AIS Transactions on Human-Computer Interaction

Volume 8 | Issue 3 Article 3

9-2016

Limited Information and Quick Decisions: Consumer Privacy Calculus for Mobile Applications

Mark J. Keith
Brigham Young University, mark.keith@gmail.com

Jeffry Babb
West Texas A & M University, jbabb@wtamu.edu

Christopher Furner
East Carolina University, furnerc@ecu.edu

Amjad Abdullat
West Texas A&M University, aabdullat@wtamu.edu

Paul Benjamin Lowry
The University of Hong Kong, paul.lowry.phd@gmail.com

Recommended Citation

Keith, M. J., Babb, J., Furner, C., Abdullat, A., & Lowry, P. (2016). Limited Information and Quick Decisions: Consumer Privacy Calculus for Mobile Applications. *AIS Transactions on Human-Computer Interaction, 8*(3), 88-130. Retrieved from https://aisel.aisnet.org/thci/vol8/iss3/3
DOI:

Transactions on Human – Computer Interaction

Research Paper

Limited Information and Quick Decisions: Consumer Privacy Calculus for Mobile Applications

Mark Jeffrey Keith
Brigham Young University
mark.keith@gmail.com

Jeffrey Babb
West Texas A & M University

Christopher P. Furner
East Carolina University

Amjad Abdullat
West Texas A & M University

Paul Benjamin Lowry
The University of Hong Kong

Abstract:

Mobile applications (also known as “apps”) have rapidly grown into a multibillion-dollar industry. Because they are available through devices that are “always on” and often with the user, users often adopt mobile apps “on the fly” as they need them. As a result, users often base their adoption and disclosure decisions only on the information provided through the mobile app delivery platform (e.g., the Apple App Store™ or Google Play™). The fact that using a mobile app often requires one to disclose an unprecedented combination of personal information (e.g., location data, preferences, contacts, calendars, browsing history, music library) means that one makes a complex risk/benefit tradeoff decision based on only the small amount of information that the mobile app delivery platform provides—and all in a short period of time. Hence, this process is much shorter and much riskier than traditional software adoption. Through two experiments involving 1,588 mobile app users, we manipulated three primary sources of information provided by a platform (app quality ratings, network size, and privacy assurances) to understand their effect on perceptions of privacy risks and benefits and, in turn, how they influence consumer adoption intentions and willingness to pay (WTP). We found that network size influenced not only perceived benefits but also the perceived risks of apps in the absence of perfect information. In addition, we found that integrating a third party privacy assurance system into the app platform had a significant influence on app adoption and information disclosure. We also found that a larger network size reduces LBS privacy risk perceptions, which confirms our information cascade hypothesis. We discuss the implications of these findings for research and practice.

Keywords: Mobile Applications, Location-based Services, Network Effects, Privacy Assurance, Electronic Commerce, Information Cascades, Privacy Seals, Privacy Calculus, Information Privacy

The manuscript was received 08/28/2016 and was with the authors 1 month for 1 revision.

1 Introduction

Mobile applications ("apps") have become pervasive (Gartner, 2015) and have changed our lives in many ways. Each mobile platform allows independent developers to produce apps that take advantage of mobile devices' many technological capabilities, such as Internet access, music playback, email, calendars, contacts, games, cameras, and shopping. Perhaps most importantly, many apps derive part of their value from smartphones' location-based service (LBS) capabilities, which allow for location-based personalization. Location data add a new facet to the risk–benefit tradeoff users make when deciding whether or not to disclose sensitive information—particularly when combined with other forms of personal information on a mobile device (Aloudat & Michael, 2011; Xu, 2010; Xu, Teo, Tan, & Agarwal, 2010). A study of 30 randomly selected, popular LBS apps indicates that 15 of these apps sent their users' location data to remote advertisement servers (Enck et al., 2014). Three of these 15 apps sent data following legitimate requests from the user, and the other 12 apps sent data to servers even though they did not display ads. More recently, a field study revealed that the average consumer's location data is collected without their knowledge 5,398 times every 14 days (Almuhimedi et al., 2015). In addition, both Apple iOS and Google Android mobile operating systems record and transmit location data without the knowledge or consent of device owners (Angwin & Valentino-Devries, 2011).

Clearly, substantial privacy risk is with associated mobile apps and their use. However, this risk does not appear to be slowing users from adopting apps and disclosing their personal information when doing so. Since mobile apps require a relatively small (or no) financial outlay and can be downloaded immediately when needed, users often adopt mobile apps "on the fly" without gathering external validation from friends, family, or other third parties. As previously unknown companies also develop most apps, users have little information about brand credibility to base their perceptions on. As a result, users often have only the limited information that the platform provider provides when making adopting and disclosure decisions. Mobile app delivery platforms such as the Apple App Store and Google Play offer consumers a standardized platform for discovering and comparing mobile apps and typically include app descriptions and consumer reviews. App reviews provide consumers with information about an app's potential quality and network size (based on the number of reviews), while app descriptions might include some form of privacy assurance, though they often do not. In our study, we examine each of these factors (quality, network size, and privacy assurance) separately to determine its influence on intention to adopt mobile apps, intention to disclose information, and willingness to pay. However, integrating these constructs in a mobile app delivery platform presents a unique scenario in which to investigate their combined effects and interactions. Therefore, we phrase our research question as:

RQ: How does the information that mobile app delivery platforms provide affect the perceived privacy risks, benefits, and subsequent adoption of and disclosure to mobile applications?

The literature contains compelling but incomplete research on the intersection between mobile technologies, the human-computer interface, and information privacy (Alter, 2010; Zhang, Li, Scialdone, & Carey, 2009). Researchers have examined privacy risk perceptions associated with LBS in case studies (Aloudat & Michael, 2011; Barkhuus & Dey, 2003; Petrova & Wang, 2011) and in surveys (Moorthy & Vu, 2015; Tsai, Kelley, Cranor, & Sadeh, 2010). However, to guide mobile app platform providers and developers, we need to design, manipulate, and test the key features and characteristics of the mobile interface that affect consumer behavior (e.g., information disclosure). Therefore, we build on the emerging research (e.g., Keith, Babb, Lowry, Furner, & Abdullat, 2015; Steinbart, Keith, & Babb, 2016; Xu, 2010; Xu & Gupta, 2009; Xu, Teo, Tan, & Agarwal, 2012; Xu et al., 2010) aimed at this purpose. While scholarly interest in issues related to privacy and location-based services in the mobile context is increasing (Dahl, Delaune, & Steel, 2012; Freudiger, Shokri, & Hubaux, 2012; Ghinita, 2013; Liccardi, Abdul-Rahman, & Chen, 2016; Papadopoulou & Pelet, 2013; Shin, Ju, Chen, & Hu, 2012; Zhou, 2012), we extend and contribute to the subset of this literature that concentrates on privacy calculus (Dinev & Hart, 2006) as its guiding theoretical lens.

In summary, we address three key research opportunities. First, the literature has yet to address the degree to which network effects and the resulting information cascades influence risk perceptions and app valuation. Second, we examine the effectiveness of privacy seals and written promises in the app context—a practice that is currently, and surprisingly, unstandardized and unused in app markets despite their common deployment in traditional e-commerce. Third, although the literature has considered the standard constructs of intent to adopt/intent to disclose information, the literature has yet to consider what consumers are willing to pay for apps.

To address our research question and the three aforementioned opportunities, we performed two laboratory experiments involving 1,588 mobile app consumers. These experiments manipulated the three primary pieces of information that may mobile app delivery platforms may offer: 1) quality ratings, 2) network size, and 3) privacy assurances. Our results demonstrate that consumers highly value platforms that incorporate third party privacy assurances. In addition, the network size that the platform implied (e.g., based on the number of app reviews) played a pivotal role not only in the perceived benefits of a mobile app but also on the perceived risks—a relationship that prior network research had not yet established.

2 Background on Mobile Privacy

In this research, we focus on how the mobile platform environment—including indicators of quality, network size, and any privacy assurances—determines a consumer's perceived privacy risks associated with mobile apps with a specific focus on location data, which is a special subset of information privacy research (Xu, 2010; Xu et al., 2010). Thus, this research builds on the foundation of location privacy in information privacy research. Research generally defines privacy as the desire to control others' access to and use of personal information (Dinev & Hart, 2006; Kim, 2008; Lukaszewski, Stone, & Johnson, 2016; Slyke, Shim, Johnson, & Jiang, 2006; Xu, 2010). Hence, this information-focused form of privacy is more accurately termed information privacy instead of the broader term privacy (Lowry, Cao, & Everard, 2011; Slyke et al., 2006; Xu et al., 2010). Information privacy refers to "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Malhotra, Kim, & Agarwal, 2004, p. 337; Pavlou, 2011). Likewise, information-privacy concerns "refer to an individual's subjective views of fairness within the context of information privacy" (Malhotra et al., 2004, p. 337; Mohamed & Ahmad, 2012).

The privacy paradox appears to extend to LBS. Although consumers claim to care about privacy (Aloudat & Michael, 2011; FTC, 2009; Keith, Thompson, Hale, Lowry, & Greer, 2013; Microsoft, 2013), they appear to be quite willing to disclose sensitive information over the latest LBS-enabled mobile devices (Kehr, Kowatsch, Wentzel, & Fleisch, 2015; Keith et al., 2013; Microsoft, 2013), which indicates that we do not yet fully understand the tradeoff between perceived benefits and risks in the minds of consumers. This contention is consistent with Williams, Dell, and Venable (2010), who demonstrate that, in a social networking context, users who disclose information generally have a low awareness of the associated risks, which suggests that social networking websites themselves need to create education campaigns to increase understanding of these risks.

Location privacy is the right to limit the extent to which parties record and share information regarding one's current and past location data with other parties (Krumm, 2009; Samuelson, 2008). Likewise, *location data* are data that identify the geographic location of phenomena on the Earth (DeSmith, Goodchild, & Longley, 2007; Krumm, 2009). Location privacy concerns are not new, but innovations in LBS have brought location privacy issues to bear in new and compelling ways. Thus, to understand these issues, this research focuses on privacy concerns specifically related to the mobile app context that prominently includes LBS, which we term LBS privacy and LBS privacy concerns. Importantly, recent research shows that looking at specific information privacy concerns—such as LBS privacy concerns—is more effective than looking at general information privacy concerns (Xu et al., 2010) because context-specific issues influence perceptions of risk.

2.1 Unique Aspects of LBS Apps that Cause High Vulnerability to Privacy Risks

Several aspects of LBS apps make their users especially vulnerable to privacy risks as compared to desktop applications. For one, most consumers do not understand how one can potentially track location data or use it against them (FTC, 2009; Tsai et al., 2010).They are also generally confused as to who has access to their personal and location data (Aloudat & Michael, 2011; FTC, 2009), which makes such data easy to exploit.

Additionally, standards and laws on LBS privacy disclosure are nebulous and less enforceable than in mainstream areas of information privacy, such as in healthcare or financial records. Several countries have recently passed laws that require customer consent for access to location data, but such consent provisions tend to be generic and weak in terms of protecting consumers. After users grant generic consent, an app can easily combine LBS with other personal information from a mobile device, which greatly compounds LBS privacy risks, of which many consumers are not fully aware. With such integration, the user is not simply an anonymous person with a known location; instead, the user is John

A. Doe, phone number 123-4567, email john@doe.com, located at position x, moving at speed y, often travels to $z_{[1\ldots\infty]}$, and so on.

A further privacy concern inherent in LBS lies with the "always on" nature of these devices (Sheng, Nah, & Siau, 2008) due to their using flash memory (Sheng et al., 2008). Thus, regardless of operating system-level controls, privacy assurances, and end-user vigilance, the mere presence of LBS threatens personal information privacy (Seriot, 2010). The growing trend for smartphone users to "jailbreak" their devices to circumvent platform-provider controls and features deemed too restricting also increases the risk that devices will be compromised. In particular, malware is a growing problem for smartphones (Seriot, 2010). Malware developers can obtain a plethora of data via Google searches, YouTube viewing history, social media transactions, keystrokes, phone numbers, photos, email addresses—all combined with current and past geographic location. One can exploit this information given the openly accessible tools inherent to mobile platform software development kits (SDKs) and application programming interfaces (APIs). Despite vigilant oversight in Apple's app-screening process, Apple's App Store has even distributed malware (Seriot, 2010). Due to its greater openness, the Android Market likely has even greater exploitation issues.

3 Theory and Hypotheses

By assessing the effects of the information provided to consumers through mobile app platforms, this study also addresses three theoretical gaps in the literature. Namely, in determining intent to adopt an app, we consider the impact of the app's network size—particularly how network size influences network effects and information cascades—on perceived risks and benefits, intent to adopt, and willingness to pay (WTP). We do so by building on the theory of LBS app adaptation by examining it through the theoretical lens of *privacy calculus* (Culnan, 1993; Culnan & Armstrong, 1999; Dinev & Hart, 2006; James, Warkentin, & Collignon, 2015; Keith et al., 2013; Krasnova, Veltri, & Günther, 2012; Xu, 2010; Xu, Dinev, Smith, & Hart, 2008; Zhang, Li, Luo, & Warkentin, forthcoming), where the decision to adopt LBS-enabled mobile apps is based on a calculated tradeoff between the perceived risks of giving up location data and the expected benefits of the app. We further integrate privacy calculus with theory on network effects and information cascades by characterizing an app's benefits in terms of the value derived from both the app's non-network-based features (i.e., consumers' quality ratings for the app) and the positive externalities associated with the app's network size.

Based on the current app-adoption process, we manipulate the three most relevant features of the mobile app platform (quality ratings, institutional privacy assurance, and network size), which influence users' perceptions of the risks and benefits associated with mobile apps. We also estimate users' adoption intentions and WTP for a given app. As pull-based (consumer-initiated) apps are much more common than push-based apps and because compensation for app use is still developing, we focus solely on non-consumer-compensated, pull-based apps—that is, apps that a user chooses to pay for. By not considering compensation, we omit Xu et al.'s (2010) justice consideration. Finally, consistent with Xu et al. (2010), we focus on initial formations of perceived benefits and risk in the decision to adopt an LBS app.

Figure 1 summarizes the theoretical model. When consumers make decisions on whether to pay for and adopt apps (and, thus, agree to disclose location data), they engage in a privacy calculus that weighs the risks (i.e., LBS privacy risk) against the benefits (i.e., usefulness and ease of use). One calculates these risks and benefits primarily through the factors of privacy assurance, network size, and app quality information, which are presently available to users pre-adoption in the app descriptions in app stores. As dependent variables, we use both intention to adopt (INT) and WTP for LBS apps. We borrowed INT from the technology acceptance model (TAM) literature (Davis, 1989). It represents users' behavioral intentions to fully appropriate an app and, by doing so, disclose their location data. Conversely, WTP is an economics-based variable that provides greater insight into the level of adoption intention (Kim & Son, 2009; Raghu, Sinha, Vinze, & Burton, 2009). WTP would traditionally measure the potential benefits of the app or the consumer's maximized utility subject to budget constraints.

