prior research (Culnan 1993; Dinev and Hart 2006; Smith et al. 1996) has measured privacy concern as if it were a unidimensional construct indicating that one first-order factor structure could explain the underlying data structure. If this model is accepted, then it is appropriate to consider MUIPC as a single dimension that governs similarities in variation among all 9 items.
- ✓ Model 2 hypothesizes that all items of MUIPC form into two first-order factors: secondary use of personal information was made to load onto a single factor whereas perceived surveillance and perceived intrusion were made to load onto the other factor. In this model, we argue that the three dimensions of MUIPC could fall into two categories: 1) users' perceptions of *surveillance* and *intrusion* that may be triggered at the *front-end* where personal information is collected and accessed from mobile devices; and 2) users' concerns over *secondary use of personal information* that may be triggered at the *back-end* where user data are transferred, stored and processed across different entities.
- ✓ Model 3 hypothesizes that all items of MUIPC form into three first-order factors: perceived surveillance, perceived intrusion, and secondary use of personal information. Smith et al. (1996) supported this structure of CFIP in their confirmatory factor analysis, which led to a practice of scaling CFIP by averaging the subscale scores to calculate an overall score. According to Stewart and

Segars (2002), the assumption of this model is that "every item is equally important in computing each factor and each factor is equally important in computing an overall score for CFIP (p.39)."

- ✓ Model 4 hypothesizes that all items form into three first-order factors which are measured by a second-order factor MUIPC. In such a model, "the inter-correlations among first-order factors form a system of interdependence (or covariation) that is itself important in measuring the construct. Conceptually, each factor and the second-order factor are necessary in capturing the nature of the construct domain (Stewart and Segars 2002, p.39)." In this case, MUIPC can be defined as three different factors as well as the structure of interrelationships among these factors.

The results of testing these four models are presented in Table 2. As shown in Table 2, Model 1 and Model 2 have very poor goodness of fit indices. The fit indices for both Model 3 and Model 4 are exactly identical, indicating no difference in the factor structure in these two models. We now discuss the indices of these two models (Model 3 and Model 4) in detail. As shown in Table 2, all the fit indices in terms of NFI, GFI, AGFI, CFI, NNFI, Std RMR and RMSEA demonstrate that the model fit for both Model 3 and 4 is satisfactory. Next we examine the convergent and discriminant validity of Model 3 and Model 4. The results of convergent validity analysis are shown in Table 3.

Table 2: Confirmatory factor analysis conducted for various factor structures using LISREL

Fit Indices	Recommended Indices	MODEL 1	MODEL 2	MODEL 3	MODEL 4
		Single Factor	Two First - Order Factors	Three First - Order Factors	Second - Order Factor
χ^2	--	807.08	540.95	42.81	42.81
df	--	27	26	24	24
Normed χ^2	< 3.00	29.89	20.81	1.78	1.78
NFI	> 0.90	0.59	0.74	0.98	0.98
GFI	> 0.90	0.63	0.72	0.97	0.97
AGFI	> 0.80	0.39	0.52	0.94	0.94
CFI	> 0.90	0.6	0.75	0.99	0.99
NNFI	> 0.90	0.47	0.65	0.99	0.99
Std RMR	< 0.05	0.18	0.19	0.028	0.028
RMSEA	< 0.08	0.306	0.253	0.063	0.063
Model CAIC		928.33	668.95	184.28	184.28
Sat CAIC		303.15	303.15	303.15	303.15

Note: The recommended indices are based on Jöreskog and Sörbom (1993)

From Table 3, we can infer that the psychometric properties for Model 3 and Model 4 are the same. The t-values obtained for the item loadings range from 12.40 to 20.21, indicating that all factor loadings are significant and providing evidence to support the convergent validity of the items measured (Anderson and Gerbing 1988). It has been shown in Table 1 that composite reliability, as a measure of internal consistency, is far in excess of 0.70 (Fornell and Larcker 1981), suggesting satisfactory levels of reliability for each factor. The average variance extracted (AVE) for each scale indicates the amount of variance extracted estimates far in excess of the 0.50 recommended level (Fornell and Larcker 1981). In sum, each first-order dimension seems to demonstrate robust properties of convergent validity.

The psychometric properties of Model 3 (first-order factor model) and Model 4 (second-order factor model) are further demonstrated in Figure 2. As shown in Model 4, the paths from the second-order factor of MUIPC to the first-order dimensions are strong and significant, indicating that the second-order factor model represents the structure of MUIPC more parsimoniously than the first-order factor model.

