Mobile Applications and Access to Personal Information: A Discussion of Users' Privacy Concerns

Completed Research Paper

Kenan Degirmenci
Leibniz Universität Hannover
Königsworther Platz 1
30167 Hannover, Germany
degirmenci@iwi.uni-hannover.de

Nadine Guhr
Leibniz Universität Hannover
Königsworther Platz 1
30167 Hannover, Germany
guhr@iwi.uni-hannover.de

Michael H. Breitner
Leibniz Universität Hannover
Königsworther Platz 1
30167 Hannover, Germany
breitner@iwi.uni-hannover.de

Abstract

Mobile applications (apps) have become highly popular and are creating new economic opportunities for app providers, developers, software companies, and advertisers. Due to the access to personal information, mobile apps may pose a threat to users' privacy, which can incite users not to install or to uninstall mobile apps. In the last twenty years, concerns for information privacy (CFIP) have been investigated by several studies, which adapted CFIP to an online and to a mobile context. Our extended approach for mobile users' information privacy concerns (MUIPC) analyzes four dimensions of access to personal information, i.e., personal identity, location, device content, and system and network settings. By conducting an online survey with 474 participants, we test the influence of these dimensions on MUIPC with a structural equation model (SEM). Three dimensions are found to be significantly influential. The results are discussed and implications for research and practice are given.

Keywords: Mobile applications, access to personal information, privacy concerns, online survey, multivariate analysis methods

Introduction

Since the widespread adoption of mobile devices such as smartphones and tablet computers, mobile applications (apps) have become highly popular and are creating new economic opportunities for app providers, developers, software companies, and advertisers (Anthes 2011). According to ABI Research (2012), mobile apps will continue to generate revenues from pay-per-download, in-app purchase, subscriptions, and in-app advertising, growing from $8.5 billion in 2011 to $46 billion in 2016. However, the use of mobile apps is often associated with privacy concerns (Keith et al. 2012; Soper 2012; Xu et al. 2012a). In this context, mobile access to personal information and related privacy concerns have been discussed by several researchers (e.g., Enck 2011; Najjar and Bui 2012). To make full use of their potential, mobile apps need to access certain functions. For example, the Google Maps mobile app requests access to the Global Positioning System (GPS) receiver of mobile devices to provide users with its navigation system, and as a result, a user's location is exposed. While this function is fundamental for the functioning of the navigation system of the Google Maps mobile app, access is requested unnecessarily in a number of cases (Enck 2011). Access to personal information, i.e., personal identity, location, device content, and system and network settings, can incite users not to install or to uninstall mobile apps. In a survey of 714 mobile app users, the Pew Research Center found that 54% of the respondents had decided not to install and 30% had decided to uninstall mobile apps due to privacy concerns about their personal information (Pew Internet 2012). Mobile users fear their personal information might be misused by malicious apps, which are predicted to proliferate quickly on mobile platforms (Leavitt 2011).

Like with Google Android version 4.2.2 (Jelly Bean), iOS 6 mobile apps ask for permission to access users' personal information. In contrast to Android, iOS 6 users can turn off access in the privacy settings. As a reaction to mobile users' privacy concerns, Apple recently changed the privacy settings with the release of iOS 6 (Apple 2013). This change implies that not only can mobile users turn off access to location, they can also restrict access to contacts, calendars, reminders, photos, Bluetooth sharing, and access to Twitter and Facebook accounts if supported by the mobile app. App providers face the challenge of both considering privacy concerns of their users and implementing measures to alleviate those concerns. Therefore, it is important to examine the balance of information privacy concerns with the advantages of location-based services (Bélanger and Crossler 2011) and other advantages derived from access to personal information.

The purpose of this paper is to investigate how access to personal information affects mobile users' information privacy concerns (MUIPC). MUIPC is measured using three dimensions: perceived surveillance, perceived intrusion, and secondary use of personal information (Xu et al. 2012a). Following Smith et al. (1996), Stewart and Segars (2002) called for research investigating antecedents and consequences of information privacy concerns. In our study, we focus on access to personal information as an antecedent to mobile users' privacy concerns. This approach attempts to offer recommendations for app providers to better address the challenge of reducing users' concerns for information privacy when they wish to install and use mobile apps.

Against this backdrop, the article focuses on the following. First, we identify various types of access to personal information that might affect mobile users' privacy concerns. Second, we offer an operationalization of access to personal information in order to measure the influence on MUIPC. Third, we propose and test a causal model on the relationship between access to personal information and MUIPC. This paper makes a theoretical contribution by conceptualizing that mobile users' privacy concerns are noticeably affected by access to their personal information. An increasing number of studies within IS research investigate mobile app security and privacy. However, a review of the literature suggests that the influence of access to personal information on mobile users' privacy concerns has not yet been addressed. This paper aims to fill this research gap. We explore the following research question:

Which type of access to personal information has a major influence on mobile users' privacy concerns?

This paper is structured as follows: first, we give a holistic literature review on the field of mobile applications and outline identified types of access to personal information. After presenting the generated hypotheses, we describe the research design and report the results of our field study of mobile users who regularly use mobile apps. Following the discussion of our findings, we give implications for research and practice. Finally, limitations and conclusions are presented.

Foundations, Conceptual Basis, and Hypotheses Generation

Mobile Applications and the Role of Mobile Application Security and Privacy in Information Systems Research

To give a holistic overview of the current research in the mobile application area, a literature review was conducted on the six major IS research databases: ACM, AISeL, IEEE, Science Direct, EBSCOhost, and SpringerLink. We used "mobile application" as a search keyword (and also "mobile applications", "mobile apps", and "mobile app"), and intensively analyzed the literature for relevance. Mobile apps are a relatively new topic in IS research, and there are two dominant streams in this area: mobile application development and mobile application security and privacy. Literature in the field of mobile application development focuses on the mobile operating systems Apple iOS and Google Android (e.g., Bergvall-Kåreborn et al. 2010; Gavalas and Economou 2011; Qiu et al. 2011). Bergvall-Kåreborn et al. (2010) outline benefits and drawbacks of Apple and Google from the developers' point of view by interviewing 49 iOS and Android developers. Another qualitative study conducted by Qiu et al. (2011) identifies and analyzes ideation, execution, and marketing as app developers' entrepreneurial areas. Further research in this field compares various runtime environments such as Java ME, .NET Compact Framework, Flash Lite, and Android, which, for example, are reviewed by Gavalas and Economou (2011). Golding and Donaldson (2009) adapt the design science paradigm for the development of mobile apps, and there is literature dealing with design characteristics of mobile apps (e.g., compatibility and functionality) and how they affect attitudes toward and adoption of mobile apps (Hu et al. 2012; Kim 2012).

The other stream in the mobile application area, mobile application security and privacy, often deals with location-based services. For example, Keith et al. (2010) discuss ethical aspects of the use of mobile apps with regard to personal location information. By means of an experiment with mobile app users, they conclude that location privacy concerns depend on location privacy assurance and the size of the base of app users. Xu et al. (2012b) focus more deeply on location privacy assurance, and empirically validate that privacy concerns are affected by a person's perceived control over personal information. Other research investigates location information disclosure as an exchange of benefits and risks (e.g., Keith et al. 2012; Xu et al. 2010) based on the privacy calculus theory, which describes the willingness to provide personal information (see privacy calculus theory in Culnan and Armstrong 1999; Dinev and Hart 2006; Laufer and Wolfe 1977). In terms of the privacy calculus theory, Najjar and Bui (2012) develop a theoretical framework and link benefits and risks to perceived value, resulting in an intention to allow access to personal information. They focus on the benefits and risks of the use of mobile apps, and mention some of the personal information that can be accessed when someone downloads, installs, and uses mobile apps, such as the smartphone's memory card, phone calls, messages, contact lists, user's accounts, location information, etc. However, the access rights are not integrated into their proposed theoretical framework. The intention to allow access to personal information is often associated with permissions, which are divided into time-of-use and install-time (Enck 2011): "A time-of-use permission is approved by the user when the application executes a sensitive operation, e.g., iOS's prompt to allow an application access to location. An install-time permission is approved by the user when the application is installed. For Android, this is the user's only opportunity to deny access; the user must accept all permission requests or not install the application." (p. 52). Enck (2011) further describes some of the permissions and discusses their necessity in the context of the danger for the users in allowing malicious mobile apps to access their personal information.

In addition to these two streams, research in the mobile application area has focused on the success of mobile apps (e.g., Dhar and Varshney 2011; Ghose and Han 2012; Kajanan et al. 2012; Lee and Raghu 2011; Liu et al. 2012), location-based services (e.g., Barbeau et al. 2011; Lehrer et al. 2011), online word-of-mouth and trust (e.g., Hao et al. 2011; Yan et al. 2010), and user acceptance of mobile apps (e.g., Chen et al. 2012). Zhang et al. (2009) conducted a literature review on mobile apps and examined research methodology perspectives. They present a list of potential future research questions regarding relevant topics in the field of mobile applications.