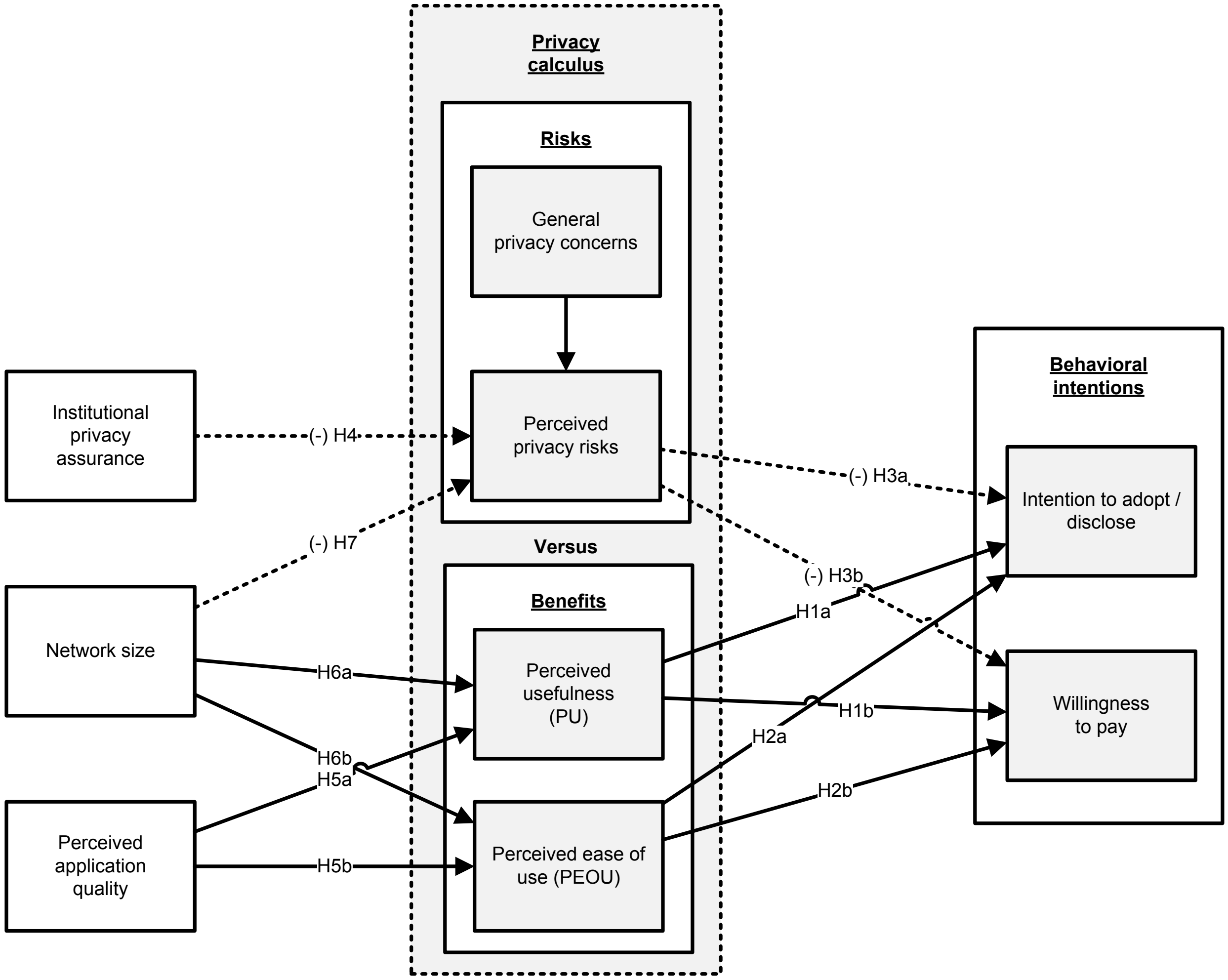


Figure 1. Operationalized Theoretical Model with Testable Hypotheses

Last, we incorporate the information privacy concerns construct, which refers to concerns about the opportunistic, information-related threats of using the Internet in general and not regarding specific mobile apps. Research has also referred to information privacy concerns to as Internet privacy risk (Dinev & Hart, 2006). Research has shown information privacy concerns to increase beliefs about specific risks and to reduce the intention to disclose personal information (Dinev & Hart, 2006; Lowry et al., 2011; Posey, Lowry, Roberts, & Ellis, 2010). As a result, we include it as a control variable in our model but do not formally hypothesize its relationships.

3.1 Privacy Calculus Theory and Hypotheses

Privacy calculus refers to the overall tradeoff of risk and benefit beliefs that lead to a user's intention to provide personal information in return for transacting with a system that provides perceived benefits (Dinev & Hart, 2006). If a user perceives that the benefits outweigh the risks, then the user discloses personal information; otherwise, the user does not. Two qualitative case studies emphasize that LBS users are more willing to accept privacy risks if they find the LBS to be useful (Aloudat & Michael, 2011; Barkhuus & Dey, 2003), and, in the context of this study, we measure users' decision to use LBS apps based not only on the apps' perceived benefits but also on the risks associated with disclosing location data.

Privacy calculus is especially applicable to the app context (Xu, 2010). Although Xu's (2010) work provides an important contribution to the literature, Xu's model's context and hypotheses do not fully answer our research question. That is, Xu uses monetary-based compensation to determine the risks and benefits of a mobile coupon app, while we focus on general non-monetary benefits that likely reflect network-based benefits (Maicas, Polo, & Sese, 2009). Thus, we specifically focus on non-monetary benefits and associated risks (see Sections 3.2 to 3.3).

3.2 Perceived Benefits Regarding LBS Apps

We predict that increased perceived LBS app benefits will increase a consumer's INT and WTP for the app. Xu (2010) focuses on two unique benefits of using apps: 1) their ability to use location-positioning features (i.e., locatability) and 2) their ability to provide personalized experiences and information (i.e., personalization). Yet, one can derive many more benefits from these apps. We focus on how users perceive and expresses apps' benefits. We leverage both TAM and trust theory for more general measures of perceived usefulness (PU) and perceived ease of use (PEOU). With this approach, which is similar to Bouwman and Wijingaert's (2009) one, the consumer self-defines whether an app is useful and easy to use. Importantly, two recent case studies on LBS show that consumers naturally think about both PU[1] and PEOU[2] (and related constructs) as core quality considerations when adopting LBS, but no study to date has empirically tested these concepts with LBS apps. Consequently, if these relationships extend to adopting LBS apps, then the following relationships with hold:

H1: PU increases a) INT and b) WTP for LBS apps.

H2: PEOU increases a) INT and b) WTP for LBS apps.

3.3 Perceived Risks Regarding LBS Apps

Researchers in other fields have studied risk for decades, but Jarvenpaa and Tractinsky (1999) were the first to apply it to online exchanges. Consumers typically assume that transacting with a website is risky unless given reasons to believe otherwise (Malhotra et al., 2004). Perceived risk has a variety of dimensions, including privacy risk (Malhotra et al., 2004), which we primarily focus on. Perceived privacy risk refers to a user's belief that the degree to which they disclose their personal information will have an associated loss (Featherman & Pavlou, 2003). Research has typically operationalized privacy risk as a unidimensional construct that measures the loss of control over personal information (Dinev & Hart, 2006; Xu, 2010). We use the construct LBS privacy risk because we are specifically interested in the effects of one's losing control over one's location data. Aloudat and Michael (2011, p. 39) define LBS privacy risk as "the individual belief of the potential loss and the adverse consequences of using the [LBS] and the probability that these consequences may occur if the service is used."

Research has demonstrated that perceived privacy risk has a negative impact on a user's behavioral intentions to disclose information through e-commerce transactions (Dinev & Hart, 2006; Malhotra et al., 2004). Likewise, we established previously that substantial LBS privacy risks are linked to negative INT in an LBS context (Aloudat & Michael, 2011; Xu, 2010). Replicating and extending this literature, we also propose that the more a consumer perceives an app to be risky, the less they will be willing to pay for the app because similar findings exist in the context of privacy in traditional online shopping (Tsai et al., 2010) and in laboratory experiments (Grossklags & Acquisti, 2007).

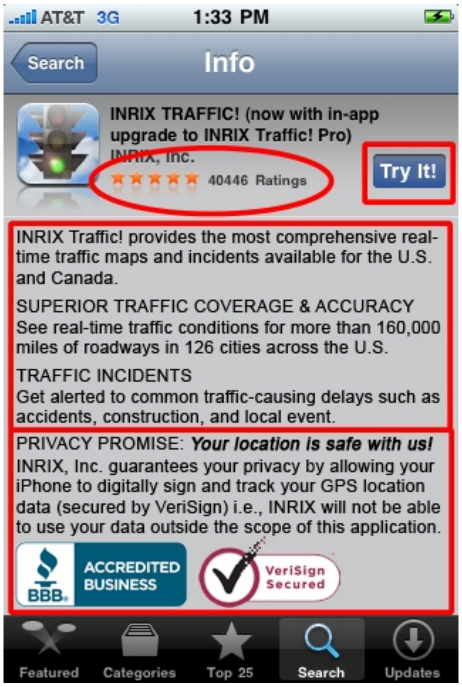
H3: Perceived privacy risks decreases a) INT and b) WTP for LBS apps.

[1] PU represents an individual's "subjective assessment of the utility offered by the new IT in a specific … context" (Gefen et al., 2003, p. 54). Utility typically refers to a system's ability to help its users be more productive in their work and improve the quality of their performance, but users define utility's ultimate nature. Consider the popular app *RedLaser*, which allows iPhone users to take pictures of the bar codes on any product and receive an immediate list of local retailers who offer that product sorted by lowest price with a map to each location. Providing *RedLaser* with one's current location reduces search costs and lowers their total transaction costs. Certainly, the benefit of disclosing location data would help the user to be more productive and efficient, but likely even more important to the consumer's utility is that such an app helps to save them money. In the case of LBS, PU is an indication that being able to customize the information to a consumer's location helps users to experience utility—and, thus, usefulness—as they define it for their context (Aloudat & Michael, 2011). Studies also emphasize that LBS users are more willing to accept privacy risks the more useful they find an LBS to be (Aloudat & Michael, 2011; Barkhuus & Dey, 2003). Hence, PU is a critical perceived benefit for LBS apps.

[2] Similarly, greater PEOU of a mobile app reflects greater perceived benefits and value. PEOU is a measure of the cognitive effort required to use a technology (Venkatesh, Morris, Davis, & Davis, 2003). Thus, PEOU in an LBS context is the degree to which an LBS user perceives the LBS to be easy to use (Aloudat & Michael, 2011). Lower cognitive effort makes a technology more beneficial to a user by making it easier to use, easier to learn, more enjoyable, more efficient, and so on. Research has demonstrated that, if users act rationally as TRA predicts, they will be more inclined to use new IT with greater PEOU (Venkatesh et al., 2003). Two recent qualitative case studies on LBS also support these relationships (Aloudat & Michael, 2011; Barkhuus & Dey, 2003).

3.4 Antecedents of Perceived Benefits and Risks

Because mobile apps typically have a low cost and because one can acquire them immediately, consumers may make their adoption and disclosure decisions based on only the information available through mobile app platform storefronts (i.e., that information in the mobile app's description) such as the Apple App Store or Google Play. This information typically includes the average consumer ratings (number of stars), the number of ratings (indicator of network size), and, in some cases, a form of privacy assurance (which the platform often omits). Figure 2 depicts an example app description with hypothetical privacy seals and a written promise. We base the antecedents of perceived benefits and risks—each with their own supporting theory—on this operationalization to maximize this study's practical implications.



INRIX TRAFFIC! (now with in-app upgrade to INRIX Traffic! Pro)
INRIX, Inc.
★★★★★ 40446 Ratings

INRIX Traffic! provides the most comprehensive real-time traffic maps and incidents available for the U.S. and Canada.

SUPERIOR TRAFFIC COVERAGE & ACCURACY
See real-time traffic conditions for more than 160,000 miles of roadways in 126 cities across the U.S.

TRAFFIC INCIDENTS
Get alerted to common traffic-causing delays such as accidents, construction, and local event.

PRIVACY PROMISE: ***Your location is safe with us!***
INRIX, Inc. guarantees your privacy by allowing your iPhone to digitally sign and track your GPS location data (secured by VeriSign) i.e., INRIX will not be able to use your data outside the scope of this application.

Figure 2. Mobile App Description with Hypothetical Manipulations

3.5 Privacy Assurance

Customer privacy assurance is critical to e-commerce given the pervasive nature of information privacy concerns online (Rifon, LaRose, & Choi, 2005; Yang, Hung, Sung, & Farn, 2006). We define privacy assurance in a way that integrates the concept of institutional privacy assurance, which refers to the mechanisms and interventions that LBS app providers take to assure users that they have taken steps to protect their personal information (Xu et al., 2008; Xu et al., 2010). Industries via self-regulation can form these mechanisms or governments can require them. Because Xue et al. (2010) found that knowledge of, and training in, government regulation is not irrelevant in pull-based app adoption (our context)[3], we consider only industry self-regulation in our model. Such voluntary privacy assurance is based on the

[3] Xu et al. (2010) also considered the effects of government regulation on perceived risks and benefits. They did so by explaining to their participants about Singapore's privacy laws involving location data disclosure and presented them with a news article related to recent legislation and issues related to the matter. They explained these laws further in the context of LBS issues of the U.S. Communication Act of 1996, and they localized the language used in this act to their Singaporean context. While this is a useful method to examine how sudden, increased knowledge of legal LBS issues affects perceived risks and benefits, we omitted this treatment so that the participants would apply their current legal knowledge to the model (which would appear as generally perceived privacy risks) and not be primed by legal knowledge to which they are normally unaware. Most consumers are not fully aware of their rights and legal mechanisms involved with LBS; thus, we felt giving them this knowledge could unduly influence factors that were more important to our study.

concept of structural assurance, which typically refers to the use of privacy seals[4] and privacy assurance statements[5] to positively influence trusting beliefs and decrease risk beliefs in e-commerce transactions.

However, establishing privacy assurance mechanisms for an LBS app does not guarantee that consumers will feel the app assures their privacy—it simply increases the likelihood that that will be the case (Xu et al., 2010). However, since consumers do not always notice or understand these seals (Lowry et al., 2012; Milne & Culnan, 2004; Moores, 2005), these seals are not always enough to overcome deeply seeded privacy concerns. Some studies have shown mixed results with these mechanisms (Hui, Teo, & Lee, 2007; Pennington, Wilcox, & Grover, 2003), and others have even shown failure to decrease perceived risks (Kim, 2008; McKnight, Kacmar, & Choudhury, 2004; Metzger, 2006). Based on such evidence, in this study, we assume reasonable levels of perceived risk and consumers who will generally recognize privacy assurance mechanisms.

H4. Institutional privacy assurance decreases perceived privacy risk for LBS apps.

3.6 Perceived App Quality

According to Katz and Shapiro (1994), a system's overall value (i.e., perceived benefits) is based on both network-dependent value as well as non-network-dependent value. One derives a system's non-network-dependent value from the various features that add value regardless of network size (Kauffman, McAndrews, & Wang, 2000). We are interested in how, in general, apps' non-network-dependent features affect consumers' perceived benefits. Thus, we employ the system quality construct from DeLone and McLean's (2003) well-established IT success model[6] that research has widely established in various contexts (e.g., Hsu, Chang, Chu, & Lee, 2014; Islam, 2012; Lee & Chung, 2009; Rouibah, Lowry, & Al-Mutairi, 2015; Wang & Liao, 2008).

In a qualitative case study on LBS, respondents emphasized the need for system quality, which they discussed in terms of accuracy, timeliness, responsiveness, and reliability (Aloudat & Michael, 2011). Such factors directly influence PEOU and ultimately affect PU. In fact, respondents in the case study "emphasized that without quality and reliability the LBS…would be useless" (p. 50). Based on this foundation and similar findings about quality in studies of m-commerce, we hypothesize:

H5: Higher perceptions of app quality increases the a) PU and b) PEOU of LBS apps.

3.7 Theory and Hypotheses Related to Network Size

Research has connected a system's overall value to both its non-network-based benefits (e.g., system quality) and network size (Katona, Zubcsek, & Sarvary, 2011; Katz & Shapiro, 1985; Kauffman et al., 2000). We expect this relationship to extend to apps. However, we argue that network size can also influence the perceived risks of disclosing location data because of the information cascades phenomenon. We discuss these two separate effects in Sections 3.7.1 and 3.7.2.

[4] A privacy seal is an endorsement from a third party organization that attests that a Web vendor adheres to the organization's privacy policy and a set of privacy standards (McKnight, Choudhury, & Kacmar, 2002). Use of such seals are an example of voluntary industry self-regulation (Xu, 2010). Common examples include TRUSTe, Versign, and BBB Online.

[5] A privacy assurance statement is a statement that a vendor voluntarily supplies that provides argumentation and claims that corresponding product/company assures the customer's privacy (Kim & Benbasat, 2003). The wording of these statements varies by a country's legal requirements but ideally describes the rights and laws involved with a consumer's voluntary disclosure (Xu, 2010).

[6] Of the three subconstructs of DeLone and McLean's (2003) conceptualization of IS quality (system quality, service quality, and information quality), we selected only system quality for this study because of its greater relevance to the LBS app context and because competing LBS apps differ primarily in terms of system quality. For example, multiple LBS apps plot the location of registered sex offenders. However, each of them draws from the same public database of information. Therefore, they provide very similar, or the same, information quality. In addition, because of the relatively small scope and cost of each LBS app, the service component of most apps is quite small compared to more comprehensive desktop-based software and e-commerce. Based on these assumptions, we assert that, of DeLone and McLean's three quality subconstructs, system quality characterizes the greatest variance among LBS apps. As a result, and to focus our study's scope, we employed only system quality, and we refer to it as "app quality" in the remainder of the paper for brevity. System quality refers to characteristics of an IS, such as the presence of "bugs", the consistency of the interface, and, more recently, the quality of the navigational structure (McKnight et al., 2002; Vance, Elie-Dit-Cosaque, & Straub, 2008). Research has found it particularly relevant in research on trust in e-commerce (McKnight et al., 2002) and, more recently, m-commerce (Lowry, Vance, Moody, Beckman, & Read, 2008; Vance et al., 2008).

3.7.1 Network Effects Increase Perceived Benefits

From a network theory perspective, LBS app users trade their location data in return for access to the information provided by a large network base of users. To illustrate, consider the app MouseWait*,* which gives its users real-time updates about the wait times for each of the rides at the Disneyland theme park. Users record their wait times in lines, which the app uses as its source for rides' current wait times. If few people use the app, the information it produces is likely to be inaccurate. However, as more people use the app, the wait times become increasingly accurate. Based on the network-based value of apps such as MouseWait, we argue that both the value of the app's technology and the size of its network base of users will influence user perceptions about the app. The value of the app refers to the consumer's valuation of an app's non-network impacts (Kauffman et al., 2000). With MouseWait, the value derives from other less dynamic information, such as maps of the park and hours, and the technical quality of the app itself and the quality of its user interface.