To assess the discriminant validity, we examine the correlations among the latent variables as shown in Table 4. As shown in Table 4, the correlations among latent variables are less than the square root of

AVEs along both the respective columns and rows. The correlations themselves are quite small. Hence, we can conclude that the measurement model exhibits strong properties of discriminant validity.

Table 3: Convergent Validity for Model 3 and Model 4

Constructs	ITEM	MODEL 3				MODEL 4			
		Std. Loading	t-value	Variance Extracted	Composite Reliability	Std. Loading	t-value	Variance Extracted	Composite Reliability
Secondary Use of Personal Information	SUSE1	0.81	16.64	0.75	0.90	0.81	16.64	0.75	0.90
	SUSE2	0.93	20.31			0.93	20.31		
	SUSE4	0.86	18.06			0.86	18.06		
Perceived Surveillance	SURV1	0.68	12.40	0.58	0.80	0.68	12.40	0.58	0.80
	SURV2	0.77	14.41			0.77	14.41		
	SURV3	0.83	15.81			0.83	15.81		
Perceived Intrusion	INTR1	0.81	16.29	0.68	0.86	0.81	16.29	0.68	0.86
	INTR2	0.89	18.43			0.89	18.43		
	INTR3	0.76	15.05			0.76	15.05		

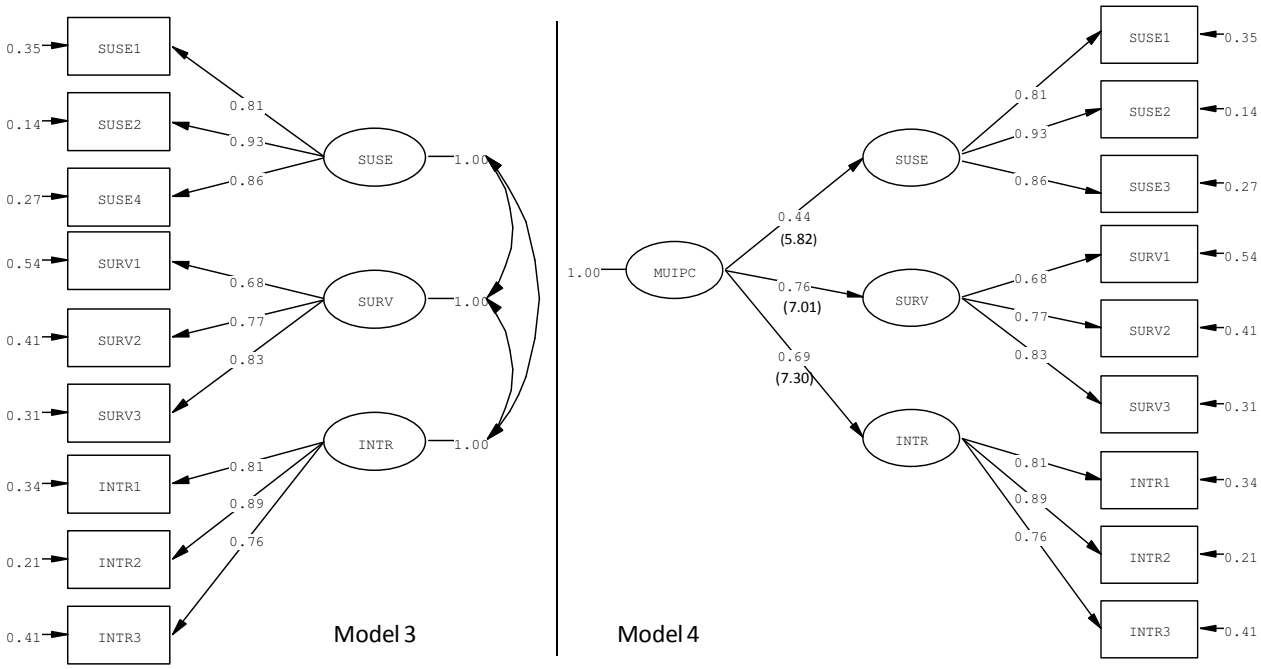


Figure 2: Convergent Validity for Model 3 and Model 4

Stage 2: Establishing the Nomological Validity of MUIPC

Following Stewart and Segars (2002), we tested the construct of MUIPC for nomological validity. According to Chin (1998), to establish the efficacy of a second-order model, it is important to assess its relationship with other constructs within the nomological network by embedding the second-order construct within a network of outcome variables and predictors to see if the second-order factor acts as a significant mediator. If a second order model of MUIPC is suggested by the data, then modeling of MUIPC within a network of other variables will provide further evidence of nomological validity (Stewart and Segars 2002). Following the procedure established by Stewart and Segars (2002), we placed MUIPC between its predictor variable (prior privacy experience) and outcome variable (behavioral intention).