Mobile Users' Information Privacy Concerns (MUIPC)

The MUIPC instrument was introduced by Xu et al. (2012a), and it is based on the scale of concern for information privacy (CFIP), developed and validated by Smith et al. (1996). An empirical confirmation of the CFIP scale's reliability and validity by Stewart and Segars (2002) followed. Then, Malhotra et al. (2004) adapted the instrument to an online environment, developing the scale of Internet Users' Information Privacy Concerns (IUIPC). The investigation of information privacy concerns attributes to scholars' efforts in trying to understand individuals' assessment of benefits and risks to provide personal information to companies (e.g., Culnan and Armstrong 1999; Dinev and Hart 2006; Hui et al. 2007; Keith et al. 2012; Xu et al. 2010). A number of studies focused on the risks, particularly on privacy concerns. The CFIP scale measures "individuals' concerns about organizational information privacy practices" with four subscales: collection, errors, unauthorized secondary use, and improper access (Smith et al. 1996, p. 169). Collection describes individuals' perception that "great quantities of data regarding their personalities, background, and actions are being accumulated" (Smith et al. 1996, p. 171). The collection of personal information enables companies to use this information about individuals in relationship marketing and to target offers more accurately to individuals' interests (Culnan and Armstrong 1999). Due to errors and improper access, individuals become concerned that companies should take more measures to reduce errors and control access to personal information (Smith et al. 1996). With regard to companies' potential opportunistic behaviors (Laufer and Wolfe 1977), unauthorized secondary use refers to the selling or sharing of a person's information without their authorization (Smith et al. 1996). Referring to Malhotra et al. (2004), IUIPC draws on the social contract and justice theories, identifying three dimensions of privacy concerns: collection of personal information (distributive justice), control over personal information (procedural justice), and awareness of organizational information privacy practices (interactional and informational justice).

Drawing on the communication privacy management theory, MUIPC theorizes privacy in the context of mobile users and presents three dimensions to measure mobile users' privacy concerns: perceived surveillance, perceived intrusion, and secondary use of personal information. Perceived surveillance expands the collection factor from CFIP and IUIPC by mobile technology capabilities for tracking and profiling mobile users (Xu et al. 2012a). Mobile devices differentiate from other IS technologies, among other characteristics, because they are equipped with environment sensors such as GPS, integrated cameras, etc. (Enck 2011). Thus, these sensors enhance mobile users' tasks, but otherwise evoke concerns about personal information. Surveillance is defined as "the watching, listening to, or recording of an individual's activities" (Solove 2006, p. 490). According to Xu et al. (2012a), perceived intrusion implies access due to CFIP dimensions errors and improper access, as well as the control dimension in IUIPC. Solove (2006) defines intrusion as "invasions or incursions into one's life," which disturb "the victim's daily activities, alters her routines, destroys her solitude, and often makes her feel uncomfortable and uneasy" (p. 549). Secondary use of personal information, which is also a dimension of CFIP, is defined as "the use of data for purposes unrelated to the purposes for which the data was initially collected without the data subject's consent" (Solove 2006, p. 519). Secondary use is described as an asymmetry of knowledge, because individuals are exposed to the uncertainty that they are likely to know little or nothing about the circumstances under which their personal information is captured, sold, or processed, which creates "a sense of powerlessness and vulnerability" (Solove 2006, p. 519).

Access to Personal Information

Mobile users are faced with the decision to allow access to their personal information in order to use mobile apps. To gain a deeper insight into the different kind of access rights, we selected twelve popular mobile apps with an equal distribution of various categories: Facebook and Twitter (Social), Google Maps (Travel & Local), WhatsApp Messenger and Skype (Communication), Angry Birds and Fruit Ninja Free (Games), YouTube (Media & Video), Adobe Reader and Dropbox (Productivity), Google Search (Tools), and Shazam (Music & Audio). With regard to permissions, iOS asks for access to location services, contacts, calendars, reminders, photos, Bluetooth sharing, and access to the Twitter and Facebook account. For a more detailed view, we installed the selected apps and identified permissions using a Samsung Galaxy Nexus with Android version 4.2.2 (Jelly Bean). The analysis of the twelve apps resulted in a request for 56 permissions, of which we present the most common 17 permissions in Table 1 (six or more of the tested apps requested these permissions).

Table 1. List of Common Permissions

Categories	**Permissions**
Phone calls	Read phone status and identity
Microphone	Record audio
Your location	Approximate location (network-based)
	Precise location (GPS and network-based)
Your social information	Read your contacts
Storage	Modify or delete the contents of your USB storage
Your accounts	Add or remove accounts
	Find accounts on the device
	Use accounts on the device
Network communication	Full network access
	Receive data from Internet
	View network connections
	View Wi-Fi connections
Affects Battery	Control vibration
	Prevent phone from sleeping
Sync settings	Read sync settings
System tools	Test access to protected storage

The permissions are further described when tapped on, while some permissions point out that access may harm the user if the app is malicious. For example, permission to directly call phone numbers is requested, indicating that malicious apps may cost the user money by making calls without the user's confirmation. Referring to the permission to read contacts, the user is advised that malicious apps may share contact data without the user's knowledge. There are further similar permissions, e.g., relating to sending text messages, to receiving data from the Internet, or modifying system settings, which could cost the user money, cause excess data usage, or corrupt the user's system configuration.

Access to personal information can be perceived by individuals as an intrusion into their privacy and in general, access by mobile apps may pose a threat to users' privacy (Najjar and Bui 2012). To consider the access to personal information in a more differentiated view, we categorize access to personal information into four dimensions: personal identity, location, device content, and system and network settings (see Figure 1).

Mobile devices are considered to be "an expression of our personality" (Meschtscherjakov 2009) and contain comprehensive information about the user's identity (e.g., name, contact information, phone number, etc.). The access to identity-related information can be of concern to users. For example, the Wall Street Journal examined 101 mobile apps, of which 56 transmitted the phone's unique device ID to other companies without users' awareness or consent (Thurm and Kane 2010). Mobile users can perceive a potential misuse of information that may result in identity theft leading to the selling or sharing of their personal identity information without their authorization (Keith et al. 2012; Najjar and Bui 2012). Retrieved identity-related information might be used for unwanted solicitations, more personalized spam email and junk mail (Keith et al. 2010). Personal identity forms the first dimension of access to personal information, and it indicates that mobile apps can identify the user and may send the user's profile information to other entities.

H^1: Access to personal identity has a significant positive influence on MUIPC.

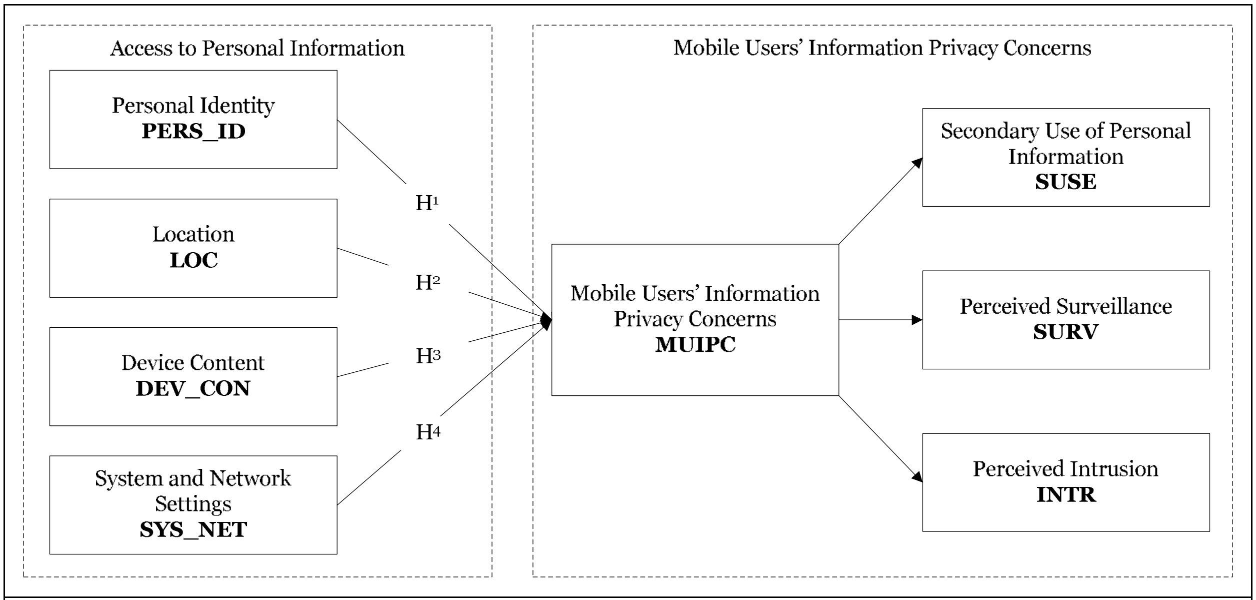
Access to Personal Information
Personal Identity
PERS_ID
Location
LOC
Device Content
DEV_CON
System and Network Settings
SYS_NET
H1
H2
H3
H4
Mobile Users' Information Privacy Concerns
Mobile Users' Information Privacy Concerns
MUIPC
Secondary Use of Personal Information
SUSE
Perceived Surveillance
SURV
Perceived Intrusion
INTR

Figure 1. Research Model

The second dimension describes access to users' location. Location-based services (LBS) have attracted considerable attention due to the potential for personalized and context-aware services (Dhar and Varshney 2011). Access to location-related information allows mobile apps to get users' approximate and precise location derived by location services using GPS or network location sources such as cell towers and Wi-Fi. LBS offer diverse benefits for personal purposes, for example, requesting driving directions to nearby gas stations, hotels, local airports, nearby attractions, or restaurants, as well as societal purposes like reducing traffic congestion, improving urban planning, arresting the spread of disease, or studying interpersonal interactions (Soper 2012). Companies like Google, Yahoo, Facebook, Foursquare, and many others use location information to provide value-added services to users (Xu et al. 2012b). However, LBS evoke mobile users' privacy concerns, because their position is tracked, or they are spammed with mobile advertising (Keith et al. 2012). Hence, we propose the following hypothesis:

H^2: Access to location has a significant positive influence on MUIPC.