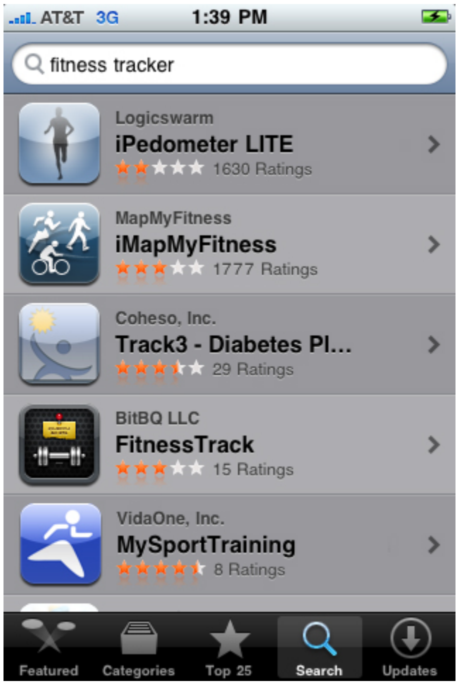
Although not every LBS app benefits from primary network effects, virtually every app can experience secondary benefits from network size. For example, the Urbanspoon app is unique and atypical, which makes it more difficult to learn due to the lack of crossover learning effects from desktop-based websites. Even though the interface might seem intuitive to advanced users, less technically savvy users would likely benefit from having a friend or family member teach them how to use it. As more consumers adopt Urbanspoon, there is a greater likelihood that future users will be able to get help learning to use the app from among their immediate social connections and through online support communities. This support would make using the app more understandable and provide more information on how to get more benefit from the app. Essentially, network size can reduce users' learning costs, which play a major role in the overall transaction costs of a product or service.

H6: Increased perceived network size of LBS apps increases a) PU and b) PEOU.

3.7.2 Information Cascades Decrease Perceived Risks

Network size affects users' valuation of app benefits and risk perceptions. We posit that the information cascades that occur from large network size can help to decrease perceived risks. Information cascades occur "when it is optimal for an individual, having observed the actions of those ahead of him, to follow the behavior of the preceding individual without regard to his own information" (Bikhchandani, Hirshleifer, & Welch, 1992, p. 994). According to information cascade theory, the most fundamental cause of convergent behavior is that individuals face similar decision problems, which Bikhchandani, Hirshleifer, and Welch (1998) indicate as meaning that "people have similar information…[and] face similar action alternatives" (p. 152). These conditions also apply to LBS apps. Each app is relatively narrow in scope compared to larger desktop applications, and, thus, the corresponding purchase and adoption decisions tend to be less complex. Unlike organizational systems such as enterprise resource planning systems—where adoption and purchasing often results from months of organizational decision processes that involve many people—individuals often make LBS app adoption decisions on the fly and based on only the sparse information provided in the app description, which one can also use to infer network size.

Another attribute of information cascades is that network size alone does not determine a cascade (Cha, Benevenuto, Ahn, & Gummadi, 2012; Duan, Gu, & Whinston, 2009). Rather, Duan et al. (2009) explain, for example, that individuals in a decision making situation should be able to decipher not only the number of previous individuals who have made a particular decision (e.g., to purchase product A) but also the number of previous individuals who faced the same decision yet chose a different outcome (e.g., to purchase product B, C, D, or no product at all). This condition also applies in the mobile app context. When consumers search for an app, they receive a list of search results with information about the network size of each app. For example, searching for "fitness tracker" might return a list such as the one that Figure 3 visualizes. Although a consumer cannot view the number of prior consumers who decided against downloading any app at all, they can decipher the approximate percentage who decided to purchase other apps than the one they decide to purchase (assuming each app has a similar percentage of consumers who decide to provide reviews). That is, if consumers decide to purchase iMapMyFitness with 1,777 reviews, they will also know that iPedometer LITE received 1,630 reviews, Fitness Track received 15 reviews (inferring small network size), and so on, which makes the information cascades phenomenon relevant to the mobile app context.



fitness tracker

Logicswarm
iPedometer LITE
1630 Ratings

MapMyFitness
iMapMyFitness
1777 Ratings

Coheso, Inc.
Track3 - Diabetes Pl...
29 Ratings

BitBQ LLC
FitnessTrack
15 Ratings

VidaOne, Inc.
MySportTraining
8 Ratings

Figure 3. Mobile App Description with Hypothetical Manipulations

Clearly, the number of reviews does not perfectly reflect network size, but we argue that it is a useful perceived surrogate. Not all app consumers will provide a review. However, if choosing between two apps where one has 1,000 ratings and another has three ratings (as was often the case when we searched for apps to use for this study), a potential consumer can infer that the app with 1,000 ratings likely has a much larger network size. Consumers can use this information (i.e., the number of reviews) to form two perceptions—each with their own theoretical justification. First, as network theory supports, the number of reviews indicates a potential network externality benefit (Katz & Shapiro, 1985). Second, as the research on information cascades supports, the number of reviews indicates the credibility of the reviews themselves, which can help to dissuade perceived privacy risks (Bikhchandani et al., 1998). Although all apps will demonstrate the latter, not all will demonstrate the former. However, we did not want to exclude this important relationship from our study. Therefore, in our experimental design, we selected two apps with direct network effects and two without.

Prior research has theorized about and examined information cascades. Walden and Brown (2009) examined the popular website download.com and discovered that the number of weekly downloads of a particular online software package was a primary indicator of new adoption decisions (Walden & Browne, 2009). Similarly, Simonsohn and Ariehly (2004) found that the number of existing bids on eBay auctions increased the likelihood of future bids even if the high number of bids simply resulted from a low starting price. Although network size does not directly cause information cascades, it strengthens the cascade and adds to its momentum (Duan et al., 2009).

In the LBS app context, we care about whether information cascades are manifested not in the direct relationship between observed prior behavior and new app adoption but between observed prior behavior and the perceived LBS privacy risks of potential adopters. In other words, does the presence of an observed large network base reduce one's fear that an app provider will act unethically with one's location data? Whereas this effect seems logical—and related research suggests it to be the case—no one has yet examined it empirically. For instance, the literature on online product reviews has demonstrated that the presence, quality, and source of reviews all increase trust in an online product (Ba & Pavlou, 2002; Pavlou & Dimoka, 2006). Yet, we do not know whether review characteristics have the same effect on risk perceptions or how the quantity of online reviews affects perception.

Information cascades is also remarkable because of the opportunities it creates for error to prevail when local experience comes into contention with prevailing sentiment toward the widespread adoption of an LBS app or service. Anderson and Holt (1997) describe situations in which error is compounded via a cascade despite other indications that the cascade's direction is false or erroneous (e.g., the mimetic effect of certain Internet and Web-driven phenomenon that quickly sweep through the general population and then prove to be false in some respect such as the KONY 2012 phenomenon) (Gregory, 2012). Similarly, Watts (2002) notes that, due to their precipitous nature, one cannot easily anticipate what initiates cascades in a network the size of the few notable online app stores because disruptive new cascades are infrequent due to network density and size. Thus, when cascades bring change, it is often swift and complete. In the interim, is the cascade has some inherent stability in its persuasive influence.

Based on information cascades theory (Bikhchandani et al., 1998), as network size increases, potential users feel a greater sense of safety in numbers. Accordingly, potential users are more likely to perceive the decisions of prior adopters as assurance that an LBS provider will not behave opportunistically with user location data regardless of whether it is true.

> **H7:** Increased perceived network size of LBS apps decreases the perceived privacy risk associated with those apps.

4 Methodology

4.1 Design

We used a 3 × 2 × 2 factorial experimental design of 12 different groups. The variables were privacy assurance (none vs. low vs. high), quality rating (low vs. high), and network size (small vs. large). Due to the many possible methods of manipulating privacy assurance, we performed two separate experiments (seven months apart) to assess whether users understood the importance of separating personal identity from location data. Based on the outcomes of the first experiment, we adjusted the wording of the privacy-promise manipulation by adding more details. As the privacy-promise treatment was unique and new to this study, our reviewing the results from the first experiment led to our developing a more granular manipulation.

4.2 Participants

We used college students as participants because the largest demographic block of mobile Internet users are those between the ages of 18 and 29 (Rainie, 2010). We also note that using students as participants to evaluate mobile privacy is advantageous because, in the context of mobile commerce, they are not only more likely to be early adopters but also more apt to pick up on signals regarding privacy risks at the point of app distribution (Pedersen, 2005). Moreover, Rogers (2010) suggests that innovation diffusion is partially predicated on the degree to which a social system and its channels of communication help to spread the innovation. Given the youth bias in innovation diffusion for mobile apps and smartphones, the interface by which apps parties distribute apps constitutes a social channel that youth are more likely to frequent. For these reasons and more, researchers have efficaciously used students in privacy studies that involve mobile information disclosure (e.g., Kehr et al., 2015; Keith et al., 2013; Lowry et al., 2011).

We recruited participants from three large public universities located in Virginia, Texas, and Arizona. Among those universities, 1,588 (509 for experiment 1 and 1,079 for experiment 2) undergraduate and graduate students from their respective business colleges successfully completed the experiment, which took place outside of regular class time. We offered participants both extra credit and a chance to win one of several $50 gift cards. The 1,588 participants represent a 55 percent response rate from those who we solicited to complete the experiment. All three universities provided institutional review-board approval prior to our collecting data, and we followed standard human-subject protocols. Table 1 summarizes the participants' demographic data for experiments 1 and 2.

Table 1. Demographic Statistics for Both Experiments

Demographics	Experiment 1	Experiment 2
Mobile purchases (last year)	7.10 $\bar{x}$ (22.907 σ)	7.08 $\bar{x}$ (17.63 σ)
Age	21.81 $\bar{x}$ (5.18 σ)	20.13 $\bar{x}$ (5.58 σ)
Smartphone users	52.1%	78.8%
Apple iPhone users	18.5%	24.8%

Table 1. Demographic Statistics for Both Experiments

Gender (male/female)	55.0% / 45.0%	53.0% / 47.0%

4.3 Tools, Task, and Procedures

We conducted a scenario-based experiment using an Apple iPhone. Based on a pilot test of 58 participants (26 for experiment 1 and 32 for experiment 2), we selected four different real apps from the iPhone App Store for each experiment. The apps chosen reflected a variety of salient uses for LBS apps: 1) one gave real-time updates on traffic congestion along roads and highways, 2) one allowed users to map their fitness routes, 3) one allowed users to locate friends and family members on a map, and 4) one mapped and located registered sex offenders in the user's area. These apps do not represent manipulations of independent variables but rather offer a range of contexts to reduce any variance attributed to uncaptured, context-dependent variables. Conversely, we chose two of them (the fitness and locator apps) specifically because they offered a primary network-based value to their users[7]. In each context, we selected apps with the fewest reviews of its type to reduce potential participant bias from having prior knowledge. This scenarios approach has been effectively used in the location privacy literature (Xu et al., 2010). Both experiments involved the same five steps, which Appendix B summarizes along with the detailed scenarios. Most participants spent between 15 and 25 minutes with the apps.

4.4 Manipulations of Independent Variables

We manipulated quality, institutional privacy assurance, and network size in the experimental design. We manipulated quality by using Adobe Photoshop to make one version of the app have (out of a total five stars) one star (low quality) and another version have four-and-a-half stars (high quality). The stars represent an overall rating received from prior users. We manipulated network size by editing the total number of reviews (again, for justification on this surrogate, see support for H7). Small network sizes for the four contexts received less than 10 reviews, whereas large network sizes received over 10,000 reviews. As the app store contains many apps, we deemed those that provide the highest potential for network effects and information cascades to be those with 10,000 reviews or more (see Figure 4).

To maximize the study's practical implications, we manipulated privacy in different ways in experiments 1 and 2. In experiment 1, we manipulated the description to include one of the following treatments: 1) no mention of privacy assurance (no assurance), 2) a Better Business Bureau (BBB) privacy seal only (low assurance), or 3) a BBB seal, VeriSign seal, and written statement (high assurance). In experiment 2, the description included either 1) no mention of privacy assurance (no assurance), 2) a written promise stating that the user's location *and* personal identity would be stored but not shared (low assurance), or 3) a written promise stating that the location would be stored but not shared and that their personal identification would *not* be stored at any time. We conducted this manipulation to understand how the user regarded the threat of having their personal identification tied to their location data.

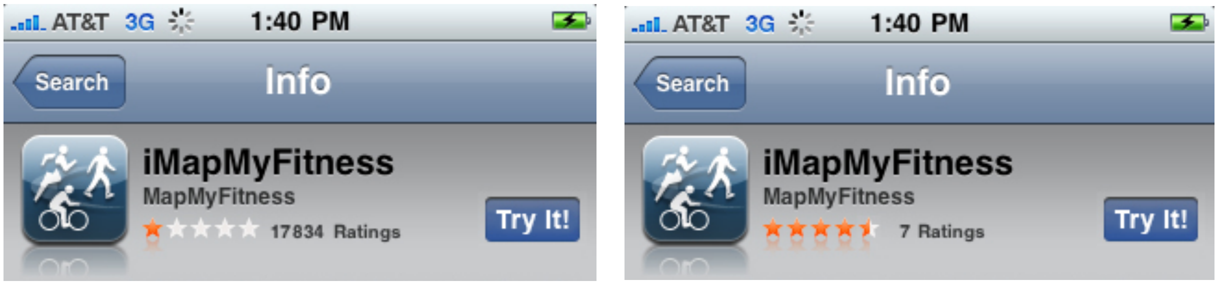


Figure 4. Example of Quality and Network-size Manipulations

[7] Users of app 2 can upload their favorite fitness routes so that they can be shared with others, and app 3 will only locate friends and family members using the same app. Apps 1 and 4 still offer indirect, network-based value in that, as more people adopt these apps, the uncertainty and potential learning curves of future users will be increasingly reduced.

4.5 Measures

Appendix A provides all measurement detail. Here, we summarize our measures. We based PU, PEOU, and INT all on well-validated instruments from existing TAM research (Davis, 1989; Venkatesh et al., 2003). We minimally changed them to reflect the four contexts we describe above.

We drew the privacy concerns construct from prior validated instruments (Dinev & Hart, 2006). We measured perceived privacy risk with items created in a similar manner to those created in prior research (Xu, 2010) but focused primarily on *location* privacy—this study's context. To measure WTP, we used the stated-choice method, which many marketing studies have used (Cameron & James, 1987; Homburg, Koschate, & Hoyer, 2005; Krishna, 1991). Thus, participants were asked: "How much would you be willing to pay for [mobile app name]?"[8]. We also included several controls (including age and gender) based on prior studies. We included a control for the mobile app context and asked participants if they currently used a smartphone or other mobile device (e.g., iPod touch). We also asked them to indicate the number of transactions they had made in the last year over a mobile device (indicating their m-commerce experience) and how many times, to their knowledge, their personal information had been misused as the result of any e-commerce transaction (indicating their privacy risk experience).

5 Data Analysis and Results

Using the latest techniques, we conducted extensive pre-analysis to establish whether the measures were formative and/or reflective. We then determined factorial validity of the reflective measures through convergent and discriminant validity to establish that multicollinearity was not a problem with any of the measures. We also pre-analyzed the data to establish strong reliabilities and to check for common methods bias. Appendix B shows all of these analyses in detail. The results of the factorial validity procedures, checks for multicollinearity, reliability checks, and tests for common method bias show that the models met or exceeded the rigorous validation standards for partial least squares (PLS) structural equation modeling analysis (Gefen & Straub, 2005; Lowry & Gaskin, 2014; Pavlou, Liang, & Xue, 2007; Straub, Boudreau, & Gefen, 2004).

5.1 Manipulation Checks

Before completing our analyses, we first conducted a series of manipulation checks to see if subjects noticed and remembered intended manipulations, which involved a series of four one-item checks that we asked the user after the experiment: 1) "How many stars out of five did this app receive on average from prior users?"; 2) "How many ratings did this app receive?", 3) "Was there a privacy statement?", 4) "Was there a BBB seal?". Results indicate that over 80 percent of all participants answered all questions correctly, which compares well to similar studies.

To establish the intended effects of the manipulations, we captured latent measures of each participant's perceptions of quality, network size, and privacy assurance (see Appendix B). In both experiments, participants perceived significant differences between each manipulation with one exception: participants perceived the privacy assurances manipulation in experiment 1, which included only a BBB seal (low assurance), as no better than no assurance at all. However, in both experiments, participants perceived the inclusion of the VeriSign seal and a written privacy statement as significantly more assuring.