Smith et al. (1996) positioned CFIP as a mediator between individual characteristics (e.g., prior privacy experience) and behavioral intention to use technology. Individuals who have been exposed to or been the victims of information abuses in the past are found to have stronger levels of privacy concerns (Smith et al. 1996). Therefore, we argue that MUIPC should behave as a consequent of prior privacy experience. Mobile consumers with high levels of prior privacy experiences should exhibit high levels of MUIPC.

Table 4: Correlations among Latent Variables

	SUSE	SURV	INTR
Secondary use of personal information (SUSE)	**0.86**		
Perceived Surveillance (SURV)	0.33	**0.80**	
Perceived Intrusion (INTR)	0.30	0.52	**0.92**

Note: The diagonal values are square root of AVEs for the respective construct

Regarding the predictor variable of MUIPC, individuals with higher levels of privacy concerns are more likely to decline information disclosure, and refuse to use a technology that demands data collection. The negative effect of privacy concerns on behavioral intention has been empirically supported in prior literature (Xu and Teo 2004). Hence, we expect a similar negative relationship between MUIPC and behavioral intention.

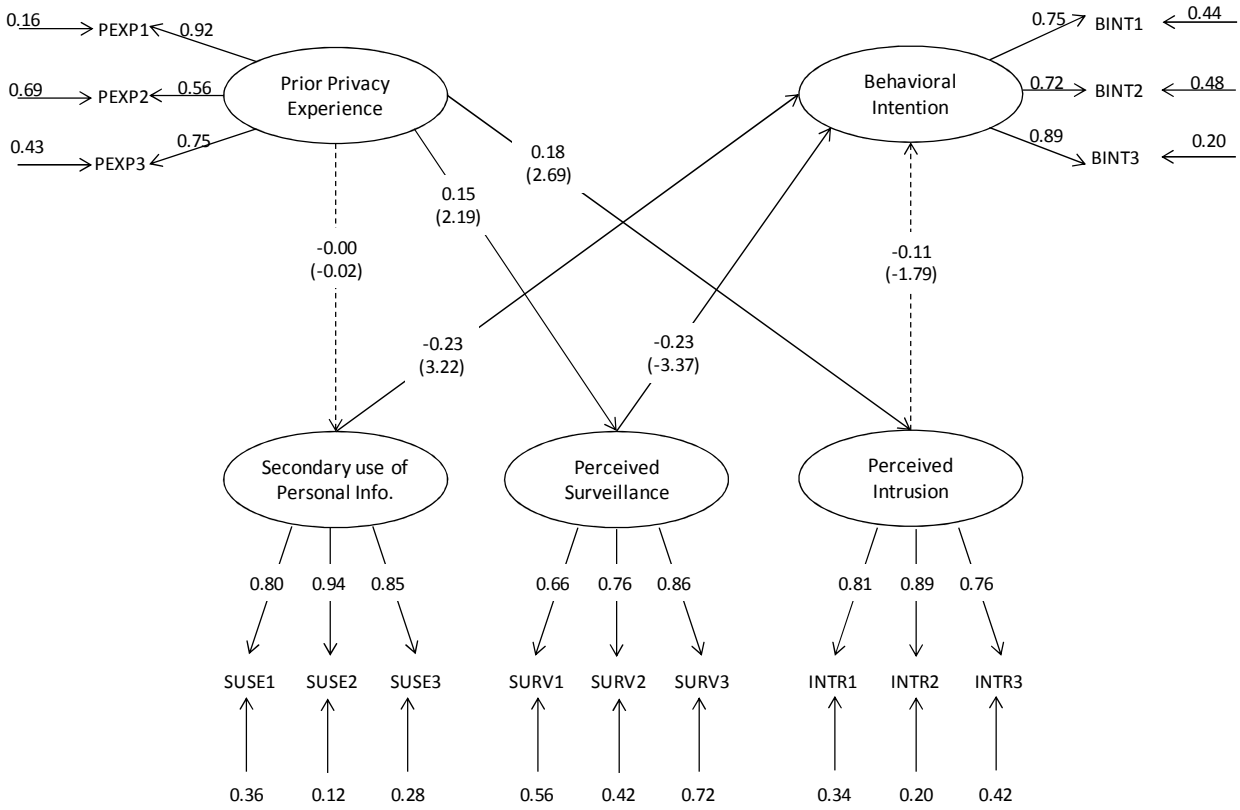
Using previously defined scales for prior privacy experience (Smith et al. 1996) and behavioral intention (Xu and Teo 2004), we expand the analysis of MUIPC using a 15 x 15 covariance matrix consisting of a nine-item MUIPC scale, a three-item prior privacy experience scale, and a three-item behavioral intention scale. The results of structural models for both first-order (Model 5) and second-order (Model 6) are presented in Table 5.