Device content refers to information stored on mobile devices that may provide value for users in specific contexts. Allowing mobile apps to write to the storage of mobile devices implies the modification or deletion of the storage contents, which could result in unwanted intrusion. The storage often contains sensitive information such as contacts, photos, videos, calendar events, reminders, browser bookmarks and navigation history, etc. Integrated cameras are a standard feature of mobile devices, and with the permission of the user, mobile apps are allowed to take photos and videos with the camera at any time without confirmation. For example, mobile social networking apps use the camera of mobile devices, process photos and videos, transfer private messages from one user to another, etc., which is why users' privacy is a serious challenge for app developers (Jabeur et al. 2013). Communication apps such as WhatsApp Messenger transfer sensitive text messages, and productivity apps like Dropbox have access to private files as well as sensitive company data that is stored on mobile devices. Giving mobile apps permission to read or modify calendar events and reminders also enables the apps to share or save this kind of data, regardless of confidentiality or sensitivity. Access to mobile browser's bookmarks and navigation history allows mobile apps to read all of the browser's bookmarks saved on the mobile device, as well as to read the history of all websites that the browser has visited. Thus, mobile apps can put content in a user-centered context, and process data such as user preferences, information needs, and personal time schedule (Zhang et al. 2009). Due to the confidentiality and sensitivity of mobile devices' content, we hypothesize:

H^3: Access to device content has a significant positive influence on MUIPC.

The fourth dimension deals with system and network settings, which relate to configuration preferences for system components and network connections on mobile devices. System components include the configuration of several functions of the mobile device, e.g., vibration, alarm, or screen lock. With regard to network connections, the access allows mobile apps to view, change, and control network connections such as Wi-Fi connections, Near Field Communication (NFC), and Bluetooth. Mobile users benefit from networking standards like Wi-Fi, which provides fast internet connectivity, or short-range communication technologies such as NFC for services like mobile payment, or Bluetooth for data synchronization, headset applications, etc. However, access to network connections enables malicious apps to intercept and control users' data (Leavitt 2011). Due to a potential risk of privacy intrusion through the access to system and network settings, we posit:

H4: Access to system and network settings has a significant positive influence on MUIPC.

Research Design and Methodology

Survey Design

Acknowledging the challenges associated with gaining acceptable empirical data in the critical domain of privacy concerns in the context of mobile applications, we chose the survey methodology to collect empirical data and multivariate analysis methods to test the revised model statistically. To increase content validity, the questionnaire was pre-tested twice. Two pilot studies were conducted among participants to assess the conciseness and clarity of the survey questions and instructions, and evaluate the measurement models. Participation in the study was completely voluntary, and in the final study incentives in the form of two $25 Amazon vouchers were offered. Offering incentives to subjects in exchange for participation is well applied in survey methodology (Xu et al. 2012b). In the first pilot study a total of 161 subjects participated, with 98 producing usable data (61 percent). In the second pilot study a total of 56 subjects participated, with 40 producing usable data (71 percent). Comments and opinions on the survey questions were collected and used to revise the final questionnaire and to modify several items, especially in their wording. Furthermore, as described by Johnston and Warkentin (2010), content validity for the instrument scales was established through a content validity expert panel comprised of ten doctoral and faculty students who were skilled in quantitative research methods and analysis. For the final study, with participants from the USA, we used two approaches to collect empirical data. First, we used online networking websites with an international focus (LinkedIn), Android and iOS forums, and American university groups on Facebook. We recruited participants by posting announcements on those websites. The posting provided some background information about the study and the subjects could easily participate by using the URL provided in the posting. Second, we contacted potential participants from the USA via email. In the final study a total of 775 subjects participated, with 474 producing usable data (61 percent), see Table A1, of which 61.4% use Apple iOS, 34.4% Google Android, 2.1% BlackBerry OS, and 1.3% Windows Phone. The remaining 0.8% of participants were using other operating systems that were not specified. The survey consists of closed-ended questions on a five-point Likert scale. The respondents were instructed to indicate how strongly they agree or disagree with a number of statements relating to their privacy concerns when using mobile apps and their feelings concerning the intrusion if mobile apps are able to access to different information, data, application, etc. (e.g., contact information, call logs, approximate location, and the browser's navigation history).

Measurement and Instrumentation

Overall, seven constructs were measured in this study using five-point Likert scale items. Access to personal information, which is represented by Personal Identity (PERS_ID), Location (LOC), Device Content (DEV_CON), System and Network Settings (SYS_NET) as first-order factors as well as a second-order MUIPC with three first-order dimensions: Secondary Use of Personal Information (SUSE), Surveillance (SURV), and Intrusion (INTR) (Xu et al. 2012a). By enabling the collection of complex concepts in comparatively simple abstractions, multidimensional constructs such as second-order constructs provide opportunities to advance research (Polites et al. 2012) and increase the realism in empirical models (Edwards 2001). While Smith et al. (1996) operationalize CFIP as a first-order construct, Stewart and Segars (2002) as well as Angst and Agarwal (2009) demonstrated that CFIP was indeed a second-order phenomenon (Malhotra et al. 2004; Xu et al. 2012b). As mentioned by Jarvis et al. (2003), the historical roots of this type of model can be traced back to the work of Gerbing and Anderson (1984) and Bentler and Weeks (1980). The conceptualization in this manner avoids several problems in the interpretation of the role of MUIPC in the structural model. "Of course, some researchers might argue that a construct must be conceptually and empirically unidimensional to be meaningful," nevertheless "such a view is often inconsistent with the way constructs are defined" (Jarvis et al. 2003, p. 204). If all indicators are bundled together, the explication of the construct is not complete (Gerbing et al. 1994) and finally it would be difficult to ascertain the contribution of each domain on the overall construct (Koufteros et al. 2009). This could be the case if, for example, all indicators are bundled together through just one first-order latent variable (Koufteros et al. 2009). Therefore, a first-order model with multiple factors makes it difficult for researchers to clearly interpret the relationship between MUIPC and the research variables of interest. However, the second-order model does not suffer from these problems. Furthermore, Xu et al. 2012a argue that "the second-order factor model represents the structure of MUIPC more parsimoniously than the first-order factor model" (p. 8). Therefore, we conceptualize MUIPC as a second-order construct, because it is theoretically sound, substantively meaningful, operationally convenient, and empirically justified.

The constructs of access to personal information and MUIPC were multi-item scales partly drawn from previous validated measures. The constructs SUSE, SURV, and INTR (MUIPC) were measured by items adapted from Xu et al. (2012a), while PERS_ID, LOC, DEV_CON, and SYS_NET were measured by items based on a detailed analysis of access rights and privacy settings (iOS 6, Android version 4.2.2) and an extensive literature review. This is due to the fact that we could find no rigorously validated instrument that captured the constructs of access to personal information during our research. Since the construct of access to personal information was developed based on prior literature and theory, it was important to establish a proper factor structure of the construct. Due to the large number of indicators, we therefore first conducted an explorative factor analysis (EFA) as a dimensional reduction method using the principal component analysis (PCA) with varimax rotation as the extraction method. The total number of items was reduced based on four constructs: PERS_ID, LOC, DEV_CON, and SYS_NET, with a total of 25 indicators (see Appendix Table A2). These constructs that represent the overall dimension of access to personal information, were expected to influence MUIPC. The component structure of MUIPC was also examined by means of a factor analysis. In the first implementation of the EFA, there were cross-loadings between two components for the item SURV1, so this was removed. After excluding SURV1, the results of the EFA show a very clean component structure in which discriminant and convergent validity are evident by the high loadings within components, and no cross-loadings between components that exceed 0.40; see Table 2. Cronbach's Alpha was more than 0.7 for all seven constructs. All constructs ranged from minimum 0.807 to 0.948, demonstrating that all constructs satisfied the criteria for adequate convergent validity (Nunnally 1978).