5.2 Results of Hypotheses Testing

Following our validation steps, we analyzed the path model with the PLS-SEM technique using Smart PLS 2.0.M3. We chose PLS because it is an effective technique for early theory development (Chin, Marcolin, & Newsted, 2003; Lowry & Gaskin, 2014) and it does not depend on normal distributions and interval scales (Fornell & Bookstein, 1982), which makes it better suited for WTP and the control variables. To test the structural model, we used the manipulation check scores for quality and network size were because they reflected the participants' perceptions as affected by the treatments—similar to what Komiak and

[8] One minor difference between experiments 1 and 2 is that, in the first experiment, we measured WTP using an open text-box control, which allowed the participant to specify any value. Experiment 2 used a drop-down box with the values 0.00, 0.99, 1.99, 2.99, 3.99, 4.99, 5.99, 6.99, 7.99, and more than 7.99. We based these values on the current average price of iPhone apps (i.e., $3.87) (Kincaid, 2010).

Benbasat (2006) did. We standardized all measurement items and used Chin et al.'s (2003) product-indicator approach to measure the exploratory interaction effects.

Figure 5 summarizes the tests of the theoretical paths in the model for each experiment.

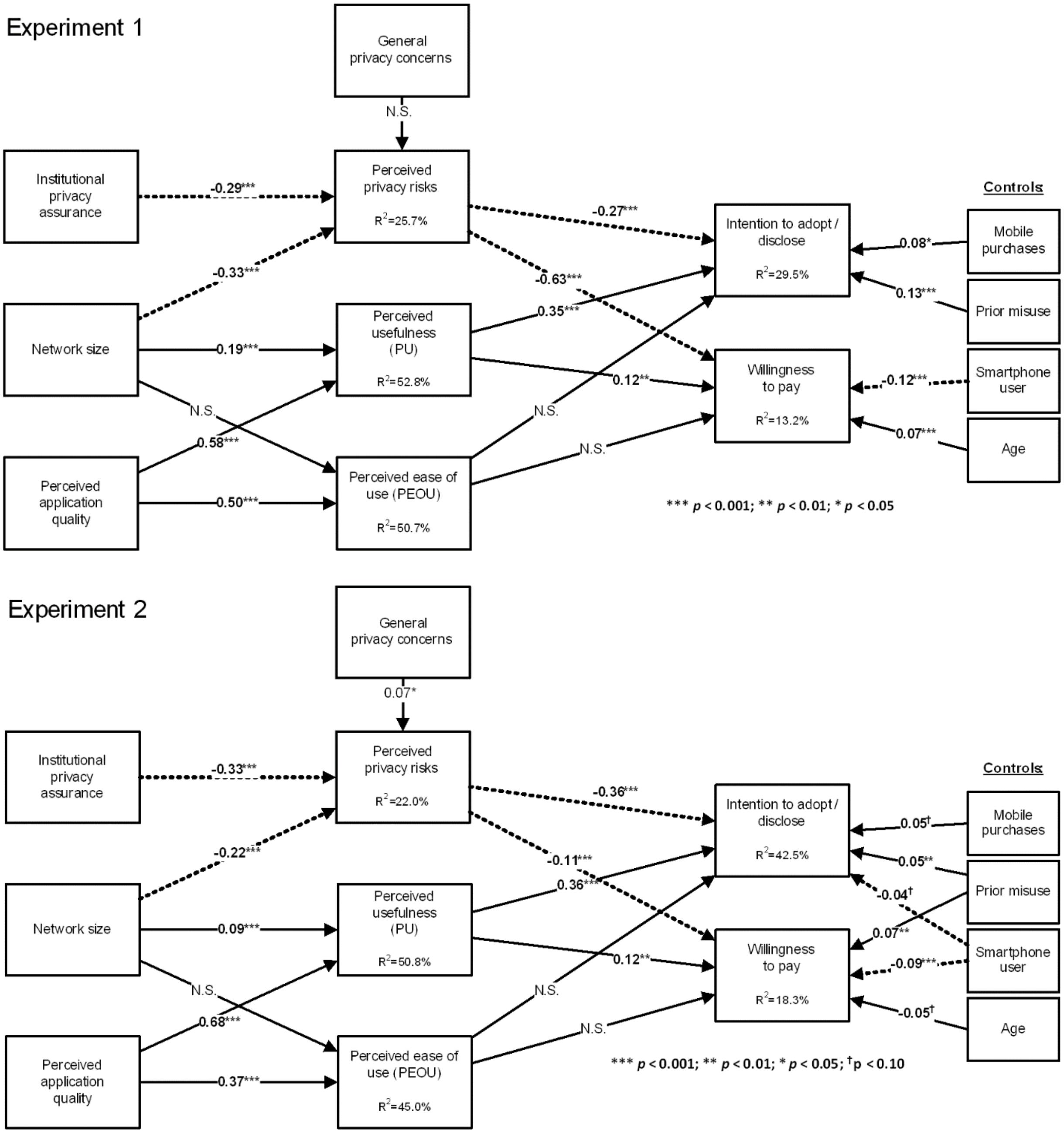


Figure 5. Results of PLS Analysis

The paths between two constructs, along with their direction and significance, indicate the path coefficients or betas (βs). We calculated the significance of the path estimates using a bootstrap technique with 500 resamples. Tables 2 and 3 summarize the measurement model statistics of the two studies. Table 4 summarizes the full testing results. We also explored using five covariates and report their significant relationships. For simplicity, Figure 5 does not include the control variable representing the four mobile app contexts. However, for experiment 1, the mobile app context had no significant direct effects on any variable but did have a significant interaction effect with network size on location privacy risk (β = −0.21, *p* < 0.01). In this experiment, context also moderated the effect of location privacy risk on

WTP (β = −0.19, p < 0.01). In experiment 2, mobile app context moderated the effect of network size on location privacy risk (β = −0.18, p < 0.001).

Table 2. Measurement Model Statistics for Experiment 1

Construct	Mean	SD	1	2	3	4	5	6	7
Willingness-to-pay (1)	$4.89	$8.62							
Intent to adopt (2)	4.01	1.58	.232						
Perceived usefulness (3)	4.59	1.39	.200	.534					
Perceived ease of use (4)	5.14	1.28	.103	.346	.613				
LBS privacy risk (5)	3.93	1.48	−.152	−.463	−.495	−.344			
Network effect (6)	4.39	1.58	.124	.399	.468	.343	−.428		
Quality (7)	4.93	1.34	.144	.444	.680	.692	−.425	.440	
Privacy concern (8)	5.80	1.38	−.070	−.066	.113	.255	.026	.008	.190

Table 3. Measurement Model Statistics for Experiment 2

Construct	Mean	SD	1	2	3	4	5	6	7
Willingness-to-pay (1)	$1.39	$1.55							
Intent to adopt (2)	4.01	1.65	.355						
Perceived usefulness (3)	5.00	1.35	.296	.535					
Perceived ease of use (4)	5.49	1.20	.153	.301	.594				
LBS privacy risk (5)	4.07	1.54	−.272	−.547	−.426	−.344			
Network effect (6)	4.32	1.76	.189	.340	.311	.346	−.428		
Quality (7)	5.03	1.36	.298	.488	.680	.692	−.425	.440	
Privacy concern (8)	5.97	1.23	−.004	−.044	.113	.255	.026	.008	.190

Table 4. Final Model Testing Results

Tested paths	B	t-value	Supports model?	β	t-value	Supports model?
Hypotheses	**Experiment 1**			**Experiment 2**		
H1a: Perceived usefulness → Intention to adopt/disclose	0.348	5.700***	Yes	0.360	10.432***	Yes
H1b: Perceived usefulness → Willingness-to-pay	0.117	1.974*	Yes	0.122	3.075**	Yes
H2a: Perceived ease of use → Intention to adopt/disclose	−0.027	0.502	No	−0.059	1.107	No
H2b: Perceived ease of use → Willingness-to-pay	0.014	0.253	No	0.006	0.158	No
H3a: Perceived privacy risks → Intention to adopt/disclose	−0.272	5.637***	Yes	−0.356	10.568***	Yes
H3a: Perceived privacy risks → Willingness-to-pay	−0.627	2.925**	Yes	−0.113	3.400***	Yes
H4: Institutional privacy assurance → Perceived privacy risks	−0.292	7.433***	Yes	−0.332	5.889***	Yes
H5a: Perceived application quality → Perceived usefulness	0.576	9.726***	Yes	0.675	31.138***	Yes

Table 4. Final Model Testing Results

H5b: Perceived application quality → Perceived ease of use	0.500	16.792***	Yes	0.374	10.408***	Yes
H6a: Network size → Perceived usefulness	0.193	5.173***	Yes	0.085	3.432***	Yes
H6b: Network size → Perceived ease of use	−0.037	1.144	No	0.025	0.915	No
H7: Network size → Perceived privacy risks	−0.330	7.860***	Yes	−0.223	4.361***	Yes
Covariates						
Age → WTP	0.067	3.918***	(n /a)	−0.050	$1.729^{\dagger}$	(n /a)
Smartphone user → WTP	−0.115	2.828**	(n /a)	−0.092	3.280***	(n /a)
Smartphone user →Intent to adopt / disclose	(n / a)	(n /a)	(n /a)	−0.041	$1.700^{\dagger}$	(n /a)
Mobile purchases → Intent to adopt / disclose	0.076	2.358**	(n /a)	0.041	$1.713^{\dagger}$	(n /a)
Prior misuse → WTP	(n / a)	(n /a)	(n /a)	0.074	2.629**	(n /a)
Prior misuse → Intent to adopt / disclose	0.132	2.280*	(n /a)	0.054	2.200*	(n /a)
General privacy concern → perceived privacy risks	(n / a)	(n /a)	(n /a)	0.074	2.285*	(n /a)

Notes: *** p < 0.001, ** p < 0.01, *p < 0.05, $^{\dagger}p$ < 0.10, n/s = not significant; we removed the relationships of non-significant control variables (including app context) from the model and refer to them as N/A in this table.

5.3 Post Hoc Analysis

We performed several exploratory post-hoc tests of interaction effects on endogenous constructs. We examined several interaction effects proposed in prior IT acceptance research to see how factors such as experience, age, and gender influenced adoption intentions. In particular, participants' levels of prior information misuse (β = 0.25, p < 0.05) and whether or not they were smartphone users (β = −0.20, p < 0.05) moderated the effect of perceived LBS privacy risk on WTP. In addition, age moderated the effect of perceived LBS privacy risk on INT (β = 0.62, p < 0.05); PU moderated the effect of perceived LBS privacy risk on WTP (β = −0.31, p < 0.05), indicating that users may be willing to trade a certain amount of LBS privacy risk for greater benefits. We then analyzed the direct effect of increasing privacy assurance on WTP. Both experiment 1 (F = 4.20, p < 0.05) and experiment 2 (F = 5.30, p < 0.05) revealed significant positive effects. Also as part of a post-hoc analysis, we examined the direct effects of institutional privacy assurance, network size, and quality ratings on WTP and INT. Institutional privacy assurances directly impacted WTP (β = 0.13, p < 0.01) but not INT. Network size directly impacted INT (β = 0.26, p < 0.001) but not WTP. Last, quality significantly influenced INT (β = 0.08, p < 0.05) but not WTP.

6 Discussion

Using a privacy calculus model integrated with theory on network effects, we investigated the effects of quality, network size, and institutional privacy assurance on users' adoption intentions and WTP for apps that employ LBS. We found support for most of our hypotheses concerning the adoption and WTP variables. Location privacy risk did significantly reduce both WTP (H3b) and the intention to adopt (H3b). In addition, PU increased both WTP (H1b) and the intention to adopt (H1a). However, after accounting for the impact of location privacy risk and PU, PEOU showed no significant effects (H2a and H2b).

As expected, institutional privacy assurances did reduce users' perceptions of LBS privacy risk (H4). In addition, network size also reduced LBS privacy risk perceptions, which confirms our information cascade hypothesis (H7). Participants clearly understood the added effect of large network size on an LBS app's usefulness (H6a), but they did not believe (or perhaps did not understand) that large network sizes would make an LBS app easier to use (H6b). Finally, perceived LBS app quality had a significant impact on both PU (H5a) and PEOU (H5b).

Moreover, the two data sets (which we captured seven months apart) have several interesting and significant differences. First, the rates of smartphone and iPhone users increased sharply and were well above industry estimates at the time of the original experiment (Kincaid, 2010). The average age of participants was below 22 in both studies but over a year and a half lower in experiment 2. Both of these statistics signal that smartphone use is greater in younger demographics; thus, the sample was biased toward younger participants. As might be expected with a younger sample, the participants in experiment 2 had experienced less information misuse. However, most striking was that average WTP was only US$1.39 in experiment 2 compared to $4.89 in experiment 1. Due to the sharp increase in smartphone users, participants in experiment 2 were more likely to be aware of fair and accurate prices for the apps because of their increased adoption. As the subjects in experiment 2 were slightly younger on average, their lower WTP could also be the result of lower purchasing power.

We did not find support for a relationship between PEOU and intention to adopt nor between PEOU and willingness to pay. These results are surprising because research has demonstrated the relationship between PEOU and positive behavioral outcomes across multiple computing contexts (Davis, 1989; Gefen, Karahanna, & Straub, 2003; Lowry, Gaskin, Twyman, Hammer, & Roberts, 2013; Vance, Elie-Dit-Cosaque, & Straub, 2008; Venkatesh et al., 2003). As such, some characteristics of mobile apps may mitigate the effect that PEOU has on behavioral outcomes. Alternatively, the standardized interface established by mobile app platforms such as Apple iOS may create an environment that maximizes ease of use for all apps. If most apps have a near identical ease of use, PEOU would then become less important in adoption and WTP decisions. Also, we need to consider the physical form factor of the devices as well. Many mobile devices are of a size where the UI experience is more uniform than not.

6.1 Implications for Research and Theory

This study supports the privacy calculus assumption that system adoption decisions are a tradeoff between privacy risks and the benefits of using/adopting a given technology (Dinev & Hart, 2006). Specifically, based on our PLS results, LBS privacy and PU seemed to have similar, albeit competing, influences on adoption intentions. These results also confirm the role that institutional privacy assurances play in reducing perceived risk (Xu, 2010). However, unique to this study, we demonstrate that network effects influence both sides of the privacy calculus equation: network size enhances the perceived value of apps through both direct and indirect network effects and network size reduces apprehension due to LBS privacy risk. With limited information, a large number of positive reviews for an app encourages further adoption.

We also found that network size significantly interacts with privacy signals such as seals and statements of privacy assurance. While most studies on information cascades typically employ economic models of system adoption (e.g., Duan et al., 2009; Walden & Browne, 2009), we confirm, through behavioral experimentation, that a large network size, coupled with limited information, produces the “herd behavior” inherent in information cascades (Bikhchandani et al., 1998). For platform owners, this presents an opportunity to provide additional governance and standardization so that potentially useful apps that are not widely used can claim assurances beyond network effects and information cascades.

This study also demonstrates that technology users are willing to pay for privacy—a notion that has received mixed and controversial support and relatively limited attention. It is possible that the failures of some prior research to find the effects of perceived privacy risk on technology valuation result from poor assurances or manipulations. It is also possible that the new risks associated with location data are not simply minor variations from past privacy risks but something more unique, which requires additional research and theory development.

We can also deduce from our findings that the mobile application platform itself can potentially exert great and authoritative influence on privacy risk perceptions. While risk will remain a tradeoff, satisficing is easier when privacy assurances trickle down from the higher authority of the platform owner who controls all of the key information points that ultimately influence risk perception. In the cases of Google and Apple, their sphere of control influences app developers, the app-acquisition experience, device manufacturers, and communications network providers. These platforms can enforce standards for information privacy assurance, but it is not clear that the imperative to do so exists. On one hand, mobile users care about privacy and will increasingly expect information and controls that enable informed decision making about mobile app adoption. On the other hand, app developers, third party content providers, and platform owners may all wish to use users’ information as a means of monetizing mobile platforms. Given that users do not expect to pay more than a dollar or two for most apps and given that the effort and resources to provide apps to the ecosystem is high, providers will seek some means of profit. Personal data, particularly in the use of LBS, is a rich source of information from which one can make a profit. Some users may not care if someone uses their personal information if it brings some utility, discount, or profit. Thus, our results provide some input for platform owners to consider in developing their strategies to provide information and controls regarding information privacy in the use of mobile apps.

Because our study shows that the effect of network size produces strong results, platform owners can play a strong role in managing network size impressions by displaying numbers of reviewers, numbers of adopters, and so on. However, much as was the case with Web browsers in their infancy, platform owners are competing by differentiating features rather than by embracing standards. Moreover, platforms are often tightly coupled with network providers to the degree that an individual may not uniquely experience the platform.