Table 5: Structural Analysis of First-Order and Second-Order MUIPC Scale in its Nomological Network

Fit Indices	Recommended Indices	First-Order Model	Second-Order Model
		Model 5	Model 6
χ^2	--	247	150.14
df	--	84	85
Normed χ^2	< 3.00	2.94	1.77
NFI	> 0.90	0.91	0.94
GFI	> 0.90	0.9	0.94
AGFI	> 0.80	0.86	0.91
CFI	> 0.90	0.94	0.97
NNFI	> 0.90	0.93	0.97
Std RMR	< 0.05	0.13	0.063
RMSEA	< 0.08	0.079	0.05
Model CAIC		489.51	385.92
Sat CAIC		808.39	808.39

From Table 5, we can infer that the fit indices in terms of Normed χ^2, GFI, AGFI, CFI, NNFI and RMSEA indicate good model fit for both Model 5 and Model 6. Std RMR is on the higher side for Model 5 whereas for Model 6, it indicates moderate fit. On comparing Model 5 and Model 6, we can infer that fit indices are better for Model 6 than Model 5. Figure 3 further illustrate Model 5 and associated estimates of MUIPC as a set of first-order factors that mediate the relationship between prior privacy experience and behavioral intention. The fit indices of Model 5 are lower than those observed for Model 3 and Model 4. However, according to Stewart and Segars 2002 (p.44), "given the complexity as well as the direction and

significance of paths, the model seems to provide a reasonable representation for the underlying covariance."



Note: Numbers are shown as standardized loadings (t-values)

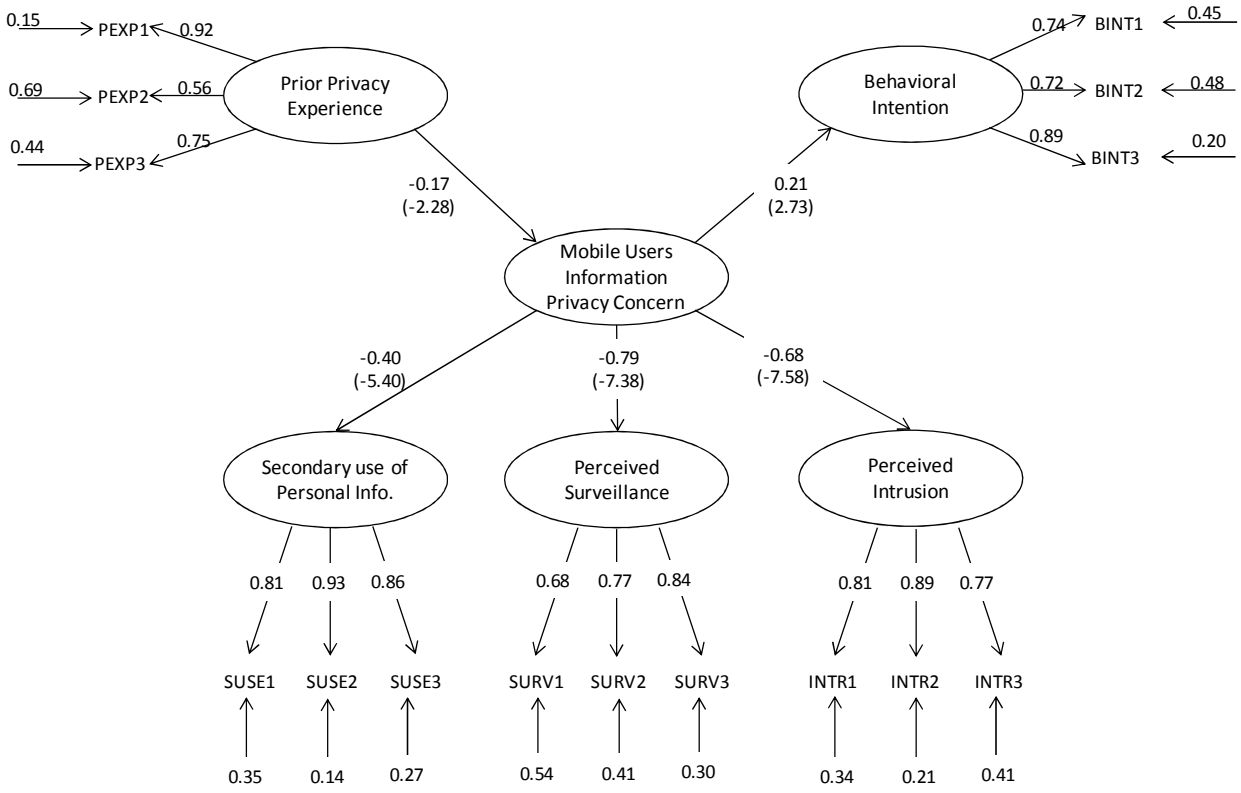
Figure 3: First-Order Factor Model of MUIPC within its Nomological Network