Table 2. Results PCA using Varimax Rotation for MUIPC

Construct	Items	Component			Cronbach's Alpha
		1	2	3	
SUSE	SUSE 1	**.824**	.296	.268	.916
	SUSE 2	**.853**	.236	.260	
	SUSE 3	**.865**	.247	.262	
SURV	SURV 2	.352	.392	**.740**	.816
	SURV 3	.332	.325	**.807**	
INTR	INTR 1	.227	**.794**	.281	.855
	INTR 2	.212	**.861**	.237	
	INTR 3	.349	**.734**	.278	
Rotation Sum of Squared Loadings	Total	2.608	2.373	1.619	
	% Variance	32.602	29.664	20.237	
	Cumulative Variance	32.602	62.266	82.503	

Furthermore, the potential for common method variance (CMV) should be addressed because the data was collected from a survey instrument (Chang et al. 2010; McElroy et al. 2007; Podsakoff and Organ 1986) and in many empirical studies, CMV remains a critical methodological concern (Siemsen et al. 2010). We tried to minimize these methodological concerns ex-ante in the research design stage and ex-post in different ways: first, a number of procedural remedies were used in designing and administering the questionnaire to reduce the likelihood of CMV. The measures for the different constructs (independent and dependent variables) were collected from different sources (Chang et al. 2010). Furthermore, counterbalancing the order of questions in relation to different constructs makes CMV less likely. This is due to the fact that the participant cannot easily combine related indicators to cognitively create the correlation needed to produce a CMV-biased pattern of responses (Murray et al. 2005). Therefore, we implemented the online survey questionnaire in such way as to prevent participants from backtracking to change their answers. To achieve this, the pages of the survey items were presented in a random manner to discourage participants from figuring out the relationship between the predictor and criterion variable that we were trying to establish. Second, anonymity and confidentiality of the study were guaranteed (Chang et al. 2010). This also mitigated self-serving answers and the probability that respondents provided answers they believe were expected. These remedies can ex-ante reduce the likelihood of the consistency motive in participants' responses and theory-in-use biases (Chang et al. 2010; Podsakoff et al. 2003). Third, this study employed Harman's single-factor test (Podsakoff et al. 2003) to access the common method bias ex-post. The results of the EFA show that no single factor accounted for the covariance in the variables and no single factor emerged from the unrotated factor solution (Podsakoff et al. 2003).

Data Analysis and Results

In this section, following the description of the analysis, which includes, e.g., a description of instrument validity and an internal validity test, the results are described and further presented in a model (see Figure 2). Constructs that are the basic elements of a theory are not inherently reflective or formative and the choice of measurement rest on theoretical considerations (Centefelli and Bassellier 2009, Howell et al. 2007). The measurement formulation depends on the direction of the relationship between the constructs and the corresponding manifest variables (Fornell and Bookstein 1982). We therefore captured the entire domain of the constructs and decided at the theoretical level whether the constructs in the underlying research field were reflective, formative, or a combination (MIMIC model) of the two previously mentioned models to ensure content validity. After examining the relationship between each indicator and the construct in the field of access to personal information and MUIPC, we determined the overall constructs in the research model to be reflective. In reflective measurement models, each variable is a function of the underlying factor and each manifest variable is assumed to measure a unique underlying concept (Esposito Vinzi et al. 2010).

Empirical data was analyzed via structural equation modeling (SEM) to test the causal-effect relations among the latent constructs. SEM integrates the measurement and the structural model (hypothesized causal paths) into a simultaneous assessment (Gefen et al. 2011). Therefore, SEM provides researchers with the flexibility to model a relationship among criterion variables and multiple predictors, such as model errors in measurements for observed variables, to design unobservable latent variables, and statistically test a priori theoretical and measurement assumptions against empirical data (Chin 1998). Model testing and measurement validation were conducted using SmartPLS (partial least squares) version 2.0.M3, a variance analytical SEM technique that utilizes a component-based approach to estimation. It is advantageous when the research model has a variety of indicators, is relatively complex, and the measures are not well-established (Fornell and Bookstein 1982).

Before the overall model was analyzed, the reflective measurement models for access to personal information and MUIPC were analyzed. In this context, we examined item reliability, construct validity, composite reliability, and convergent and discriminant validity. To ensure item reliability, the loadings of each item were examined to their respective underlying construct. Acceptable item loadings are recommended to be above at least 0.6 and ideally above the threshold of 0.707, indicating that at least 50 percent of the variance is shared with the respective construct (Chin 1998). The item reliability analysis of access to personal information and MUIPC shows that all items ranged from minimum 0.703 to 0.939, demonstrating that all items are reliable for further analysis. The t-values ranged from 20.170 to 123.954, which indicates significance for all item loadings at p < 0.001. In addition to the item reliability, the construct validity was checked by reviewing whether there were cross-loadings. In this study, no cross-loadings were identified, which means that all indicators load on those constructs to which they were intended to load (Straub et al. 2004). The composite reliability or internal consistency reliability (ICR) is similar to Cronbach's alpha and is used to measure the internal consistency, except that the latter presumes, a priori, that each indicator of a construct contributes equally (i.e., the loadings are set to unity) (Chin 1998; Fornell and Larcker 1981). The measure is superior to Cronbach's alpha because it uses the actual indicator loadings obtained within the nomological network to calculate internal consistency reliability (Fornell and Larcker 1981). ICR, which is unaffected by scale length, is more general than Cronbach's alpha, but the interpretation of the values obtained is similar and the guidelines offered by Nunnally can be adopted (Howell and Avolio 1993). The value for ICR should be 0.70 or higher (Diamantopoulos et al. 2008). The composite reliability (ICR) is above the threshold and the values range from 0.8924 to 0.9548, so that the internal consistency reliability for all constructs is given. Discriminant and convergent validity was assessed by the average variance extracted (AVE). First, "discriminant validity can be established if item-to-construct correlations are higher with each other than with other construct measures and their composite values" (Johnston and Warkentin 2010, p. 557, Loch et al. 2003). Here, the condition for discriminant validity is met. Furthermore, the AVE estimate is the overall amount of variation that a latent construct is able to explain in the manifest or observed variables to which is theoretically related. The reported values provide evidence of discriminant and convergent validity, since the AVE is well above the recommended level of 0.50 (Bhattacherjee and Premkumar 2004). The AVE values for all constructs in this model are higher than the recommended threshold value of 0.50 (smallest AVE: 0.6052), suggesting the convergent validity of the scale (Bhattacherjee and Premkumar 2004). Overall, the evidence of reliability, convergent validity, and discriminant validity indicates that the measurement model was appropriate for testing the structural model at a subsequent stage.

Table 3. Validity and Reliability Criteria

Constructs	Indicators	Std. Loading	t-value	Average Variance Extracted (AVE) AVE(ξi) ≥ 0.5	Composite Reliability (ICR) (ρ ≥ 0.7)
INTR	INTR 1 - 3	0.865 - 0.901	60.160 - 90.729	0.7752	0.9118
SURV	SURV 2 - 3	0.917 - 0.921	99.065 - 103.944	0.8448	0.9159
SUSE	SUSE 1 - 3	0.919 - 0.936	85.700 - 123.954	0.8559	0.9469
DEV_CON	DEV_CON 1 - 9	0.734 - 0.826	21.723 - 38.011	0.6052	0.9324
PERS_ID	PERS_ID 1 - 3	0.801 - 0.905	35.369 - 71.544	0.7348	0.8924
LOC	LOC 1 - 2	0.936 - 0.939	91.628 - 105.992	0.8792	0.9357
SYS_NET	SYS_NET 1 - 11	0.703 - 0.862	20.170 - 58.763	0.6585	0.9548

INTR = Perceived Intrusion; SURV = Perceived Surveillance; SUSE = Secondary Use of Personal Information; DEV_CON = Device Content; PERS_ID = Personal Identity; LOC = Location; SYS_NET = System and Network Settings

To receive valid results, the bootstrapping resampling procedure was used with 1000 resamples to obtain estimates of standard errors for testing the statistical significance of a path coefficient using the t-test. In this way, the analysis produced estimates of both the explained variance and path coefficients. Of the four hypotheses, all but one involving the influence of SYS_NET were found to be significant, as shown in the overall findings in Table 4.

Table 4. Overview of Findings

Hypothesis (with direction)	Path Coefficient (ß)	t-value	p-value	Support
H[1]: PERS_ID --> MUIPC (+)	0.249	5.592	$p < 0.001$	Supported
H[2]: LOC --> MUIPC (+)	0.206	4.021	$p < 0.001$	Supported
H[3]: DEV_CON --> MUIPC (+)	0.225	4.129	$p < 0.001$	Supported
H[4]: SYS_NET --> MUIPC (+)	-0.006	0.167	$p > 0.10$	Not supported

As indicated in Figure 2, the model explains approximately 27 percent of the overall variance. This explanatory power of 27 percent are the paths from the constructs of access to personal information leading to MUIPC. Consistent with H[1], PERS_ID has a significant positive effect on MUIPC ($\beta = .249$, $p < .001$). Similarly, H[2] and H[3] are supported as both LOC ($\beta = .206$, $p < .001$) and DEV_CON ($\beta = .225$, $p < .001$) have significant positive effects on MUIPC.