6.2 Implications for Practice

Our results have many implications for practice, so we now elaborate on actions and strategies that platform holders could adopt to regulate the app industry. The results of our studies show that: 1) measures and mechanisms that provide privacy assurance are critical for app vendors who have not built a large network of users, which is the case for many mobile app developers in the emerging LBS market; 2) even in a large network, a low-rated (and, thus, perceived as low-quality) app must compensate with strong privacy assurance mechanisms; 3) strong ratings and/or a large network may give a false sense of privacy assurance, and 4) a market for privacy assurances in the mobile app market exists. In addition, the second experiment revealed that consumers perceive a greater threat when an app combines their location data with their personal identities. One can argue that location data, because it can be archived as part of a permanent record about an individual, will constitute part of a mobile app user's online reputation and image (Microsoft, 2013). Accordingly, when generating privacy assurance statements, app producers should strongly consider specifying how their product will keep this information separate and safe. Users, app developers, information aggregators and disseminators, and device manufacturers should jointly create privacy assurance mechanisms that effectively increase transparency about privacy risks. By understanding how privacy assurance, network size, and quality interact, developers can tune their businesses' goals to match those that would also benefit their apps.

It is probable that, these results notwithstanding, LBS users will have to take personal responsibility for protecting their privacy. Technical solutions that might facilitate users' personal responsibility could resemble the certificate authority (CA) and public key infrastructure (PKI) systems in place to ensure data integrity using paid third parties. As CA typically issues a digital certificate to verify an owner's identity, a similar third party could verify that location data (or other such private data) has also been signed in a manner consistent with PKI. Until such a complementary industry emerges, mobile app developers must find their own means of assuring privacy. Given the typically quick decision cycle under which individuals purchase most apps, an app developer has only a few tools with which to assure LBS privacy. Although a third party assurance system may help, we found that a short written privacy statement prominently displayed in the app description is a more effective assurance than privacy seals. Mobile platform owners can help this assurance by making such a system a natural, standardized, and governed aspect of the mobile ecosystem into which users and app developers can opt. Users who are more risk tolerant or simply do not care about information privacy in mobile LBS apps and transactions can simply ignore the system.

It is possible, however, that the expense of third party assurance mechanisms, as described above, might not outperform a simple set of assurances realized through standardizing and normalizing mobile platforms or simply through the power of branding (e.g., Lowry et al., 2012; Lowry et al., 2008). As long as Research in Motion, Microsoft, Nokia, Google, and Apple (who each control different mobile platforms) do not fundamentally cooperate on standards related to privacy assurance in their mobile ecosystems, many measures will continue to have a piecemeal effect. We can see a similar situation in the PC platform. Recent versions of Microsoft Windows operating systems certainly establish normative mechanisms that are less confusing around firewall filters for Internet traffic, whereas firewall software was (and, in some cases, remains) the purview of third party solutions. Thus, newer versions of Microsoft Windows ship with an integrated firewall. Thus, the default mode of operation in Microsoft Windows would be to enable the firewall or the system would strongly suggest its use. This tight integration provides norms and expectations in personal computing. Although firewalls are not failure proof (much as privacy controls and assurances are not failure proof), the normative presence of firewalls has adjusted behavior by creating non-ambiguous expectations in users. Although mobile platforms are opening new forms of information access and communication, it is likely that shifting the burden of privacy assurance mechanisms to the platform is the best means of shaping privacy assurance perceptions.

Last, note that mobile app companies may not desire third party privacy assurances. Even if consumers are willing to pay more for an assured app, the provider may lose precious revenue from advertising partners. As a result, consumers' greater WTP for privacy assurance may not recoup information sharing losses. If so, then app providers will prefer to have all apps ignore third party assurances or other governance mechanisms so that customers cannot distinguish between apps that do or do not share consumer information.

6.3 Limitations and Future Research Opportunities

This study has several limitations. First, the measures focus only on the initial formation of trust and privacy impressions—we do not know how this model works with continued app use over time. Risk perceptions could possibly shift based on the actual performance of the app and any associated privacy incidents. One area for future research is longitudinal studies that follow app use over time.

Second, another concern lies in this study's uniform (and binary) presentation of benefits in exchange for privacy, which we simply controlled for. In a manner consistent with contingency theory, the satisficing on constraints that users undertake as they consider privacy risks and trust exists on a wider and more nuanced scale than we afforded in this study. Thus, future research may examine a more nuanced exploration of benefits. Similarly, there are other covariates, such as experience or mobile computing self-efficacy, that we did not include but that research has demonstrated to be salient in IT adoption decisions. Future research should examine such factors.

Third, another limitation relates to the WTP measure and its associated construct. The results indicate that non-iPhone users (or even iPhone users who rarely, or never, pay for apps) do not understand the WTP measure well. We are not certain that pricing and value have stabilized in this market, which has possibly distorted the WTP measure and, thus, resulted in its low variance in experiment 1 (13.2 percent). The results show an improvement in experiment 2 (18.3 percent), which compares well to a related study. We believe that these results arise due to a combination of factors that one cannot fully separate and, hence, that it constitutes a limitation. First, as our descriptive statistics indicate, smartphone adoption dramatically increased in the seven months between the first and second experiments. Naturally, as users become more aware of app pricing schemes, they will have less certainty in their WTP choices. Further, as our treatment presented a hypothetical scenario in which users did not have to spend real money, it is uncertain that subjects experienced a vested basis for valuation. However, this limitation is a common problem with stated-choice measurements. To remedy this limitiation, future studies could present narrow pricing bands based on a market review of existing apps.

Extending this work to make it more generalizable is also important; likewise, others need to challenge and extend this work in contexts where it may not generalize. For example, research has already shown that there can be big cultural differences between Chinese and American mobile technology users that affect risk and privacy perceptions (Lowry et al., 2011). Meaningful cultural differences can also appear in collaborative interactions (Zhang & Lowry, 2008), and these differences can affect trust/risk perceptions (Lowry, Zhang, Zhou, & Fu, 2010), which may also extend to social mobile networks. However, we do not adequately understand the influence of these factors. Moreover, we cannot expect factors such as privacy concerns to hold in other mobile contexts. For example, in a healthcare mobile text setting involving young African Americans, Carter, Corneille, Hall-Byers, Clark, and Younge (2015) found that risk beliefs and privacy concerns were not important factors but technology diffusion factors were.

7 Conclusion

In summary, we found LBS privacy to be a primary concern for LBS adoption, which is increasing and evolving. These findings should motivate both mobile app developers and platform providers to explore new means of assuring LBS privacy in the app marketplace. This need is especially poignant given developments in the mobile app space, where it is increasingly evident that users are not in total control of their location privacy. Indeed, cases in which iPhone users have discovered that the entirety of their location data is stored and easily accessible on their device exist (Johnson, 2011). In particular, mobile app developers will most successfully address LBS privacy when platform providers provide clear structure, guidance, and norms regarding how both users and developers can expect the platform to handle LBS privacy assurances and controls. This research also presents a unique perspective on the relationship between network effects and privacy calculus theory. We believe that platform providers can take advantage of these findings by working together to establish platform-level norms for LBS privacy control. These results should also help to encourage researchers to develop this research stream and keep research at the forefront of practice to not only “observe and report” but also “lead and guide” development related to LBS apps.

References

Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., Cranor, L. F., & Agarwal, Y. (2015). Your location has been shared 5,398 times! A field study on mobile app privacy nudging. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (pp. 787-796).

Aloudat, A., & Michael, K. (2011). Toward the regulation of ubiquitous mobile government: A case study on location-based emergency services in Australia. *Electronic Commerce Research, 11*(1), 31-74.

Alter, S. (2010). Designing and engineering for emergence: A challenge for HCI practice and research. *AIS Transactions on Human-Computer Interaction*, *2*(4), 127-140

Anderson, L. R., & Holt, C. A. (1997). Information cascades in the laboratory. *The American Economic Review*, *87*(5), 847-862.

Angwin, J., & Valentino-Devries, J. (2011). Apple, Google collect user data. *The Wall Street Journal.* Retrieved from http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html

Ba, S. L., & Pavlou, P. A. (2002). Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behavior. *MIS Quarterly, 26*(3), 243-268.

Barkhuus, L., & Dey, A. (2003). Location-based services for mobile telephony: A study of users' privacy concerns. In *Proceedings of the 9th IFIP TC13 International Conference on Human-Computer Interaction* (pp. 709-712).

Bikhchandani, S., Hirshleifer, D., & Welch, I. (1998). Learning from the behavior of others: Conformity, fads, and informational cascades. *Journal of Economic Perspectives, 12*(3), 151-170.

Bouwman, H., & Wijingaert, L. (2009). Coppers context, and conjoints: A reassessment of TAM. *Journal of Information Technology, 24*(2), 186-201.

Burnham, T. A., Frels, J. K., & Mahajan, V. (2003). Consumer switching costs: A typology, antecedents, and consequences. *Journal of the Academy of Marketing Science, 31*(2), 109-126.

Cameron, T. A., & James, M. D. (1987). Estimating willingness to pay from survey Data: An alternative pre-test market evaluation procedure. *Journal of Marketing Research, 24*(4), 389-395.

Carter, L., Corneille, M., Hall-Byers, N. M., Clark, T., & Younge, S. N. (2015). Exploring user acceptance of a text-message base health intervention among young African Americans. *AIS Transactions on Human-Computer Interaction, 7*(3), 110-124.

Cenfetelli, R. T., & Bassellier, G. (2009). Interpretation of formative measurement in information systems research. *MIS Quarterly, 33*(4), 689-707.

Cha, M., Benevenuto, F., Ahn, Y.-Y., & Gummadi, K. P. (2012). Delayed information cascades in Flickr: Measurement, analysis, and modeling. *Computer Networks, 56*(3), 1066-1076.

Chin, W. W., Marcolin, B. L., & 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), 189-217.

Culnan, M. J. (1993). How did they get my name? An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly, 17*(3), 341-361.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*(1), 104-115.

Dahl, M., Delaune, S., & Steel, G. (2012). Formal analysis of privacy for anonymous location based services. In S. A. Mödersheim & C. Palamidessi (Eds.), *Theory of security and applications: Joint* workshop (pp. 98-112). UK: Springer Heidelberg Dordrech.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-340.

DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success: A ten-year update. *Journal of Management Information Systems, 19*(4), 9-30.

DeSmith, M. J., Goodchild, M. F., & Longley, P. (2007). *Geospatial analysis: A comprehensive guide to principles, techniques and software tools*. Leicester: Matador.

Diamantopoulos, A., & Siguaw, J. A. (2006). Formative versus reflective indicators in organizational measure development: A comparison and empirical illustration. *British Journal of Management, 17*(4), 263-282.

Diamantopoulos, A., & Winklhofer, H. M. (2001). Index construction with formative indicators: An alternative to scale development. *Journal of Marketing Research, 38*(2), 269-277.

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

Duan, W., Gu, B., & Whinston, A. B. (2009). Informational cascades and software adoption on the internet: An empirical investigation. *MIS Quarterly, 33*(1), 23-48.

Enck, W., Gilbert, P., Han, S., Tendulkar, V., Chun, B.-G., Cox, L., Jung, J., McDaniel, P., & Sheth, A. (2014). TaintDroid: An information-flow tracking system for real time privacy monitoring on smartphones. *ACM Transactions on Computer Systems, 32*(4).

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human-Computer Studies, 59*(4), 451-474.

Fornell, C., & Bookstein, F. L. (1982). Two structural equation models: LISREL and PLS applied to consumer exit-voice theory. *Journal of Marketing Research, 19*(4), 440-452.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*, 39-50.

Freudiger, J., Shokri, R., & Hubaux, J.-P. (2012). Evaluating the privacy risk of location-based services. In G. Danezis (Ed.), *Financial cryptography and data security* (LNCS 7035, pp. 31-46). Berlin: Springer.

FTC. (2009). *Beyond voice: Mapping the mobile marketplace*. Retrieved from http://www.ftc.gov/reports/mobilemarketplace/mobilemktgfinal.pdf

Gartner. (2015). Gartner says mobile app adoption is maturing as usage mellows. Retrieved from http://www.gartner.com/newsroom/id/3018618

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

Gefen, D., & Straub, D. W. (2005). A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Communications of the Association for Information Systems, 16*, 91-109.

Ghinita, G. (2013). Privacy for location-based services. *Synthesis Lectures on Information Security, Privacy, & Trust, 4*(1), 1-85.

Gregory, S. (2012). Kony 2012 through a prism of video advocacy practices and trends. *Journal of Human Rights Practice*, *4*(3), 463-468.

Grossklags, J., & Acquisti, A. (2007). *When 25 cents is too much: An experiment on willingness-to-sell and willingness-to-protect personal information.* In *Proceedings of the Workshop on Economics of Information Security* (pp. 1-22).

Homburg, C., Koschate, N., & Hoyer, W. D. (2005). Do satisfied customers really pay more? A study of the relationship between customer satisfaction and willingness to pay. *Journal of Marketing, 69*(2), 84-96.

Hsu, M.-H., Chang, C.-M., Chu, K.-K., & Lee, Y.-J. (2014). Determinants of repurchase intention in online group-buying: The perspectives of DeLone & McLean IS success model and trust. *Computers in Human Behavior, 36*, 234-245.

Hui, K. L., Teo, H. H., & Lee, S. Y. T. (2007). The value of privacy assurance: An exploratory field experiment. *MIS Quarterly, 31*(1), 19-33.

Islam, A. (2012). The role of perceived system quality as educators' motivation to continue e-learning system use. *AIS Transactions on Human-Computer Interaction, 4*(1), 25-43.

James, T. L., Warkentin, M., & Collignon, S. E. (2015). A dual privacy decision model for online social networks. *Information & Management, 52*(8), 893-908.

Jarvenpaa, S. L., & Tractinsky, N. (1999). Consumer trust in an internet store: A cross-cultural validation. *Journal of Computer-Mediated Communication, 5*(2), 1-35.

Johnson, B. (2011). Researcher: iPhone location data already used by cops. *Bloomberg Businessweek*. Retrieved from http://www.businessweek.com/technology/content/apr2011/tc20110421_195911.htm

Katona, Z., Zubcsek, P. P., & Sarvary, M. (2011). Network effects and personal influences: The diffusion of an online social network. *Journal of Marketing Research, 48*(3), 425-443.

Katz, M. L., & Shapiro, C. (1985). Network externalities, competition, and compatibility. *American Economic Review, 75*(3), 424-440.

Katz, M. L., & Shapiro, C. (1994). Systems competition and network effects. *Journal of Economic Perspectives, 8*(2), 93-115.

Kauffman, R. J., McAndrews, J., & Wang, Y. M. (2000). Opening the "black box" of network externalities in network adoption. *Information Systems Research, 11*(1), 61-82.

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal, 25*(6), 607-635.

Keith, M. J., Babb, J. S., Lowry, P. B., Furner, C. P., & Abdullat, A. (2015). The role of mobile-computing self-efficacy in consumer information disclosure. *Information Systems Journal, 25*(6), 637-667.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies, 71*(12), 1163-1173.

Kim, D. (2008). Self-perception-based versus transference-based trust determinants in computer-mediated transactions: A cross-cultural comparison study. *Journal of Management Information Systems, 24*(4), 13-45.

Kim, D., & Benbasat, I. (2003). Trust-related arguments in Internet stores: A framework for evaluation. *Journal of Electronic Commerce Research,* 4(2), 49-64.

Kim, S. S., & Son, J. Y. (2009). Out of dedication or constraint? A dual model of post-adoption phenomena and its empirical test in the contest of online services. *MIS Quarterly, 33*(1), 49-70.

Kincaid, J. (2010). comScore: Android market share continues to gain on the iPhone. *TechCrunch*. Retrieved from http://techcrunch.com/2010/04/05/comscore-android-market-share-continues-to-gain-on-the-iphone/

Kock, N. (2010). *WarpPLS 1.0 user manual*. Laredo, TX: ScriptWarp Systems.

Komiak, S. Y. X., & Benbasat, I. (2006). The effects of personalization and familiarity on trust and adoption of recommendation agents. *MIS Quarterly, 30*(4), 941-960.

Krasnova, H., Veltri, N. F., & Günther, O. (2012). Self-disclosure and privacy calculus on social networking sites: The role of culture. *Business & Information Systems Engineering, 4*(3), 127-135.

Krishna, A. (1991). Effect of dealing patterns on consumer perceptions of deal frequency and willingness to pay. *Journal of Marketing Research, 28*(4), 441-451.

Krumm, J. (2009). A survey of computational location privacy. *Personal and Ubiquitous Computing, 13*(6), 391-399.

Lee, K. C., & Chung, N. (2009). Understanding factors affecting trust in and satisfaction with mobile banking in Korea: A modified DeLone and McLean's model perspective. *Interacting with Computers, 21*(5-6), 385-392.

Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilation of enterprise systems: The effect of Institutional pressures and the mediating role of top management. *MIS Quarterly, 31*(1), 59-87.

Liccardi, I., Abdul-Rahman, A., & Chen, M. (2016). I know where you live: Inferring details of people's lives by visualizing publicly shared location data. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (pp. 1-12). Santa Clara, CA: ACM.

Lowry, P. B., Cao, J., & Everard, A. (2011). Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems, 27*(4), 165-204.

Lowry, P. B., & Gaskin, J. (2014). Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it. *IEEE Transactions on Professional Communication, 57*(2), 123-146.