Figure 4 demonstrates the model and associated estimates of MUIPC as a second-order factor mediating the relationship between prior privacy experience and behavioral intention (Model 6). From Table 2, we can infer that the fit indices indicate a good fit considering the number of paths and number of constructs. The paths are all significant and consistent with the theoretical prediction. When compared to Model 5, Model 6 (second-order factor model) appears to have a better fit with more degrees of freedom. In addition, the path coefficients between MUIPC and the predictor and the outcome variables are higher than that for the first-order model. Given the theoretical support for the second-order structure of MUIPC, the results appear to confirm the conceptualization of MUIPC as a second-order structure, which is consistent with the structure of CFIP empirically confirmed by Stewart and Segars (2002) and the structure of IUIPC empirically confirmed by Malhotra et al. (2004).

Discussion and Conclusion

This study aims to respond to the call for a better understanding of mobile users' concerns for information privacy. As Xu et al. (2010, p.137) noted, "the Big Brother imagery looms in the popular press" where mobile apps are discussed. Such a ubiquitous and pervasive computing environment offers mobile users with anytime and anywhere access to network and services than has been the case with the Internet. Accordingly, privacy issues in such contexts become critically important as merchants and vendors may access a large volume of potentially sensitive personal information. Although several pioneering studies have examined privacy risks in the context of location-based services (e.g., Barkhuus and Dey 2003; Junglas et al. 2008; Xu et al. 2010), few studies have made systematic attempts to provide a theory-driven framework to specify the nature of privacy concerns among mobile consumers. To fill the gap in the

literature, this article is intended to examine mobile users' information privacy concerns (MUIPC) by extending the current literature centering on the Internet domain to the mobile environment.



Note: Numbers are shown as standardized loadings (t-values)

Figure 4: Second-Order Factor Model of MUIPC within its Nomological Network

Drawing on the CPM theory (Petronio 2002), we empirically measured MUIPC based on three dimensions through an online survey: perceived surveillance, perceived intrusion, and secondary use of personal information. The three-factor structure of MUIPC as revealed in exploratory factor analysis was further confirmed through confirmatory factor analysis. Further analysis revealed that the second-order model of MUIPC performed better than its first-order model. The second-order MUIPC exhibited desirable psychometric properties in the context of mobile environment, which is consistent with the second-order structure of CFIP (Stewart and Segars 2002) and that of IUIPC (Malhotra et al. 2004). The better fit indices in the case of second-order MUIPC scale not only imply that mobile users are concerned about all of these issues, but also suggest that the interdependencies among these three dimensions is an essential element of precisely measuring MUIPC.

Contribution

Smith et al.'s (1996) seminal work on information privacy laid a strong foundation for further work on consumer privacy. As Bansal et al. (2008) noted, the four dimensions of CFIP are aligned with the four principles of the Federal Trade Commission's (FTC) fair information practices (FTC 2000), including the stipulations and control that consumers be given: (a) *notice* on any activity that their personal information is being collected (mapped as *collection* of CFIP), (b) *consent* with regard to the appropriate use of the collected information (mapped as *unauthorized secondary use* of CFIP), (c) *access* to gathered personal information to assure data accuracy (mapped as *errors* of CFIP), and (d) *security* to prevent the accumulated information from unauthorized access (mapped as *improper access* of CFIP). Stewart and Segars (2002) further demonstrated that CFIP exhibits better psychometric properties when used as a second-order construct.