Kirk (1996) argues that "statistical significance is concerned with whether a research result is due to chance of sampling variability; practical significance is concerned with whether a research result is useful in the real world." (p. 746). Therefore, it is essential that we interpret the significance of the results not only statistically, but according to their real world or practical significance as well. For practical purposes it is the differential effects of the latent variables that are important and not primarily the statistical significance (Boßow-Thies and Albers 2010). In order to examine the practical significance, the effect size referring to Cohen (1988) is calculated. Effect size measures have been offered as indices of meaningfulness or practical significance (Olejnik and Algina 2000; Onwuegbuzie and Leech 2004). Effect sizes have the advantages that they are independent of the sample size and that the measures of the effect sizes allow a direct comparison of different quantities measured, e.g., on different scales (Selya et al. 2012). As Kirk pointed out in 1996, "Cohen's definitions of small, medium, and large effects represent a good beginning." (p. 756), with respect to determining the practical significance. Cohen's f^2 is one of several effect size measures to use in the context of multiple regression analysis (Chin et al. 2003; Cohen 1988). Next to the value of the path coefficients, the effect size f^2 is another measure of substantial effect of exogenous latent variables on the latent endogenous variable. f^2 then provides information about the size of the effects, although it has to be noted that a small f^2 does not necessarily imply an unimportant effect (Chin et al. 2003). It can thus also be used to illustrate the practical relevance of statistical significant results. The effect sizes are shown in Table 5.

Table 5. Effect Size

Latent variable being explained (endogenous)	Explanatory latent variable (exogenous)	$R^2_{incl.}$ [a]	$R^2_{excl.}$ [b]	f^2
MUIPC	PERS_ID	0.270	0.221	0.067
	LOC	0.270	0.240	0.041
	DEV_CON	0.270	0.241	0.040
	SYS_NET	0.270	0.270	0

[a] → R^2 of the latent variable being explained (endogenous), together with the explanatory latent variable (exogenous).
[b] → R^2 of the latent variable being explained (endogenous), in the absence of the explanatory latent variable (exogenous).
Note: Cohen's f^2-statistics = $[R^2_{incl.} - R^2_{excl.}] / [1- R^2_{incl.}]$ (1988). $f^2 \geq 0.02$, 0.15, and 0.35 are termed small, medium, and large effect sizes. The rationale for these benchmarks (f^2) can be found in Cohen (1988) on the following pages: pp. 413-414.

Discussion and Recommendations

This paper demonstrates that access to personal information is influential in determining mobile users' information privacy concerns (MUIPC). Figure 2 shows the estimates of the path coefficients and a summary of the test results of research hypotheses.

Access to personal identity is hypothesized to show a positive relation to MUIPC. Our results indicate a positive significant relationship. Usually it is almost impossible for mobile users to avoid exposing information related to their identity. For example, platforms like Apple App Store, Google Play Store, and Windows Phone Store, where mobile apps usually are available, require users to register with at least a valid email address and further identity-related information like name, date of birth, gender, phone number, etc. Even if users try to avoid stating identity-related information or give fake information, their phone's unique device ID cannot be changed or turned off (Thurm and Kane 2010), and it links any other information accessed by mobile apps to a user's mobile device. Referring to the MUIPC dimension of intrusion, users may feel uncomfortable providing identity-related information to mobile apps.

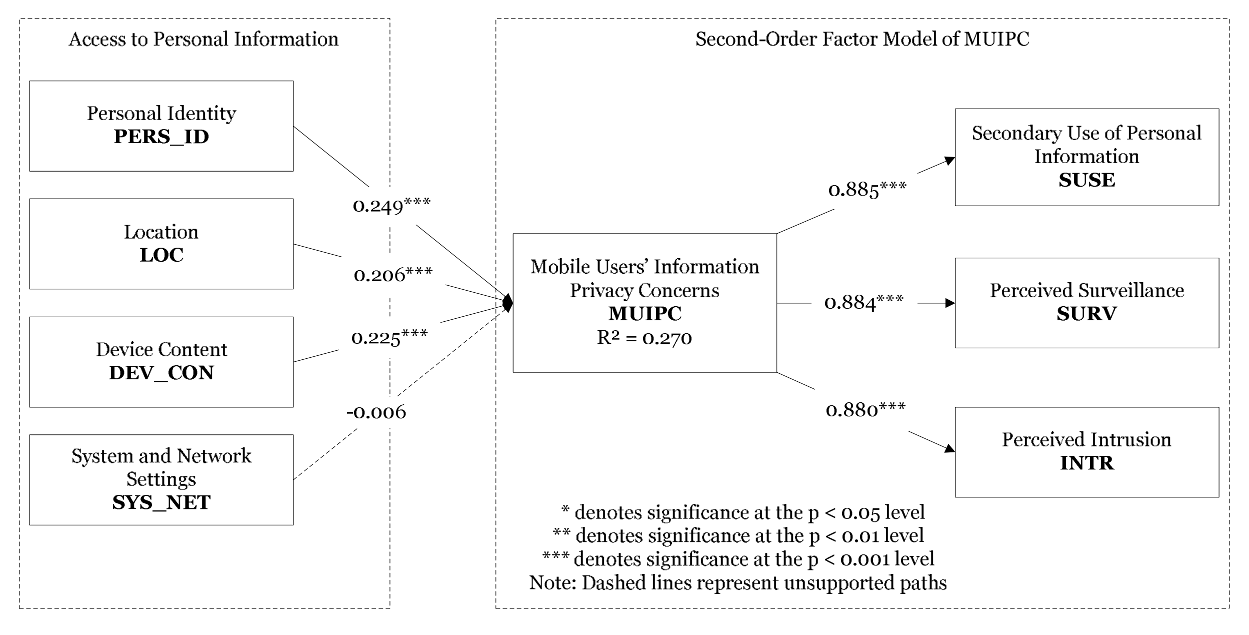
Access to Personal Information
Second-Order Factor Model of MUIPC
Personal Identity
PERS_ID
Location
LOC
Device Content
DEV_CON
System and Network Settings
SYS_NET
0.249***
0.206***
0.225***
-0.006
Mobile Users' Information Privacy Concerns
MUIPC
R² = 0.270
0.885***
0.884***
0.880***
Secondary Use of Personal Information
SUSE
Perceived Surveillance
SURV
Perceived Intrusion
INTR
* denotes significance at the p < 0.05 level
** denotes significance at the p < 0.01 level
*** denotes significance at the p < 0.001 level
Note: Dashed lines represent unsupported paths

Figure 2. Results

As hypothesized, the results indicate that access to location has a positive impact on MUIPC. Prior research stated that the disclosure of location is of great concern for mobile users. In particular, the surveillance dimension of MUIPC indicates that the tracking of mobile users' location can be of concern. Due to the permission given to mobile apps, users' activities are tracked wherever and whenever users are located. In the last few years, LBS has become a common feature of mobile apps. For example, Google Maps applies GPS and network location sources to provide users with street maps, satellite images, navigation assistance, a route planner for travelling by foot, car, bike, or with public transportation. Many other mobile apps offer LBS, such as check-in options on Facebook or Foursquare. Referring to the MUIPC dimension secondary use of personal information, location-related information could be used for purposes other than those expected and authorized by the user, e.g., location-based advertising, which could make the user feel uncomfortable. For example, since the launch of Google Street View, privacy concerns have been raised with the result that Google implemented an option to request removal of images (Mills 2007), later replacing it by an option to request blurring of images. As proposed by many researchers before, location is an essential factor in the context of mobile security and privacy. The results of our research model suggest that access to mobile users' location affects mobile users' privacy concerns.

With regard to access to device content, the path coefficient is significantly positive in relation to MUIPC. The use of photos and videos has become very common on mobile devices. Access to such private data can be perceived as intrusive to users. In addition, photos and videos can include further information like when and where the photo or the video was taken, which can increase mobile users' level of concern. Further content like contacts stored on mobile devices, including the frequency with which the user called, emailed, etc. can be accessed by mobile apps, revealing information that might trace to relatives, friends, colleagues, acquaintances, etc. Calendars and reminders are another source of information, revealing users' time schedules. For example, they contain information about when and where a user will perform which task. When mobile apps are given access to browser bookmarks and navigation history, detailed user web browsing behavior and web browsing preferences can be obtained. This information is especially useful for context-aware advertising. However, mobile users may perceive access to content as an intrusion into their privacy, and this was confirmed by our model testing.

Eventually, the influence of access to system and network settings on MUIPC was not found to be influential (t-value 0.167). At first glance, it appears that settings do not relate to personal information. However, access to settings can give information on user behavior. For example, Shirazi et al. (2013) developed a mobile app to track users sleep behavior by implementing a social alarm clock. It allowed mobile apps to access the alarm of mobile devices, giving information on users' routines, which could make them feel uncomfortable due to perceived privacy intrusion. Synchronization settings and statistics show the history of synchronization events and how much data is synchronized, which is another pattern of user behavior. Allowing mobile apps to retrieve running apps reveals information about which apps are used on the mobile device. Regarding network settings, the using of Wi-Fi, NFC, and Bluetooth gives information on where, when, and in which context network connections have been used. Thus, considering access to both system and network settings, it was hypothesized to have an effect on MUIPC. However, a significant relationship cannot be identified.