Lowry, P. B., Gaskin, J., Twyman, N. W., Hammer, B., & Roberts, T. L. (2013). Taking "fun and games" seriously: Proposing the hedonic-motivation system adoption model. *Journal of the Association for Information Systems, 14*(11), 617-671.

Lowry, P. B., Moody, G. D., Vance, A., Jensen, M. L., Jenkins, J. L., & Wells, T. (2012). Using an elaboration likelihood approach to better understand the persuasiveness of website privacy assurance cues for online consumers. *Journal of the American Society for Information Science and Technology, 63*(4), 755-766.

Lowry, P. B., Vance, A., Moody, G. D., Beckman, B., & Read, A. (2008). Explaining and predicting the impact of branding alliances and web site quality on initial consumer trust of e-commerce web sites. *Journal of Management Information Systems, 24*(4), 199-244.

Lowry, P. B., Zhang, D., Zhou, L., & Fu, X. (2010). Effects of culture, social presence, and group composition on trust in technology-supported decision-making groups. *Information Systems Journal, 20*(3), 297-315.

Lukaszewski, K. M., Stone, D. L., & Johnson, R. D. (2016). Impact of human resource information system policies on privacy. *AIS Transactions on Human-Computer Interaction, 8*(2), 58-73.

Maicas, J. P., Polo, Y., & Sese, F. J. (2009). The role of (personal) network effects and switching costs in determining mobile users' choice. *Journal of Information Technology, 23*(2), 160-171.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns: The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336-355.

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

McKnight, D. H., Kacmar, C. J., & Choudhury, V. M. (2004). Shifting factors and the ineffectiveness of third party assurance seals: A two-stage model of initial trust in a web business. *Electronic Markets,* 14(3), 252-266.

Metzger, M. J. (2006). Effects of site, vendor, and consumer characteristics on web site trust and disclosure. *Communication Research, 33*(3), 155-179.

Microsoft. (2013). *Data privacy day.* Retrieved from http://www.microsoft.com/privacy/dpd/default.aspx

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read or (or don't read) online privacy notices. *Journal of Interactive Marketing, 18*(3), 15-29.

Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior, 28*(6), 2366-2375.

Moores, T. (2005). Do consumers understand the role of privacy seals in e-commerce? *Communications of the ACM, 48*(3), 86-91.

Moorthy, A. E., & Vu, K. P. L. (2015). Privacy concerns for use of voice activated personal assistant in the public space. *International Journal of Human-Computer Interaction, 31*(4), 307-335.

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory*. New York, NY: McGraw-Hill.

Papadopoulou, P., & Pelet, J.-E. (2013). Trust and privacy in the shift from e-commerce to m-commerce: A comparative approach. In C. Douligeris, N. Polemi, A. Karantjias, & W. Lamersdorf (Eds.), *Collaborative, trusted and privacy-aware e/m-services: 12th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society* (pp. 50-60). London, UK: Springer Heidelberg Dordrecht.

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly, 35*(4), 977-988.

Pavlou, P. A., & Dimoka, A. (2006). The nature and role of feedback text comments in online marketplaces: Implications for trust building, price premiums, and seller differentiation. *Information Systems Research, 17*(4), 392-414.

Pavlou, P. A., Liang, H. G., & Xue, Y. J. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly, 31*(1), 105-136.

Pedersen, P. E. (2005). Adoption of mobile Internet services: An exploratory study of mobile commerce early adopters. *Journal of Organizational Computing and Electronic Commerce, 15*(3), 203-222.

Pennington, R., Wilcox, H. D., & Grover, V. (2003). The role of system trust in business-to-consumer transactions. *Journal of Management Information Systems, 20*(3), 197-226.

Petrova, K., & Wang, B. (2011). Location-based services deployment and demand: A roadmap model. *Electronic Commerce Research, 11*(1), 5-29.

Petter, S., Straub, D. W., & Rai, A. (2007). Specifying formative constructs in information systems research. *MIS Quarterly, 31*(4), 623-656.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & 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), 879-903.

Posey, C., Lowry, P. B., Roberts, T. L., & Ellis, S. (2010). Proposing the online community self-disclosure model: The case of working professionals in France and the UK who use online communities. *European Journal of Information Systems, 19*(2), 181-195.

Raghu, T. S., Sinha, R., Vinze, A., & Burton, O. (2009). Willingness to pay in an open source software environment. *Information Systems Research, 20*(2), 218-236.

Rainie, L. (2010). Internet, broadband, and cell phone statistics. *Pew Research Center*. Retrieve, from http://www.pewinternet.org/Reports/2010/Internet-broadband-and-cell-phone-statistics.aspx

Rifon, N. J., LaRose, R., & Choi, S. M. (2005). Your privacy is sealed: Effects of Web privacy seals on trust and personal disclosures. *The Journal of Consumer Affairs, 39*(2), 339-362.

Rogers, E. M. (2010). *Diffusion of innovations* (4th ed.). New York, NY: The Free Press.

Rouibah, K., Lowry, P. B., & Al-Mutairi, L. (2015). Dimensions of business-to-consumer (B2C) systems success in Kuwait: Testing a modified DeLone and McLean IS success model in an e-commerce Context. *Journal of Global Information Management, 23*(3), 41-70.

Samuelson, P. (2008). *Information law and policy video lectures*. Berkeley, CA: University of California at Berkeley.

Seriot, N. (2010). *iPhone privacy.* Paper presented at the Black Hat DC 2010, Arlington, VA, USA.

Sheng, H., Nah, F. F. H., & Siau, K. (2008). An experimental study on ubiquitous commerce adoption: Impact of personalization and privacy concerns. *Journal of the Association for Information Systems, 9*(6), 344-376.

Shin, K. G., Ju, X., Chen, Z., & Hu, X. (2012). Privacy protection for users of location-based services. *IEEE Wireless Communications, 19*(1), 30-39.

Simonsohn, U., & Ariely, D. (2004). *e-Bay's happy hour: Non-rational herding in on-line auctions* (working paper). Philadelphia, PA: University of Pennsylvania.

Slyke, C. V., Shim, J. T., Johnson, R., & Jiang, J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems, 7*(6), 415-443.

Staples, D. S., Hulland, J. S., & Higgins, C. A. (1999). A self-efficacy theory explanation for the management of remote workers in virtual organizations. *Organization Science, 10*(6), 758-776.

Steinbart, P. J., Keith, M. J., & Babb, J. (2016). Examining the continuance of secure behavior: A longitudinal field study of mobile device authentication. *Information Systems Research, 27*(2), 219-239.

Straub, D. W., Boudreau, M. C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the AIS, 13*, 380-427.

Sun, H. (2010). Developing an interdisciplinary area of economics and human-computer interaction. *AIS Transactions on Human-Computer Interaction, 2*(4), 151-166.

Tsai, J. Y., Kelley, P. G., Cranor, L. F., & Sadeh, N. (2010). Location-sharing technologies: Privacy risks and controls. *Information Society Journal of Law & Policy, 6*(2), 1-26.

Vance, A., Elie-Dit-Cosaque, C., & Straub, D. W. (2008). Examining trust in information technology artifacts: The effects of system quality and culture. *Journal of Management Information Systems, 24*(4), 73-100.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425-478.

Walden, E. A., & Browne, G. J. (2009). Sequential adoption theory: A theory for understanding herding behavior in early adoption of novel technologies. *Journal of the Association for Information Systems, 10*(1), 31-62.

Wang, Y.-S., & Liao, Y.-W. (2008). Assessing eGovernment systems success: A validation of the DeLone and McLean model of information systems success. *Government Information Quarterly, 25*(4), 717-733.

Watts, D. J. (2002). A simple model of global cascades on random networks. *Proceedings of the National Academy of Sciences, 99*(9), 5766-5771.

Williams, N. F. H. T., Dell, P., & Venable, J. (2010). Understanding information disclosure behaviour in Australian Facebook users. *Journal of Information Technology, 25*(2), 126-136.

Xu, H. (2010). Locus of control and location privacy: An empirical study in Singapore. *Journal of Global Information Technology Management, 13*(3), 63-87.

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). *Examining the formation of individual's privacy concerns: Toward an integrative view.* Paper presented at the 29th International Conference on Information Systems, Paris, France.

Xu, H., & Gupta, S. (2009). The effects of privacy concerns and personal innovativeness on potential and experienced customers' adoption of location-based services. *Electronic Markets, 19*(2/3), 137-149.

Xu, H., Teo, H.-H., Tan, B. C. Y., & Agarwal, R. (2012). Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. *Information Systems Research, 23*(4), 1342-1363.

Xu, H., Teo, H. H., Tan, B. C. Y., & 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), 135-174.

Yang, S.-C., Hung, W.-C., Sung, K., & Farn, C.-K. (2006). Investigating initial trust toward e-tailers from the elaboration likelihood model perspective. *Psychology & Marketing, 23*(5), 429-445.

Zhang, D., & Lowry, P. B. (2008). Issues, limitations, and opportunities in cross-cultural research on collaborative software in information systems. *Journal of Global Information Management, 16*(1), 61-84.

Zhang, J., Li, H., Luo, X., & Warkentin, M. (Forthcoming). Exploring the effects of the privacy-handling management styles of social networking sites on user satisfaction: A conflict management perspective. *Decision Sciences*.

Zhang, P., Li, N., Scialdone, M., & Carey, J. (2009). The intellectual advancement of human-computer interaction research: A critical assessment of the MIS literature (1990-2008). *AIS Transactions on Human-Computer Interaction,* 1(3), 55-107.

Zhou, T. (2012). Examining location-based services usage from the perspectives of unified theory of acceptance and use of technology and privacy risk. *Journal of Electronic Commerce Research*, *13*(2), 135-144.

Appendix A: Detailed Measurement Items

Construct	Item code	Lead questions and item scales	When gathered	Citation
Privacy concern	PC1 PC2 PC3	1. Companies should take more steps to make sure that unauthorized people cannot access personal information on their computers. 2. Companies should not use personal information for any purpose unless such use has been authorized by the individuals who provided the information. 3. When companies ask me for my personal information, I sometimes think twice before providing it.	Pre-experiment	(Malhotra et al., 2004)
Perceived app quality	QU1 QU2 QU3 QU4	1. I think the [app name] mobile application would likely be technically reliable. 2. I think the [app name] mobile application would be simple to navigate. 3. I think the [app name] mobile application would make it easy to find the traffic updates I would be interested in. 4. Overall, I think the [app name] mobile application would likely work very well.	Post-experiment	Based on McKnight, Choudhury, & Kacmar (2002)
Perceived location privacy risk	LPR1 LPR2 LPR3 LPR4	1. I think [app name] would protect its customers' location information. 2. I think [app name] would not share or sell my location information. 3. I don't think [app name] would use my location information for unethical purposes. 4. I don't think [app name] would use my location information for any reason other than making their application more useful.	Post-experiment	New for this study, but based on Malhotra et al. (2004)
Perceived network size	NE1 NE2	1. The [app name] mobile application is used by many other people. 2. Many other people have experience with [app name].	Post-experiment	New for this study, but based on relevant theory (Katz & Shapiro, 1985, 1994)
Perceived usefulness	PU1 PU2 PU3	1. The *INRIX Traffic!* mobile application would help me find traffic congestion updates more quickly. 2. The *INRIX Traffic!* mobile application would improve the quality of my traveling. 3. The *INRIX Traffic!* mobile application would make my traveling/commuting more productive. 1. The *iMapMyFitness* mobile application would help me map and record my walking/running/biking routes more quickly. 2. The *iMapMyFitness* mobile application would improve the quality of my fitness training. 3. The *iMapMyFitness* mobile application would make my exercise routine more productive. 1. The *Sex Offenders Search* mobile application would help me locate and map sex offenders in my area more quickly. 2. The *Sex Offenders Search* mobile application would improve the quality of my safety precautions. 3. The *Sex Offenders Search* mobile application would make my safety precautions more productive. 1. The *GPS Tracking* mobile application would help me find my friends and family members more quickly. 2. The *GPS Tracking* mobile application would improve the quality of my location searches of friends and family.	Post-experiment	Based on Venkatesh et al. (2003), but modified to reflect the four LBS app contexts

		3. The *GPS Tracking* mobile application would make locating my friends and family members more productive.		
Perceived ease of use	PEOU1 PEOU2 PEOU3	1. I would find it easy to get [app name] to do what I want it to do. 2. I would find the [app name] mobile application easy to use. 3. The [app name] mobile application would easy to learn.	Post-experiment	(Venkatesh et al., 2003)
Intention to adopt / disclose	INT1 INT2	1. I predict I would use [app name] the next time I need such a mobile application. 2. I plan to use [app name] the next time I need such an application.	Post-experiment	(Venkatesh et al., 2003)

Appendix B: Validity and Analysis Support

Manipulation Checks

As further manipulation checks to establish the intended theoretical effects of our manipulations, we captured participant's perceptions of quality and network size using Likert-type items with a seven-point scale drawn from validated instruments (Burnham, Frels, & Mahajan, 2003; McKnight et al., 2002; Vance et al., 2008). We used these perceptual measures as checks to see if the quality and network size manipulations were valid by comparing the mean of the measurement items for each variable between groups. Participants perceived large network sizes as larger than the small network sizes in both experiment 1 ($\bar{x}$ = 4.88 > 3.89, one-way ANOVA, F(1, 508) = 60.88, p < 0.001) and experiment 2 ($\bar{x}$ = 5.22 > 3.29, one-way ANOVA, F(1, 1078) = 528.48, p < 0.001). Participants perceived higher quality-rated apps as higher quality than the low quality-rated apps in both experiment 1 ($\bar{x}$ = 5.35 > 4.61, one-way ANOVA, F(1, 508) = 57.94, p < 0.001) and experiment 2 ($\bar{x}$ = 5.47 > 4.61, one-way ANOVA, F(1, 1078) = 160.90, p < 0.001).

In experiment 1, we manipulated privacy to include either no mention of privacy assurance (no assurance), a Better Business Bureau (BBB) privacy seal only (low assurance), or a BBB seal, VeriSign seal, and verbal privacy assurance (high assurance). We used the measures for perceived location privacy risk, described below, as a validation check for these manipulations, and it appears that participants did not perceive any value of a BBB seal alone ($\bar{x}$ = 3.88 (low assurance) > 3.85 (no assurance), t(506) = 0.219, p = 0.413). However, participants did perceive a difference between the verbal privacy promise with seals over the seal alone ($\bar{x}$ = 4.44 (high assurance) > 3.88 (low assurance), t(506) = 3.96, p < 0.001).

In experiment 2, the description included either 1) no mention of privacy assurance (no assurance), 2) a written promise stating that the user's location *and* personal identity would be stored but not shared (low assurance), or 3) a written promise stating that the location would be stored but not shared and that their personal identification would *not* be stored at any time. The difference between no privacy assurance and low privacy assurance was significant ($\bar{x}$ = 3.72 (low assurance) > 3.55 (no assurance), t(1076) = 1.77, p < 0.05) as was the difference between low and high privacy assurance ($\bar{x}$ = 4.58 (high assurance) > 3.72 (low assurance), t(1076) = 8.59, p < 0.001). Based on the latter result, participants did appear to comprehend the added risk of disclosing their identification along with the location data to some extent.

Determining the Nature of Our Measures

A key step before assessing factorial validity, which has recently come to light in IS research (Cenfetelli & Bassellier, 2009; Petter, Straub, & Rai, 2007), is to determine which constructs are formative and which are reflective (Diamantopoulos & Winklhofer, 2001). Should researchers make a default assumption that all constructs are reflective, they risk invalidating the results of the factorial validity tests. A high percentage of the recent research in *MISQ* and *ISR* misspecifies constructs as reflective when they are actually formative, which leads to problems in empirical results and theoretical interpretations, including the potential increase in both type I and type II errors. A key sign that one is dealing with a formative measure is that a construct's items are not interchangeable as they are in reflective measures. We used the latest standards as the basis for determining whether we had formative and/or reflective constructs (e.g., Cenfetelli & Bassellier, 2009). In our data collection, we determined all of our measures to be reflective, which the previous validation in the literature of our measures supports.

Establishing Factorial Validity

We then conducted the latest factorial validity checks for reflective measures. To establish the factorial validity of our reflective indicators, we followed Gefen and Straub's (2005) procedures that Lowry and Gaskin (2014) further explain and develop. To establish factorial validity, we examined convergent validity and discriminant validity of the reflective constructs.

Establishing Convergent Validity

We used two approaches to establish convergent validity. First, we examined the outer model loadings. Following (Gefen & Straub, 2005), one can establish convergent validity when the t-values of the outer model loadings are significant. Our t-values were all significant as Table B1 shows with the exception of

PC3—one of the privacy concern items. However, we still included this item in our analysis since it is part of a previously validated instrument (Dinev & Hart, 2006).

As a second check, we correlated the latent variable scores against the indicators as a form of factor loadings and examined the indicator loadings and cross-loadings to establish convergent validity. Though researchers have typically used this approach to establish discriminant validity (Gefen & Straub, 2005), convergent validity and discriminant validity are inter-dependent and help establish each other (Straub, Boudreau, & Gefen, 2004). Convergent validity is also established when each loading for a latent variable is substantially higher than those for other latent variables (Kock, 2010) (see Table B2 for Experiment 1 and Table B3 for Experiment 2).