Along similar lines, Malhotra et al. (2004) defined the specific nature of privacy concerns in the Internet context and modeled IUIPC as a second-order construct. Drawing on the social contract and justice theories, IUIPC identifies three dimensions of privacy concerns that are aligned with different dimensions of social justice: (a) *collection* of personal information (rooted in the *distributive justice*), (b) *control* over personal information (rooted in the *procedural justice*), and (c) *awareness* of organizational privacy practices (rooted in the *interactional* and *information* justice).

By attempting to theorize privacy in the context of mobile users, we use the CPM theory to derive three dimensions of MUIPC, corresponding with the three boundary coordination rules (Petronio 2002), including (a) coordinating permeability rules, (b) coordinating ownership rules, and (c) coordinating linkage rules. In the mobile environment, we argue that users' perceptions of surveillance can be very salient due to aggressive data collection activities by mobile apps, which leads to the open boundary structure with high degree of information permeability. Meanwhile, the perceptions of intrusion could be triggered when ownership rules are violated, i.e., when mobile apps are able to make independent decisions about possessing or soliciting users' personal information. Lastly, mobile users' privacy concerns over secondary use of information can be very salient when linkage coordination rules are violated, i.e., when a new linkage to personal data occurs without users' awareness or consent. Table 6 summarizes the theoretical development of CFIP, IUIPC and our MUIPC.

Table 6. CFIP, IUIPC, and MUIPC

	CFIP (15-item scale)	**IUIPC (10-item scale)**	**MUIPC (9-item scale)**
Purpose	To reflect individuals' concern about organizational privacy practices.	To reflect Internet users' concerns about information privacy.	To reflect mobile users' concerns about information privacy.
Focus	Organizations' responsibilities for the proper handling of customer information	Individuals' subjective views of fairness within the context of information privacy.	Individuals' feelings that one has the right to own private information, either personally or collectively.
Dimensions & *Theoretical Foundation*	*Fair Information Practice Principles* ▪ Collection – *Notice* ▪ Unauthorized secondary use – *Consent* ▪ Error – *Access* ▪ Improper access – *Security*	*Social Contract and Justice theories* ▪ Collection – *Distributive justice* ▪ Control – *Procedural justice* ▪ Awareness of privacy practices – *Interactional and Information justice*	*Communication Privacy Management (CPM) theory* ▪ Perceived surveillance – *Permeability rules* ▪ Perceived intrusion – *Ownership rules* ▪ Secondary use of information – *Linkage rules*

Source: Adapted from Malhotra, Kim, and Agarwal (2004)

Seeing so many instruments of measuring privacy concerns (e.g., CFIP, IUIPC and now MUIPC) in literature, we may ask a question - "why another measurement for privacy concerns?" As discussed earlier, consumers' concerns for information privacy are not only different but more aggravated in the mobile environment. An Internet user may be able to easily hide his or her online identity, if he or she desires so. However, a smartphone is often identified by a unique phone ID number (Valentino-Devries 2010), rendering the potential intrusion of privacy a critical concern. In today's mobile environment, vendors and app developers take advantage of the powerful technological surveillance means to track and profile mobile consumers. The Wall Street Journal recently revealed that users' location data appears to be transmitted through mobile operating systems regardless of whether an app is running, and is tied to the phone's unique identifier (Angwin and Valentino-Devries 2011). Therefore, we argue that the concerns for information privacy are not only different, but also aggravated in the mobile environment. Comparing to online consumers, mobile users should have higher levels of fear that their activities may be watched, recorded, and transmitted to various entities. Hence, identifying the specific nature of MUIPC makes an important contribution to the field of information privacy.

Limitations and Conclusion

In generalizing the results of this study, we caution readers to interpret the results of confirmatory factor analysis very carefully. As Stewart and Segars (2002, p.45) put forth, "criteria for comparing models and assessing goodness-of-fit indices are relative and not absolute." In other words, any model can be a good representation of reality when they can be replicated in subsequent studies. The validity for MUIPC would be enhanced when it features well in the subsequent studies. Thus, this study calls for privacy research to further confirm the validity of MUIPC. Second, although our participants may fall in the target users for mobile apps, the generalizability of the findings to the general population may be affected. Future researchers should repeat this study with a more diverse sample for enhanced generalizability. Third, and by design, this research is limited to the instrument design of MUIPC. An extension of this study can place MUIPC in a much larger nomological network to examine its role in influencing a mobile consumer's real behavior. For instance, individuals' privacy interests have often been interpreted as an information exchange (Dinev and Hart 2006; Xu et al. 2010) where individuals reveal their personal information in return for certain benefits (e.g., improved search, locating friends, and obtaining deals). Future research can examine the influences of MUIPC in affecting an individual's privacy decision making in terms of cost-benefit analysis of information disclosure.