Implications for Research and Practice

The results have theoretical and practical implications. First, our primary contribution is to investigate the relationship between access to personal information and MUIPC. In this study, we examine the influence of the four dimensions of access to personal information on MUIPC, of which three are found to be significant. Due to the highly significant path coefficients of the influence of access to personal identity, location, and device content on MUIPC, we call for a deeper examination of these three dimensions. Second, the results of our study show an R^2 of 0.270 for MUIPC. Thus, 27% of the variance of MUIPC is explained by access to personal information. To respond to the call for research investigating antecedents and consequences of information privacy concerns (Smith et al. 1996; Stewart and Segars 2002), in the mobile context, we recommend considering the construct of access to personal information along with further constructs such as prior privacy experience (Smith et al. 1996; Xu et al. 2012a), anxiety (Stewart and Segars 2002), and control over personal information (Malhotra et al. 2004; Xu et al. 2012b). Thus, a comprehension of mobile users' privacy concerns could be further enhanced. Third, we recommend further research to consider potential distinctions between free and paid apps, which can have an influence on users' privacy concerns.

From a practical perspective, the results indicate that app providers should recognize access to personal information as a significant indicator affecting MUIPC. Hence, asking mobile users for permission to access personal information can lead to privacy concerns. These concerns can prevent users from installing mobile apps or make them feel uncomfortable, with the result being that they uninstall the mobile app (Pew Internet 2012). If app providers understand mobile users' privacy concerns, they can react to them. Access to personal information is one aspect that should be recognized. App providers should ensure that they access personal information stored on mobile devices only if necessary and justified with value-added services. For example, location should only be tracked if the mobile app requires this function to work properly, such as with the navigation system of the Google Maps mobile app. In this context, trust is a key aspect to enhance users' belief to which degree "a firm is dependable in protecting consumers' personal information" (Malhotra et al. 2004, p. 341). Several studies in the field of electronic commerce have found trust to have a significant impact on information sharing and purchase decisions (e.g., Dinev and Hart 2006; Gefen et al. 2003; McKnight et al. 2002). Within the frame of mobile apps, trust can lead users to allow access to personal information and conduct transactions such as pay-per-download, in-app purchase, or subscriptions. A trust-based relationship between app providers and users can help to build user confidence and overcome privacy concerns. Thus, app users can expect safe environments in which app providers act in a regular, honest, and cooperative way. With regard to creating a trust-based relationship, several studies have identified various methods, of which different privacy assurance approaches have been in the focus of mobile application research for the last three years (e.g., Keith et al. 2010; Xu et al. 2010).

Xu et al. (2012b) distinguish between three privacy assurance approaches, i.e., individual self-protection, industry self-regulation, and government regulation, all of which have a direct negative influence on privacy concerns. That implies that privacy assurances offered by app providers can alleviate mobile users' privacy concerns. The individual self-protection approach allows users to control the access to personal information (Xu et al. 2012b), for example by turning off the location tracking from their mobile devices. In contrast to Google Android, Apple iOS users can turn off access in the privacy settings if supported by the mobile app. Taking this into account, we recommend that app providers offer users the opportunity to turn off access to their personal information. App providers should advise users that certain functions of a mobile app may not work when doing so, e.g., the navigation system of the Google Maps mobile app will not work if location tracking is turned off. Further individual self-protection approaches comprise the users' refusal to provide personal information, misrepresentation of personal information, removal of personal information, negative word-of-mouth communication to others, complaining directly to online companies, and complaining indirectly to third-party privacy organizations (Son and Kim 2008). For example, app users could refuse to provide personal information by abbreviating the names of their contacts if the mobile app has access to the contacts stored on the users' mobile devices. This could prevent app providers from linking users' contacts to information stored on the providers' databases. The industry self-regulation approach "places the responsibility for protecting information privacy in the hands of those that gather, use, and sell personal information" (Xu et al. 2010, p. 143). App providers can use privacy seals, guarantees, and promises such as privacy policies, which positively influence trusting beliefs (Keith et al. 2010). For example, TRUSTe offers a privacy seal program specifically for mobile app developers (TRUSTe 2013). We recommend that app providers take privacy seals into account and communicate privacy policies to their users, with the result that users can understand why their personal identity, location, and device content is accessed by the mobile app. The government regulation approach "relies on the judicial and legislative branches of a government agency for protecting personal information" (Xu et al. 2010, p. 143). This approach entails that users are protected from misuse and breach of privacy laws, which can lead offenders to be punished by law, establishing and maintaining a deterrent effect (Xu et al. 2012b). For example, the California Department of Justice introduced a privacy law as of October 30, 2012, and requested app developers to "post a privacy policy within their app that informs users of what personally identifiable information about them is being collected and what will be done with that private information" (California Department of Justice 2012). The implementation of privacy policies is even more important considering both industry self-regulation and government regulation. Due to the alleviating effect of privacy assurance approaches on privacy concerns, we recommend that app providers consider these approaches, i.e., individual self-protection, industry self-regulation, and government regulation, in particular when accessing users' personal identity, location, and device content. Regarding the importance for practical implications, interdependencies between privacy assurances and the access to personal information are promising for further research.

Limitations and Conclusion

Like other empirical research, the results should be read within its inherent limitations. Note that all of the measures are prone to measurement errors that could affect the results of the analysis, because all of the measures are subjective by nature. Therefore, the study is subject to following limitations, which present useful opportunities for further research. First, one limitation of this research is found in the fact that most of the participants were up to 30 years old, with the majority being younger than 20 years old (see Appendix Table A1). Although our participants may fall in the target users for mobile apps, care must be taken in any effort to generalize the findings beyond the boundaries of our sample. Some possible research approach for the future are possible: Future researchers should repeat this study with a more diverse sample for enhanced generalizability and further analyses are required to exclude possible confounded impacts of those demographic characteristics on the constructs of this research.

Second, in terms of generalizability, another bias possibility is self-selection among the survey respondents due to several reasons. One reason is that data were collected through an online survey, which is liable to a self-selection bias (Kim et al. 2002). In addition, we offered a monetary reward in the form of two $25 Amazon vouchers. This could have drawn participants who were more prone to monetary incentives, leading to a sampling bias (Hui et al. 2007). Another reason for self-selection bias is that we stated in the postings and emails that the topic of the survey is about mobile app privacy. Mobile app users who are more concerned about information privacy might also be those who are more likely to respond to the survey (Kankanhalli et al. 2005).

Third, it cannot be precluded that unacknowledged factors of the overall construct of access to personal information are not considered. Culturally driven individual differences are not part of this research model. A further limitation is that we conducted the study exclusively in the USA, which has a strong reputation in this research context. Thus, the participants may have powerful and well-formed beliefs about the access to personal information and privacy concerns. As Smith (2004) pointed out, different countries have approached privacy issues differently in various regulatory structures. Furthermore, Chen (2008) pointed out that culture has lasting impacts on privacy. Therefore, future research should be conducted in other countries to provide further insights into the effects of access to personal information and privacy concerns.

Future studies could expand to include an international context by integrating cultural differences into the evaluation of access to personal information and the impact on mobile users' information privacy concerns, taking individual differences into account. Furthermore, qualitative investigations that explore and capture the subtleties that cannot be directly measured by quantitative research can be examined in further studies.

In this paper, we presented an initial attempt to investigate the relationship between access to personal information and mobile users' information privacy concerns. Access to personal information was categorized into four dimensions: personal identity, location, device content, and system and network settings, which were identified by conducting a survey and testing collected data with principal component analysis using varimax rotation. Results of a structural equation modeling indicate that access to personal identity, location, and device content is significantly positive in relation to mobile users' information privacy concerns.

Appendix

Survey Instrument

Perceived Surveillance: Five-point scales from "strongly agree" to "strongly disagree" (Xu et al. 2012a)

(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: Five-point scales from "strongly agree" to "strongly disagree" (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: Five-point scales from "strongly agree" to "strongly disagree" (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.