We conclude that our data in both experiments exhibited strong convergent validity.

Establishing Discriminant Validity

We also used two approaches to establish discriminant validity as Gefen and Straub (2005) describe and Lowry and Gaskin (2014) demonstrate. First, just like with convergent validity, we examined the factor loadings but this this time to ensure significant overlap did not exist between the constructs (again see Table B2 and Table B3).

Second, we used the approach of examining the square roots of the AVEs described in (Gefen & Straub, 2005). The basic standard followed here is that the square root of the AVE for any given construct (latent variable) should be higher than any of the correlations involving the construct (Fornell & Larcker, 1981; Staples, Hulland, & Higgins, 1999) (see Table B4 and Table B5). We show the numbers in the diagonal for constructs (bolded and underlined). All subconstructs showed strong discriminant validity.

We conclude that our data in both experiments exhibited strong discriminant validity.

Establishing Lack of Multicollinearity

SEM methodologists have more recently stressed the potential deleterious effects of multicollinearity and thus the importance of establishing that it is not a significant factor in SEM data (Cenfetelli & Bassellier, 2009). Thus, we assessed the possibility of multicollinearity among all the indicators in the model. Research has traditionally viewed variance inflation factors (VIFs) less than 10 as justification for a model's lack of multicollinearity with 5.0 being ideal for reflective constructs (Cenfetelli & Bassellier, 2009; Diamantopoulos & Siguaw, 2006; Petter et al., 2007). All of the VIFs for the reflective constructs were below this threshold (see Table B6). Thus, we conclude that multicollinearity likely had little to no influence on our models.

Establishing Reliabilities

In terms of the reliability of the reflective constructs, we applied the two most conservative criteria: both the composite reliability and the Cronbach alpha coefficients should be ≥ 0.7 (Fornell & Larcker, 1981; Kock, 2010; Nunnally & Bernstein, 1994). Table B7 summarizes these values, which indicate strong reliabilities. Overall, we conclude that our data exhibited strong reliabilities.

Checking for Common Methods Bias

Once we validated our model for factorial validity and reliabilities, we then checked for common methods bias. We collected all data using a similar-looking online survey, but we still needed to test for common methods bias to establish that it was not a likely factor in our data collection. To do so, we used two approaches.

First, we simply examined a correlation matrix of the constructs (see measurement model statistics in main paper, Table 2 and Table 3) and determine if any of the correlations were above 0.90, which is strong evidence that common methods bias exists (Pavlou et al., 2007). All correlations were below this threshold.

Second, and a more rigorous approach to testing common method bias, we conducted the latest, most extensive form of testing for mono-method bias for PLS, which Liang, Saraf, Hu, and Xue (2007) established. Podsakoff, MacKenzie, Lee, and Podsakoff (2003) developed this test, which Liang et al. (2007) adapted for PLS. It is particularly powerful because research has established that it overcomes the classic issues of assessing common method bias (Liang et al., 2007; Podsakoff et al., 2003). The technique measures the influence of a common latent method factor on each individual indicator in the model versus the influence of each indicator's corresponding construct.

To perform this technique in PLS, one models constructs of the theoretical model and their relationships as is normally conducted with two major additions. First, one creates a single-indicator construct for each indicator in the measurement model. One then links each subconstruct to each of the single-indicator constructs that comprise the subconstruct, which effectively makes each subconstruct in the model a second-order reflective construct. Second, one creates a construct representing the method. This construct reflectively comprises all indicators of the instrument. One then links the method construct (the latent method factor) to each single-item construct.

Table B7 (experiment 1) and Table B8 (experiment 2) capture the detailed analyses of this procedure. For Experiment 1, the average substantive factor loading (λs) was 0.900 and the average variance explained of the substantive factor loading (λs2) was 81.8 percent. In stark contrast, and as desired, the average method factor loading (λm) was 0.002 and the average variance explained of the method factor loading (λm2) was 0.7 percent. The ratio of substantive variance to method variance was about 117:1. Experiment 2 followed the same stark pattern: the average substantive factor loading (λs) was 0.896 and the average variance explained of the substantive factor loading (λs2) was 80.9 percent. The average method factor loading (λm) was 0.001 and the average variance explained of the method factor loading (λm2) was 0.4 percent. The ratio of substantive variance to method variance was about 202:1. Given that our data passed both tests of common method bias—far exceeding expected thresholds—we conclude that there is little reason to believe that the data in either study exhibited negative effects from common method bias.

Table B1. Outer Model Weights to Establish Convergent Validity

	Experiment 1		Experiment 2	
Construct	**Item**	**Outer weight**	**Item**	**Outer weight**
Intention to adopt / disclose	INT1	0.518***	INT1	0.542***
	INT2	0.517***	INT2	0.495***
Perceived usefulness	PU1	0.404***	PU1	0.369***
	PU2	0.407***	PU2	0.363***
	PU3	0.371***	PU3	0.359***
Perceived ease of use	PEOU1	0.333***	PEOU1	0.344***
	PEOU2	0.388***	PEOU2	0.379***
	PEOU3	0.364***	PEOU3	0.370***
Perceived location privacy risk	LPR1	0.310***	LPR1	0.280***
	LPR2	0. 259***	LPR2	0.262***
	LPR3	0. 266***	LPR3	0.270***
	LPR4	0. 275***	LPR4	0.281***
Perceived network size	NE1	0. 559***	NE1	0.548***
	NE2	0. 493***	NE2	0.500***
Perceived app quality	QU1	0. 267***	QU1	0.273***
	QU2	0. 280***	QU2	0.286***
	QU3	0. 302***	QU3	0.300***
	QU4	0. 286***	QU4	0.289***
Privacy concern	PC1	0.310*	PC1	0.317*
	PC2	0.602*	PC2	0.640**
	PC3	0.185 n/s	PC3	0.181 n/s

Notes: *p < 0.05, **p < 0.01, ***p < 0.001, n/s = not significant

Table B2. Reflective Item Loadings and Cross-loadings (Experiment 1)

Indicators	INT	PU	PEOU	LPR	NE	QU	PC
INT1	0.97	0.53	0.36	-0.44	0.38	0.44	-0.05
INT2	0.97	0.51	0.31	-0.46	0.39	0.41	-0.08
PU1	0.39	0.82	0.61	-0.33	0.40	0.66	0.22
PU2	0.48	0.91	0.54	-0.46	0.41	0.58	0.09
PU3	0.49	0.82	0.40	-0.47	0.38	0.48	-0.03
PEOU1	0.23	0.56	0.91	-0.25	0.28	0.62	0.26
PEOU2	0.38	0.61	0.93	-0.38	0.34	0.66	0.24
PEOU3	0.34	0.54	0.92	-0.32	0.33	0.63	0.24
LPR1	-0.47	-0.45	-0.28	0.90	-0.42	-0.41	0.05
LPR2	-0.36	-0.42	-0.25	0.90	-0.38	-0.33	0.03
LPR3	-0.40	-0.45	-0.36	0.90	-0.36	-0.40	0.01
LPR4	-0.42	-0.47	-0.35	0.90	-0.37	-0.39	-0.00
NE1	0.38	0.47	0.35	-0.43	0.96	0.45	0.01
NE2	0.38	0.42	0.30	-0.38	0.94	0.38	0.00
QU1	0.42	0.60	0.54	-0.46	0.45	0.87	0.11
QU2	0.31	0.54	0.65	-0.29	0.34	0.88	0.23
QU3	0.38	0.63	0.66	-0.32	0.34	0.89	0.21
QU4	0.46	0.63	0.58	-0.43	0.44	0.89	0.12
PC1	-0.04	0.10	0.28	0.02	0.03	0.18	0.90
PC2	-0.08	0.10	0.22	0.03	-0.01	0.17	0.97
PC3	-0.02	0.11	0.20	0.01	0.03	0.16	0.75

Table B3. Reflective Item Loadings and Cross-loadings (Experiment 2)

Indicators	INT	PU	PEOU	LPR	NE	QU	PC
INT1	0.97	0.54	0.31	-0.55	0.33	0.49	-0.03
INT2	0.96	0.49	0.27	-0.50	0.32	0.45	-0.06
PU1	0.43	0.89	0.61	-0.37	0.28	0.69	0.19
PU2	0.53	0.94	0.51	-0.41	0.30	0.60	0.12
PU3	0.52	0.93	0.52	-0.40	0.27	0.59	0.12
PEOU1	0.24	0.54	0.89	-0.21	0.19	0.54	0.29
PEOU2	0.30	0.56	0.92	-0.29	0.25	0.57	0.21
PEOU3	0.28	0.53	0.93	-0.25	0.28	0.57	0.25
LPR1	-0.52	-0.40	-0.27	0.90	-0.26	-0.43	0.04
LPR2	-0.48	-0.37	-0.24	0.92	-0.24	-0.38	0.05
LPR3	-0.50	-0.39	-0.25	0.92	-0.25	-0.36	0.06
LPR4	-0.51	-0.40	-0.25	0.92	-0.27	-0.36	0.07
NE1	0.35	0.49	0.23	-0.28	0.96	0.36	0.03
NE2	0.30	0.32	0.24	-0.25	0.95	0.27	0.06
QU1	0.49	0.61	0.46	-0.44	0.32	0.86	0.09
QU2	0.31	0.53	0.60	-0.28	0.26	0.84	0.21
QU3	0.39	0.63	0.55	-0.32	0.26	0.89	0.19
QU4	0.51	0.63	0.50	-0.43	0.33	0.90	0.09
PC1	-0.06	0.14	0.25	0.07	0.05	0.15	0.95
PC2	-0.02	0.13	0.23	0.04	0.02	0.14	0.86
PC3	-0.02	0.14	0.22	0.01	0.02	0.16	0.66

Table B4. Latent Construct Correlations Experiment 1

Construct	INT	PU	PEOU	LPR	NE	QU	PC
INT	**0.966**						
PU	0.534	**0.846**					
PEOU	0.346	0.613	**0.922**				
LPR	-0.463	-0.495	-0.344	**0.901**			
NE	0.399	0.468	0.343	-0.428	**0.950**		
QU	0.444	0.680	0.692	-0.425	0.440	**0.881**	
PC	-0.066	0.113	0.255	0.026	0.008	0.190	**0.877**

Table B5. Latent Construct Correlations Experiment 2

Construct	INT	PU	PEOU	LPR	NE	QU	PC
INT	**0.964**						
PU	0.535	**0.917**					
PEOU	0.301	0.594	**0.914**				
LPR	-0.547	-0.426	-0.344	**0.916**			
NE	0.340	0.311	0.346	-0.428	**0.955**		
QU	0.488	0.680	0.692	-0.425	0.440	**0.871**	
PC	-0.044	0.113	0.255	0.026	0.008	0.190	**0.832**

Table B6. Variable Inflation Factor Scores

Experiment 1		Experiment 2	
Construct	**VIF**	**Construct**	**VIF**
INT	1.384	INT	1.762
PU	2.174	PU	2.415
PEOU	2.227	PEOU	1.867
LPR	1.486	LPR	1.487
NE	1.329	NE	1.218
QU	2.402	QU	2.435
PC	1.066	PC	1.099

Table B7. Reliability Results for Reflective Constructs

	Experiment 1			Experiment 2		
Constructs	**No. of items**	**Cronbach's alpha (α)**	**Composite reliability**	**No. of items**	**Cronbach's alpha (α)**	**Composite reliability**
Intent to adopt	2	0.929	0.966	2	0.925	0.964
Perceived usefulness	3	0.800	0.883	3	0.906	0.941
Perceived ease of use	3	0.911	0.944	3	0.902	0.939
Location privacy risk	4	0.923	0.945	4	0.936	0.954
Network effect	2	0.892	0.948	2	0.903	0.954
Quality	4	0.904	0.933	4	0.894	0.926
Privacy concern	3	0.861	0.909	3	0.798	0.868

Table B8. Common Methods Bias Analysis for Experiment 1

Construct	Indicator	Substantive factor loading (λs)	Substantive factor variance explained (λs^2)	Method factor loading (λm)	Method factor variance explained (λm^2)
Intent to adopt	INT1	0.954***	91.0%	0.018	0.0%
	INT2	0.978***	95.6%	-0.018	0.0%
Perceived usefulness	PU1	0.626***	39.2%	0.200**	4.0%
	PU2	0.964***	92.9%	-0.061*	0.4%
	PU3	0.933***	87.0%	-0.124*	1.5%
Perceived ease of use	PEOU1	1.011***	102.2%	-0.116**	1.3%
	PEOU2	0.828***	68.6%	0.120**	1.4%
	PEOU3	0.927***	85.9%	-0.004	0.0%
Location privacy risk	LPR1	0.859***	73.8%	-0.043	0.2%
	LPR2	0.970***	94.1%	0.094**	0.9%
	LPR3	0.894***	79.9%	-0.019	0.0%
	LPR4	0.880***	77.4%	-0.032	0.1%
Network effect	NE1	0.921***	84.8%	0.047*	0.2%
	NE2	0.979***	95.8%	-0.047*	0.2%
Quality	QU1	0.813***	66.1%	0.070	0.5%
	QU2	1.009***	101.8%	-0.152***	2.3%
	QU3	0.894***	79.9%	0.013	0.0%
	QU4	0.810***	65.6%	0.095*	0.9%
Privacy concern	PC1	0.903***	81.5%	0.016	0.0%
	PC2	0.928***	86.1%	-0.021	0.0%
	PC3	0.823***	67.7%	0.005	0.0%
Average		0.9000.818	81.8%	0.002	0.7%
Notes: *** *p* < 0.001, ** *p* < 0.01, * *p* < 0.05					

Table B9. Common Methods Bias Analysis for Experiment 2

Construct	Indicator	Substantive factor loading (λs)	Substantive factor variance explained (λs^2)	Method factor loading (λm)	Method factor variance explained (λm^2)
Intent to adopt	INT1	0.937***	87.8%	0.043***	0.2%
	INT2	0.992***	98.4%	-0.043***	0.2%
Perceived usefulness	PU1	0.691***	47.7%	0.222***	4.9%
	PU2	1.029***	105.9%	-0.104***	1.1%
	PU3	1.021***	104.2%	-0.106***	1.1%
Perceived ease of use	PEOU1	0.916***	83.9%	-0.023	0.1%
	PEOU2	0.890***	79.2%	0.038	0.1%
	PEOU3	0.937***	87.8%	-0.016	0.0%
Location privacy risk	LPR1	0.870***	75.7%	-0.051**	0.3%
	LPR2	0.939***	88.2%	0.027	0.1%
	LPR3	0.934***	87.2%	0.018	0.0%
	LPR4	0.921***	84.8%	0.004	0.0%
Network effect	NE1	0.938***	88.0%	0.034***	0.1%
	NE2	0.971***	94.3%	-0.034***	0.1%
Quality	QU1	0.858***	73.6%	0.005	0.0%
	QU2	0.838***	70.2%	-0.010	0.0%
	QU3	0.794***	63.0%	-0.019	0.0%
	QU4	0.809***	65.4%	0.023	0.1%
Privacy concern	PC1	0.878***	77.1%	-0.004	0.0%
	PC2	0.884***	78.1%	-0.012	0.0%
	PC3	0.767***	58.8%	0.019	0.0%
Average		0.896	80.9%	0.001	0.4%

Notes: *** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$

Experimental Steps and Scenarios

Experimental Steps

Step 1

Each participant navigated to the website where the experimental simulation was hosted. After reading an IRB cover letter, we gave them a short pretest to measure their privacy concern.

Step 2

Next, the Web application randomly assigned them to one of 48 different simulations (12 group manipulations x 4 contexts) so that each participant viewed a simulation of one particular context. To do so, we wrote an algorithm that measured the current number participants in each of the 48 groups, sorted those groups by the count of completed surveys, and then randomly assigned the next user to one of the groups with the lowest count. This process assured both random and equal assignment to treatments.

Step 3

Next, we gave participants a hypothetical scenario related to one of the four previously described applications. The idea was to set up a realistic context for an app that a typical consumer might want to use and to provide a descriptive context for why that might be the case (e.g., receive better traffic information to help with commute from work). The hypothetical scenarios also helped set up the respective LBS privacy issues associated with the given application (We provide these specific scenarios in the table that follows step 5).

Step 4

After checking a required box to confirm that they read and understood their scenario, we gave participants a series of 9-12 screen shots (depending on the context) that simulated the process of searching the Apple App Store for an app that met their needs, downloading and installing the app, opening the app, and using it once for its intended purpose. The screen shots allowed the user to use their mouse to click the actual buttons on the iPhone images to complete the simulation. These screen shots were based on actual iPhone images but modified to reflect differences in privacy assurance, quality ratings, and network size (see manipulations in the table that follows step 5).

Step 5

After they completed the simulation, we gave participants a post-test survey that included our measures and manipulation checks.