Recent headlines have highlighted aggressive practices of data access and transmission employed by mobile apps and operating systems. To address privacy issues in the mobile environment, we should first understand the very nature of mobile consumers' privacy concerns. This article introduced a 9-item scale of MUIPC, which was shown to reasonably convey the dimensionality of MUIPC, categorized as perceived surveillance, perceived intrusion, and secondary use of personal information. We hope that many researchers will employ the conceptual framework and the new instrument for further investigation and validation.

Acknowledgements

The authors are grateful to the associate editor and reviewers for their constructive comments on the earlier version of this manuscript. Heng Xu gratefully acknowledges the financial support of the U.S. National Science Foundation under grant CNS-0953749. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the U.S. National Science Foundation.

References

Anderson, J.C., and Gerbing, D.W. 1988. "Structural Equation Modeling in Practice: A Review and Recommended Two-Step Approach," *Psychological Bulletin* (103:3 (Fall)), pp 411-423.

Angst, C.M., and Agarwal, R. 2009. "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion," *MIS Quarterly* (33:2), pp 339-370.

Angwin, J., and Valentino-Devries, J. 2011. "Apple, Google Collect User Data," in: *The Wall Street Journal*.

Bagozzi, R.P. 1980. *Causal Methods in Marketing*. New York: John Wiley and Sons.

Bansal, G., Zahedi, F., and Gefen, D. 2008. "The Moderating Influence of Privacy Concern on the Efficacy of Privacy Assurance Mechanisms for Building Trust: A Multiple-Context Investigation," *Proceedings of 29th Annual International Conference on Information Systems (ICIS 2008)*, Paris, France.

Barkhuus, L., and Dey, A. 2003. "Location-Based Services for Mobile Telephony: A Study of User's Privacy Concerns," *Proceedings of the 9th IFIP TC13 International Conference on Human-Computer Interaction (INTERACT)*, Zurich, Switzerland, pp. 709-712.

Bélanger, F., and Crossler, R.E. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly* (35:4), pp 1017-1041.

Bentler, P.M., and Bonett, D.G. 1980. "Significance Tests and Goodness of Fit in the Analysis of Covariance Structures," *Psychological Bulletin* (88:3), pp 588-606.

Child, J.T., Pearson, J.C., and Petronio, S. 2009. "Blogging, Communication, and Privacy Management: Development of the Blogging Privacy Management Measure," *Journal of the American Society for Information Science and Technology* (60:10), pp 2079-2094.

Chin, W.W. 1998. "Issues and Opinion on Structural Equation Modeling," *MIS Quarterly* (22:1), pp VII-XVI.

Culnan, M.J. 1993. "'How Did They Get My Name'? An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use," *MIS Quarterly* (17:3), pp 341-363.

Culnan, M.J., and Williams, C.C. 2009. "How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and Tjx Data Breaches," *MIS Quarterly* (33:4), pp 673-687.

Dignan, L. 2011. "Google's Android Wears Big Bullseye for Mobile Malware." *ZDNet*, from http://www.zdnet.com/blog/btl/googles-android-wears-big-bullseye-for-mobile-malware/45733

Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (17:1), pp 61-80.

Fornell, C., and Larcker, D. 1981. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research* (18), pp 39-50.

FTC. 2000. "Privacy Online: Fair Information Practices in the Electronic Marketplace " Retrieved April 1, 2005, from http://www.ftc.gov/reports/privacy2000/privacy2000.pdf

FTC. 2009. "Beyond Voice: Mapping the Mobile Marketplace." from www.ftc.gov/opa/2009/04/mobilerpt.shtm

Gartner. 2012. "Gartner Identifies 10 Consumer Mobile Applications to Watch in 2012." from http://www.gartner.com/it/page.jsp?id=1544815

Jin, S.A.A. 2012. ""To Disclose or Not to Disclose, That Is the Question": A Structural Equation Modeling Approach to Communication Privacy Management in E-Health," *Computers in Human Behavior* (28:1), pp 69-77.

Jöreskog, K.G., and Sörbom, D. 1993. *Lisrel8: Structural Equation Modeling with Simplis Command Language*, (2nd ed.). Chicago, IL: Scientific Software International.

Junglas, I.A., Johnson, N.A., and Spitzmüller, C. 2008. "Personality Traits and Concern for Privacy: An Empirical Study in the Context of Location-Based Services," *European Journal of Information Systems* (17:4), pp 387-402.