Access to Personal Information: Five-point scales from “extremely high” to “extremely low” (self-developed)

How high do you feel the intrusion into your privacy if mobile apps are able to access the following on your mobile device? (see Appendix Table A2 - Description Questionnaire for further information on indicators)

Table A1. Demographics

Gender		
Female	288	60.8%
Male	166	35.0%
Missing	20	4.2%
Age		
≤ 20	274	57.8%
21 - 30	94	19.8%
31 - 40	22	4.6%
41 - 50	19	4.0%
> 50	45	9.5%
Missing	20	4.2%
Profession		
Employed	82	17.3%
Homemaker	2	0.4%
Self-employed	14	3.0%
Student	338	71.3%
Other	19	4.0%
Missing	19	4.0%
Education		
Less than high school	28	5.9%
High school degree	273	57.6%
College degree	29	6.1%
Undergraduate degree	57	12.0%
Graduate degree	59	12.4%
Other	8	1.7%
Missing	20	4.2%
Income		
≤ $ 20,000	73	15.4%
$ 20,001 - $ 40,000	39	8.2%
$ 40,001 - $ 60,000	33	7.0%
$ 60,001 - $ 100,000	50	10.5%
> $ 100,000	105	22.2%
Not specified	152	32.1%
Missing	22	4.6%

Table A2. Results PCA using Varimax Rotation for Access to Personal Information

Construct	Items	Description Questionnaire	Component				Cronbach's Alpha
			1	2	3	4	
SYS_NET	SYS_NET 1	Access_Sync_Settings	**.828**				.948
	SYS_NET 2	Access_Sync_Statistics	**.812**				
	SYS_NET 3	Access_Vibrator	**.812**				
	SYS_NET 4	Access_Alarm	**.783**				
	SYS_NET 5	Access_Network_Connection	**.780**				
	SYS_NET 6	Access_System_Settings	**.779**				
	SYS_NET 7	Access_Bluetooth	**.772**				
	SYS_NET 8	Access_Wi-Fi	**757**				
	SYS_NET 9	Access_Info_Running_Apps	**.730**				
	SYS_NET 10	Access_Screen_Lock	**.642**				
	SYS_NET 11	Access_NFC	**.622**				
DEV_CON	DEV_CON 1	Access_Videos		**.836**			.918
	DEV_CON 2	Access_Photos		**.828**			
	DEV_CON 3	Access_Call_Logs		**.742**			
	DEV_CON 4	Access_Calendar_Events		**.710**			
	DEV_CON 5	Access_Reminders		**.700**			
	DEV_CON 6	Access_Contacts		**.697**			
	DEV_CON 7	Access_USB_Storage		**.691**			
	DEV_CON 8	Access_Browser_Navi_History		**.606**			
	DEV_CON 9	Access_Browser_Bookmarks		**.582**			
PERS_ID	PERS_ID 1	Access_Contact_Information			**.864**		.807
	PERS_ID 2	Access_Phone_Number			**.836**		
	PERS_ID 3	Access_Name			**.746**		
LOC	LOC 1	Access_Approximate_Location				**.851**	.860
	LOC 2	Access_Precise_Location				**.779**	
Rotation Sum of Squared Loadings	Total		7.189	5.616	2.361	1.983	
	% Variance		28.756	22.462	9.443	7.933	
	Cumulative Variance		28.756	51.218	60.661	68.594	

* Factor loadings less than 0.4 suppressed.

References

ABI Research. 2012. "In-App Purchases to Outpace Pay-Per-Download Revenues in 2012," from http://www.abiresearch.com/press/in-app-purchases-to-outpace-pay-per-download-reven

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.

Anthes, G. 2011. "Invasion of the Mobile Apps," *Communications of the ACM* (54:9), pp. 16-18.

Apple. 2013. "iOS SDK Release Notes for iOS 6," from http://developer.apple.com/library/ios/#releasenotes/General/RN-iOSSDK-6_0

Barbeau, S. J., Perez, R. A., Labrador, M. A., Perez, A. J., Winters, P. L., and Georggi, N. L. 2011. "A Location-Aware Framework for Intelligent Real-Time Mobile Applications," *Pervasive Computing* (10:3), pp. 58-67.

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 Weeks, D. G. 1980. "Linear Structural Equations with Latent Variables," *Psychometrika* (45:3), pp. 289-308.

Bergvall-Kåreborn, B., Howcroft, D., and Chincholle, D. 2010. "Outsourcing Creative Work: a Study of Mobile Application Development," in *Proceedings of the 31st International Conference on Information Systems*, St. Louis, MO, USA.

Bhattacherjee, A., and Premkumar, G 2004. "Understanding Changes in Belief and Attitude Toward Information Technology Usage: A Theoretical Model and Longitudinal Test," *MIS Quarterly* (28:2), pp. 229-254.

Boßow-Thies, S., and Albers, S. 2010. "Application of PLS in Marketing: Content Strategies on the Internet," in *Handbook of Partial Least Squares: Concepts, Methods and Applications*, V. Esposito Vinzi, W. W. Chin, J. Henseler, and H. Wang (eds.), Springer Handbooks of Computational Statistics, Berlin: Springer, pp. 589-604.

California Department of Justice. 2012. "Attorney General Kamala D. Harris Notifies Mobile App Developers of Non-Compliance with California Privacy Law," from http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-notifies-mobile-app-developers-non-compliance

Cenfetelli, R. T., and Bassellier, G. 2009. "Interpretation of Formative Measurement in Information Systems Research," *MIS Quarterly* (33:4), pp. 689-708.

Chang, S.-J., van Witteloostuijn, A., and Eden, L. 2010. "From the Editors: Common method variance in international business research," *Journal of International Business Studies* (41:2), pp. 178-184.

Chen, L., Meservy, T. O., and Gillenson, M. 2012. "Understanding Information Systems Continuance for Information-Oriented Mobile Applications," *Communications of the AIS* (30:9), pp. 127-146.

Chin, W. W. 1998. "Issues and Opinion on Structural Equation Modeling," *MIS Quarterly* (29:3), pp. vii-xvi.

Chin, W. W., Marcolin, B. L., and Newsted, P. R. 2003. "A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results from a Monte Carlo Simulation Study and an Electronic-Mail Emotion/Adoption Study," *Information Systems Research* (14:2), pp. 189-217.

Cohen, J. 1988. *Statistical Power Analysis for Behavioral Sciences,* 2nd ed., Hillsdale, NJ: Lawrence Erlbaum.

Culnan, M. J., and Armstrong, P. K. 1999. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), pp. 104-115.

Dhar, S., and Varshney, U. 2011. "Challenges and Business Models for Mobile Location-based Services and Advertising," *Communications of the ACM* (54:5), pp. 121-129.

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

Edwards, J. R. 2001. "Multidimensional Constructs in Organizational Behavior Research: An Integrative Analytical Framework," *Organizational Research Methods* (4:2), pp. 144-192.

Enck, W. 2011. "Defending Users against Smartphone Apps: Techniques and Future Directions," in *Proceedings of the Lecture Notes in Computer Science* (7093), S. Jajodia and C. Mazumdar (eds.): Information Systems Security, Berlin: Springer, pp. 49-70.

Esposito Vinzi, V., Trinchera, L., and Amato, S. 2010. "PLS Path Modeling: From Foundations to Recent Developments and Open Issues for Model Assessment and Improvement," in *Handbook of Partial Least Squares: Concepts, Methods and Applications*, V. Esposito Vinzi, W. W. Chin, J. Henseler, and H. Wang (eds.), Springer Handbooks of Computational Statistics, Berlin: Springer, pp. 47-82.

Fornell, C., and Larcker, D. F. 1981. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research* (18:1), pp. 39-50.

Fornell, C., and Bookstein, F. L. 1982. "Two Structural Equation Models: LISREL and PLS Applied to Consumer Exit-Voice Theory," *Journal of Marketing Research* (19:4), pp. 440–452.

Gavalas, D., and Economou, D. 2011. "Development Platforms for Mobile Applications: Status and Trends," *IEEE Software* (28:1), pp. 77-86.

Gefen, D., Karahanna, E., and Straub, D. W. 2003. "Trust and TAM in Online Shopping: An Integrated Model," *MIS Quarterly* (27:1), pp. 51-90.

Gefen, D., Rigdon, E. E., and Straub, D. 2011. "An Update and Extension to SEM Guidlines for Administrative and Social Science Research," *MIS Quarterly* (35:2), pp. iii-xiv.

Gerbing, D. W., and Anderson, J. C. 1984. "On the Meaning of Within-Factor Correlated Measurement Errors," *Journal of Consumer Research* (11:1), pp. 572-580.

Gerbing, D. W., Hamilton, J. G., and Freeman, E. B. 1994. "A Large-scale Second-order Structural

Equation Model of the Influence of Management Participation on Organizational Planning Benefits," *Journal of Management* (20:4), pp. 859-885.

Ghose, A., and Han, S. P. 2012. "Estimating Demand for Mobile Applications in the New Mobile Economy," in *Proceedings of the 33rd International Conference on Information Systems*, Orlando, FL, USA.

Golding, P., and Donaldson, O. 2009. "A Design Science Approach for Creating Mobile Applications," in *Proceedings of the 33rd International Conference on Information Systems*, Orlando, FL, USA.

Hao, L., Li, X., Tan, Y., and Xu, J. 2011. "The Economic Role of Rating Behavior in Third-Party Application Market," in *Proceedings of the 32nd International Conference on Information Systems*, Shanghai, China.

Howell, J. M., and Avolio, B. J. 1993. "Transformational Leadership, Transactional Leadership, Locus for Control, and Support for Information: Key Predictors of Consolidated-Business-Unit Performance," *Journal of Applied Psychology* (78:6), pp. 891-902.

Howell, R. D., Breivik, E., and Wilcox, J. B. 2007. "Reconsidering Formative Measurement," *Psychological Methods* (12:2), pp. 205-218.