Malhotra, N.K., Kim, S.S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (Iuipc): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), December, pp 336-355.

Marsh, H.W., and Hocevar, D. 1988. "A New, More Powerful Approach to Multitrait-Multimethod Analyses: Application of Second-Order Confirmatory Factor Analysis," *Journal of Applied Psychology* (73:1 (February)), pp 107-117.

Nunnally, J.C. 1978. *Psychometric Theory*, (2nd ed.). New York: McGraw-Hill.

Petronio, S. 2002. *Boundaries of Privacy: Dialectics of Disclosure*. Albany: State University of New York Press.

Petronio, S. 2010. "Communication Privacy Management Theory: What Do We Know About Family Privacy Regulation?," *Journal of Family Theory & Review* (2:3), pp 175–196.

PEW-Internet. 2010. "Pew Internet & American Life Project: Mobile Access 2010 ", from http://www.pewinternet.org/Reports/2010/Mobile-Access-2010.aspx

Smith, H.J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp 989-1015.

Smith, H.J., Milberg, J.S., and Burke, J.S. 1996. "Information Privacy: Measuring Individuals' Concerns About Organizational Practices," *MIS Quarterly* (20:2), June, pp 167-196.

Solove, D.J. 2006. "A Taxonomy of Privacy," *University of Pennsylvania Law Review* (154:3), pp 477-560.

Stewart, K.A., and Segars, A.H. 2002. "An Empirical Examination of the Concern for Information Privacy Instrument," *Information Systems Research* (13:1), pp 36-49.

Thurm, S., and Kane, Y.I. 2010. "Your Apps Are Watching You: A Wsj Investigation Finds That Iphone and Android Apps Are Breaching the Privacy of Smartphone Users," in: *The Wall Street Journal*.

Valentino-Devries, J. 2010. "Unique Phone Id Numbers Explained," in: *The Wall Street Journal*.

Van Slyke, C., Shim, J.T., Johnson, R., and Jiang, J.J. 2006. "Concern for Information Privacy and Online Consumer Purchasing," *Journal of the Association for Information Systems* (7:6), pp 415-444.

Xu, H., Dinev, T., Smith, H.J., and Hart, P. 2008. "Examining the Formation of Individual's Information Privacy Concerns: Toward an Integrative View," *Proceedings of 29th Annual International Conference on Information Systems (ICIS 2008)*, Paris, France.

Xu, H., Dinev, T., Smith, H.J., and Hart, P. 2011. "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances," *Journal of the Association for Information Systems* (12:12), pp 798-824.

Xu, H., and Teo, H.H. 2004. "Alleviating Consumer's Privacy Concern in Location-Based Services: A Psychological Control Perspective," *Proceedings of the Twenty-Fifth Annual International Conference on Information Systems (ICIS 2004)*, Washington, D. C., United States, pp. 793-806.

Xu, H., Teo, H.H., Tan, B.C.Y., and Agarwal, R. 2010. "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services," *Journal of Management Information Systems* (26:3), pp 135-174.

Appendix: Research Constructs and Measures

Perceived surveillance (self-developed)

(1) I believe that the location of my mobile device is monitored at least part of the time.
(2) I am concerned that mobile apps are collecting too much information about me.
(3) I am concerned that mobile apps may monitor my activities on my mobile device.

Perceived intrusion (Xu et al. 2008)

(1) I feel that as a result of my using mobile apps, others know about me more than I am comfortable with.
(2) I believe that as a result of my using mobile apps, information about me that I consider private is now more readily available to others than I would want.
(3) I feel that as a result of my using mobile apps, information about me is out there that, if used, will invade my privacy.

Secondary use of personal information (Smith et al. 1996)

(1) I am concerned that mobile apps may use my personal information for other purposes without notifying me or getting my authorization.
(2) When I give personal information to use mobile apps, I am concerned that apps may use my information for other purposes.
(3) I am concerned that mobile apps may share my personal information with other entities without getting my authorization.

Prior Privacy Experience (Smith et al. 1996)

(1) How often have you personally experienced incidents whereby your personal information was used by some company or e-commerce web site without your authorization?
(2) How much have you heard or read during the last year about the use and potential misuse of the information collected from the Internet?
(3) How often have you personally been the victim of what you felt was an improper invasion of privacy?

Behavioral Intention (Xu et al. 2004)

(1) I am likely to disclose my personal information to use mobile apps in the next 12 months.
(2) I predict I would use mobile apps in the next 12 months.
(3) I intend to use mobile apps in the next 12 months.