Hu, H.-f., Moore, W. L., and Hu, P. J. 2012. "Incorporating User Perceptions and Product Attributes in Software Product Design and Evaluation," in *Proceedings of the 33rd International Conference on Information Systems*, Orlando, FL, USA.

Hui, K.-L., Teo, H. H., and Lee, S.-Y. 2007. "The Value of Privacy Assurance: An Exploratory Field Experiment," *MIS Quarterly* (31:1), pp. 19-33.

Jabeur, N., Zeadally, S., and Sayed, B. 2013. "Mobile Social Networking Applications," *Communications of the ACM* (56:3), pp. 71-79.

Jarvis, C. B., MacKenzie, S. B., and Podsakoff, P. M. 2003. "A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research," *Journal of Consumer Research* (30:2), pp. 199-218.

Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:3), pp. 549-566.

Kajanan, S., Pervin, N., Ramasubbu, N., and Dutta, K. 2012. "Takeoff and Sustained Success of Apps in Hypercompetitive Mobile Platform Ecosystems: An Empirical Analysis," in *Proceedings of the 33rd International Conference on Information Systems*, Orlando, FL, USA.

Kankanhalli, A., Tan, B. C. Y., and Wei, K.-K. 2005. "Contributing Knowledge to Electronic Knowledge Repositories: An Empirical Investigation," *MIS Quarterly* (29:1), pp. 113-143.

Keith, M. J., Babb Jr., J. S., Furner, C. P., and Abdullat, A. 2010. "Privacy Assurance and Network Effects in the Adoption of Location-Based Services: An iPhone Experiment," in *Proceedings of the 31st International Conference on Information Systems*, St. Louis, MO, USA.

Keith, M. J., Thompson, S. C., Hale, J. E., and Greer, C. 2012. "Examining the Rationality of Information Disclosure through Mobile Devices," in *Proceedings of the 33rd International Conference on Information Systems*, Orlando, FL, USA.

Kim, J., Lee, J., Han, K., and Lee, M. 2002. "Businesses as Buildings: Metrics for the Architectural Quality of Internet Businesses," *Information Systems Research* (13:3), pp. 239-254.

Kim, J. 2012. "The Effect of Design Characteristics of Mobile Applications on User Retention: An Environmental Psychology Perspective," in *Proceedings of the 18th Americas Conference on Information Systems*, Seattle, WA, USA.

Kirk, R. E. 1996. "Practical Significance: A Concept Whose Time Has Come," *Educational and Psychological Measurement* (56:5), pp. 746-759.

Koufteros, X., Babbar, S., and Kaighobadi, M. 2009. "A paradigm for examining second-order factor models employing structural equation modeling," *International Journal of Production Economics* (120:2), pp. 633-652.

Laufer, R. S., and Wolfe, M. 1977. "Privacy as a Concept and a Social Issue: Multidimensional Development Theory," *Journal of Social Issues* (33:3), pp. 22-42.

Leavitt, N. 2011. "Mobile Security: Finally a Serious Problem?," *Computer* (44:6), pp. 11-14.

Lee, G., and Raghu, T. S. 2011. "Product Portfolio and Mobile Apps Success: Evidence from App Store Market," in *Proceedings of the 17th Americas Conference on Information Systems*, Detroit, MI, USA.

Lehrer, C., Constantiou, I., and Hess, T. 2011. "A Cognitive Process Analysis of Individuals' Use of Location-Based Services," in *Proceedings of the 19th European Conference on Information Systems*, Helsinki, Finland.

Liu, C. Z., Au, Y. A., and Choi, H. S. 2012. "An Empirical Study of the Freemium Strategy for Mobile Apps:

Evidence from the Google Play Market," in *Proceedings of the 33rd International Conference on Information Systems*, Orlando, FL, USA.

Loch, K. D., Straub, D. W., and Kamel, S. 2003. "Diffusing the Internet in the Arab World: The Role of Social Norms and Technological Culturation," *IEEE Transactions Engineering Management* (50:1), pp. 45-63.

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), pp. 336-355.

McElroy, J. C., Hendrickson, A. R., Townsend, A. M., and DeMarie, S. M. 2007. "Dispositional factors in internet use: Personality versus cognitive styles," *MIS Quarterly* (31:4), pp. 809-820.

McKnight, D. H., Choudhury, V., and Kacmar, C. 2002. "Developing and Validating Trust Measures for e-Commerce: An Integrative Typology," *Information Systems Research* (13:3), pp. 334-359.

Meschtscherjakov, A. 2009. "Mobile Attachment - Emotional Attachment Towards Mobile Devices and Services," in *Proceedings of the 11th International Conference on Human-Computer Interaction with Mobile Devices and Services*.

Mills, E. 2007. "Google's street-level maps raising privacy concerns," from http://usatoday30.usatoday.com/tech/news/internetprivacy/2007-06-01-google-maps-privacy_N.htm

Murray, J. Y., Kotabe, M., and Zhou, J. N. 2005. "Strategic alliance-based sourcing and market performance: Evidence from foreign firms operating in China," *Journal of International Business Studies* (36:2), pp. 187-208.

Najjar, M., and Bui, S. 2012. "The Influence of Technology Characteristics on Privacy Calculus: A Theoretical Framework," in *Proceedings of the 18th Americas Conference on Information Systems*, Seattle, WA, USA.

Nunnally, J.C. 1978. *Psychometric Theory,* 2nd ed., NY: McGraw-Hill.

Olejnik, S., and Algina, J. 2000. "Measures of Effect Size for Comparative Studies: Applications, Interpretations, and Limitations," *Contemporary Educational Psychology* (25:3), pp. 241-286.

Onwuegbuzie, A. J., and Leech, N. L. 2004. "Enhancing the Interpretation of "Significant" Findings: The Role of Mixed Methods Research," *The Qualitative Report* (9:4), pp. 770-792.

Pew Internet. 2012. "Apps and privacy: More than half of app users have uninstalled or decided to not install an app due to concerns about their personal information," from http://pewinternet.org/Reports/2012/Mobile-Privacy/Main-Findings/Section-1.aspx

Podsakoff, P. M., and Organ, D. 1986. "Self-Reports in Organizational Research: Problems and Prospects," *Journal of Management* (12:4), pp. 531-544.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.Y., and Podsakoff, N. P. 2003. "Common method biases in behavioral research: A critical review of the literature and recommended remedies," *Journal of Applied Psychology* (88:5), pp. 879-903.

Polites, G. L., Roberts, N., and Thatcher, J. 2012. "Conceptualizing Models Using Multidimensional Constructs: A Review and Guidelines for Their Use," *European Journal of Information Systems* (21:1), pp. 22-48.

Qiu, Y., Gopal, A., and Hann, I.-H. 2011. "Synthesizing Professional and Market Logics: A Study of Independent iOS App Entrepreneurs," in *Proceedings of the 32nd International Conference on Information Systems*, Shanghai, China.

Selya, A. S., Rose, J. S., Dierker, L. C., Hedeker, D., and Mermelstein, R. 2012. "A practical guide to calculating Cohen's f^2, a measure of local effect size, from PROC MIXED," *Frontiers in Psychology* (3:111), pp. 1-6.

Shirazi, A. S., Clawson, J., Hassanpour, Y., Tourian, M. J., Schmidt, A., Chi, E. H., Borazio, M., and Laerhoven, K. V. 2013. "Already Up? Using Mobile Phones to Track & Share Sleep Behavior," *International Journal of Human-Computer Studies*, http://dx.doi.org/10.1016/j.ijhcs.2013.03.001

Siemsen, E., Roth, A., and Oliveira, P. 2010. "Common Method Bias in Regression Models With Linear, Quadratic, and Interaction Effects," *Organizational Research Methods* (13:3), pp. 456-476.

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

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

Son, J.-Y., and Kim, S. S. 2008. "Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model," *MIS Quarterly* (32:3), pp. 503-529.

Soper, D. 2012. "Is Human Mobility Tracking a Good Idea?," *Communications of the ACM* (55:4), pp. 35-

37.

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," from http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html

TRUSTe. 2013. "Solutions for App Developers," from http://www.truste.com/industry-solutions/app-developers

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

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. 135-173.

Xu, H., Gupta, S., Rosson, M.B., and Carroll, J.M. 2012a. "Measuring Mobile Users' Concerns for Information Privacy," in *Proceedings of the 33rd International Conference on Information Systems*, Orlando, FL, USA.

Xu, H., Teo, H.-H., Tan, B. C. Y., and Agarwal, R. 2012b. "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), pp. 1342-1363.

Yan, Z., Liu, C., Niemi, V., and Yu, G. 2010. "Effects of Displaying Trust Information on Mobile Application Usage," in *Proceedings of the Lecture Notes in Computer Science* (6407), B. Xie, J. Branke, M. Sadjadi, D. Zhang, and X. Zhou (eds.): Autonomic and Trusted Computing, Berlin: Springer, pp. 107-121.

Zhang, D., Adipat, B., and Mowafi, Y. 2009. "User-Centered Context-Aware Mobile Applications - The Next Generation of Personal Mobile Computing," *Communications of the AIS* (24:3), pp. 27-46.