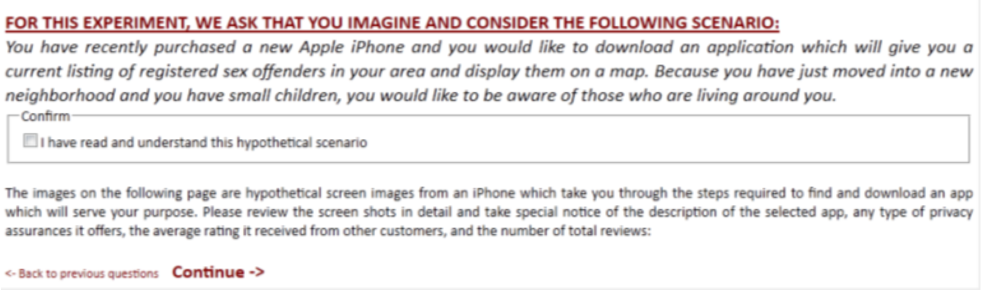
Documentation on Scenarios

Page 1

We took the screenshots to the right from the Web-based simulation and represent the four scenarios (1 per participant) adminsitered after participants completed all pre-experiment survey questions and before we administered the post-experiment survey questions.

The screen shots below vary depending on which of the four scenarios the participant was randomly (and systematically) assigned to.

Sex offender scenario



FOR THIS EXPERIMENT, WE ASK THAT YOU IMAGINE AND CONSIDER THE FOLLOWING SCENARIO:

You have recently purchased a new Apple iPhone and you would like to download an application which will give you a current listing of registered sex offenders in your area and display them on a map. Because you have just moved into a new neighborhood and you have small children, you would like to be aware of those who are living around you.

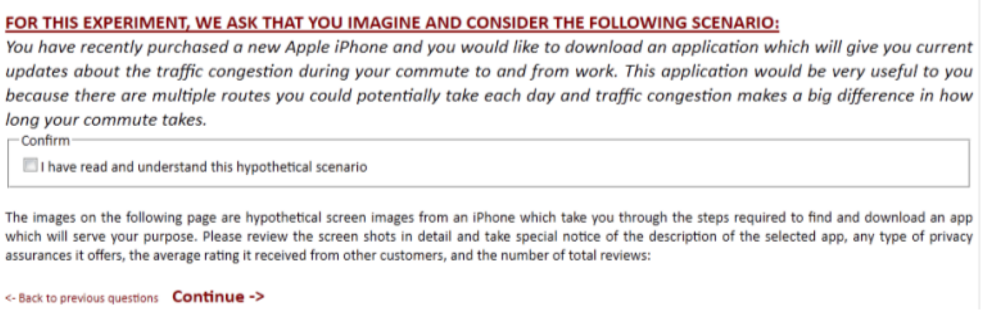
Confirm

□ I have read and understand this hypothetical scenario

The images on the following page are hypothetical screen images from an iPhone which take you through the steps required to find and download an app which will serve your purpose. Please review the screen shots in detail and take special notice of the description of the selected app, any type of privacy assurances it offers, the average rating it received from other customers, and the number of total reviews:

<- Back to previous questions **Continue ->**

Traffic congestion scenario



FOR THIS EXPERIMENT, WE ASK THAT YOU IMAGINE AND CONSIDER THE FOLLOWING SCENARIO:

You have recently purchased a new Apple iPhone and you would like to download an application which will give you current updates about the traffic congestion during your commute to and from work. This application would be very useful to you because there are multiple routes you could potentially take each day and traffic congestion makes a big difference in how long your commute takes.

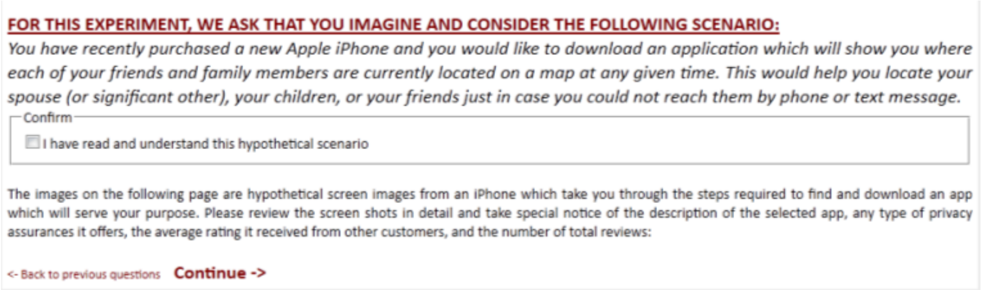
Confirm

□ I have read and understand this hypothetical scenario

The images on the following page are hypothetical screen images from an iPhone which take you through the steps required to find and download an app which will serve your purpose. Please review the screen shots in detail and take special notice of the description of the selected app, any type of privacy assurances it offers, the average rating it received from other customers, and the number of total reviews:

<- Back to previous questions **Continue ->**

Friend locator scenario



FOR THIS EXPERIMENT, WE ASK THAT YOU IMAGINE AND CONSIDER THE FOLLOWING SCENARIO:

You have recently purchased a new Apple iPhone and you would like to download an application which will show you where each of your friends and family members are currently located on a map at any given time. This would help you locate your spouse (or significant other), your children, or your friends just in case you could not reach them by phone or text message.

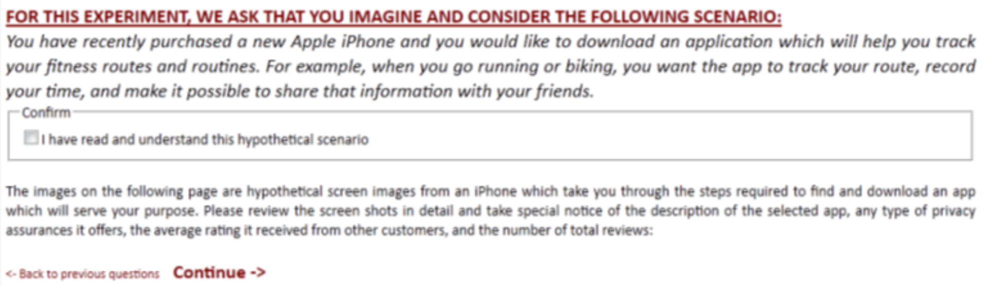
Confirm

□ I have read and understand this hypothetical scenario

The images on the following page are hypothetical screen images from an iPhone which take you through the steps required to find and download an app which will serve your purpose. Please review the screen shots in detail and take special notice of the description of the selected app, any type of privacy assurances it offers, the average rating it received from other customers, and the number of total reviews:

<- Back to previous questions **Continue ->**

Fitness tracker scenario



FOR THIS EXPERIMENT, WE ASK THAT YOU IMAGINE AND CONSIDER THE FOLLOWING SCENARIO:

You have recently purchased a new Apple iPhone and you would like to download an application which will help you track your fitness routes and routines. For example, when you go running or biking, you want the app to track your route, record your time, and make it possible to share that information with your friends.

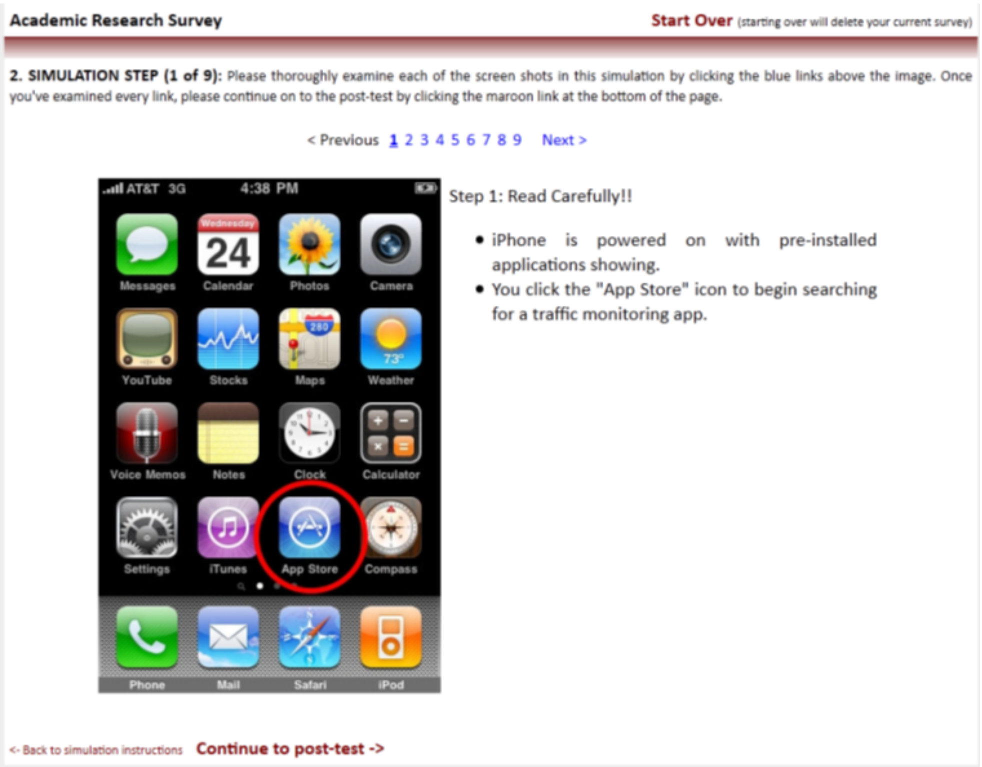
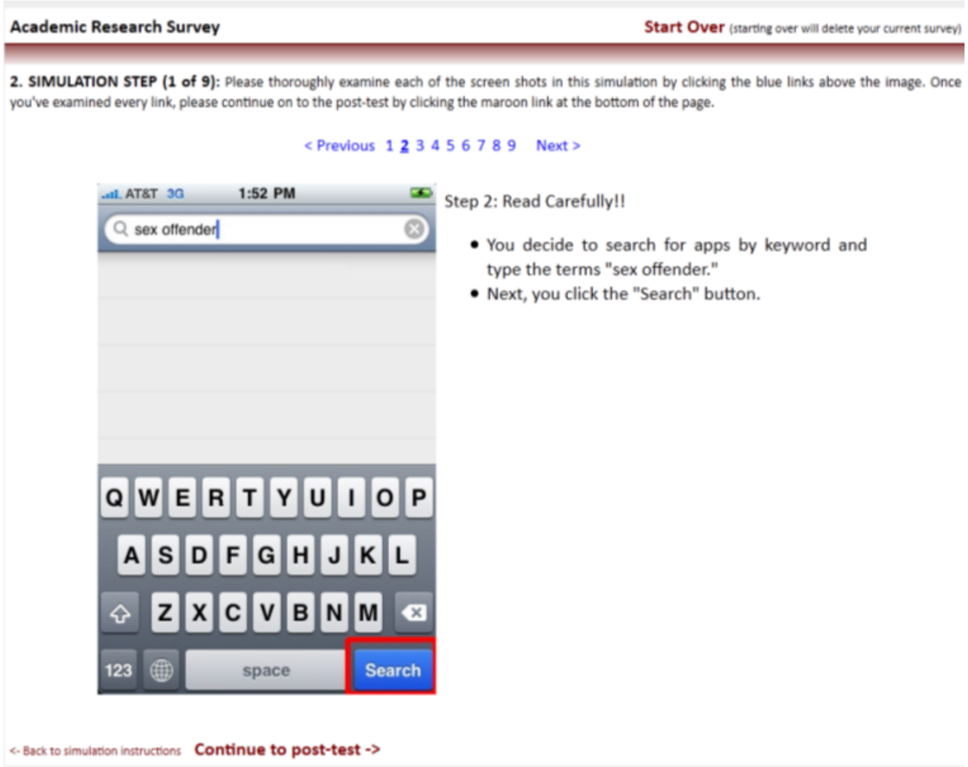
Confirm

□ I have read and understand this hypothetical scenario

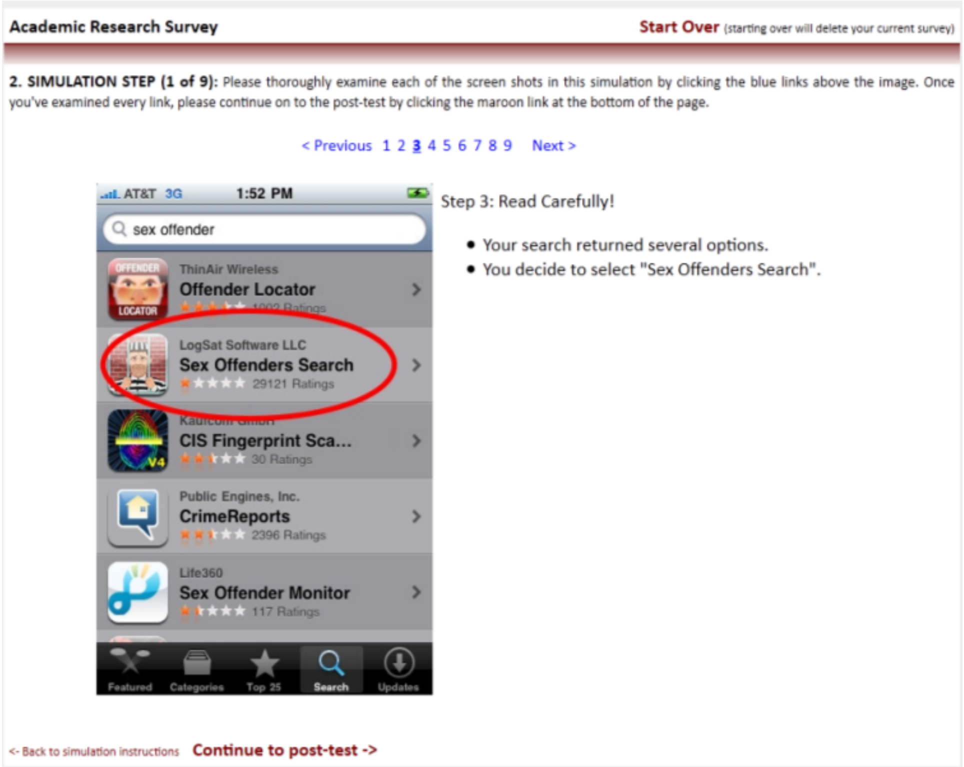
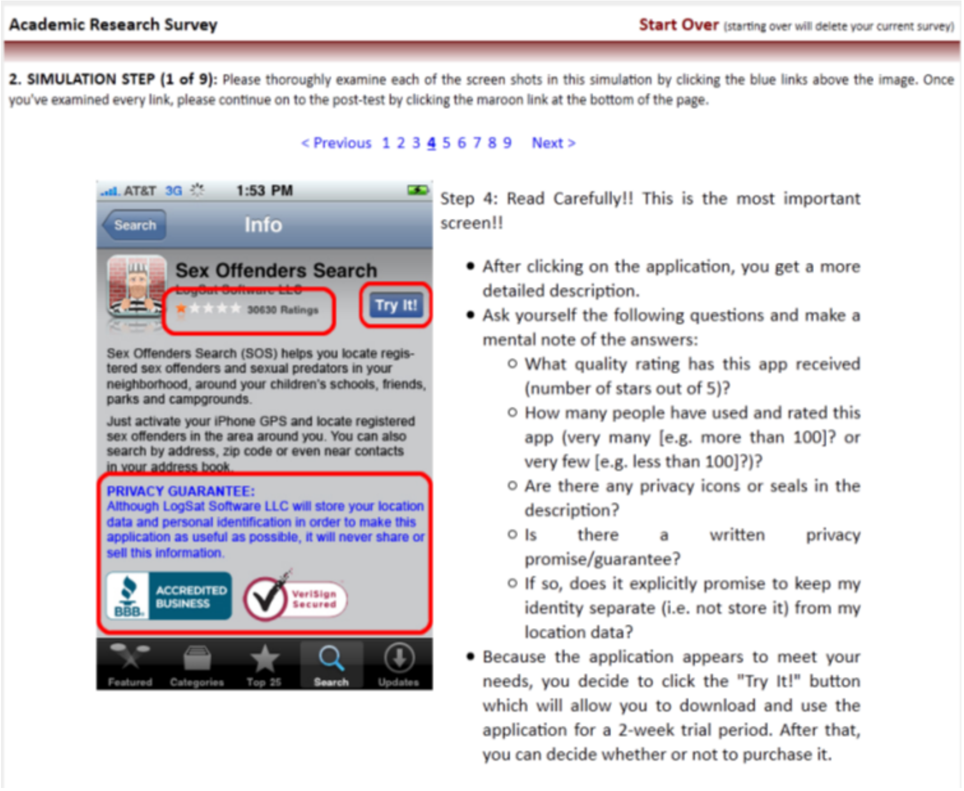
The images on the following page are hypothetical screen images from an iPhone which take you through the steps required to find and download an app which will serve your purpose. Please review the screen shots in detail and take special notice of the description of the selected app, any type of privacy assurances it offers, the average rating it received from other customers, and the number of total reviews:

<- Back to previous questions **Continue ->**

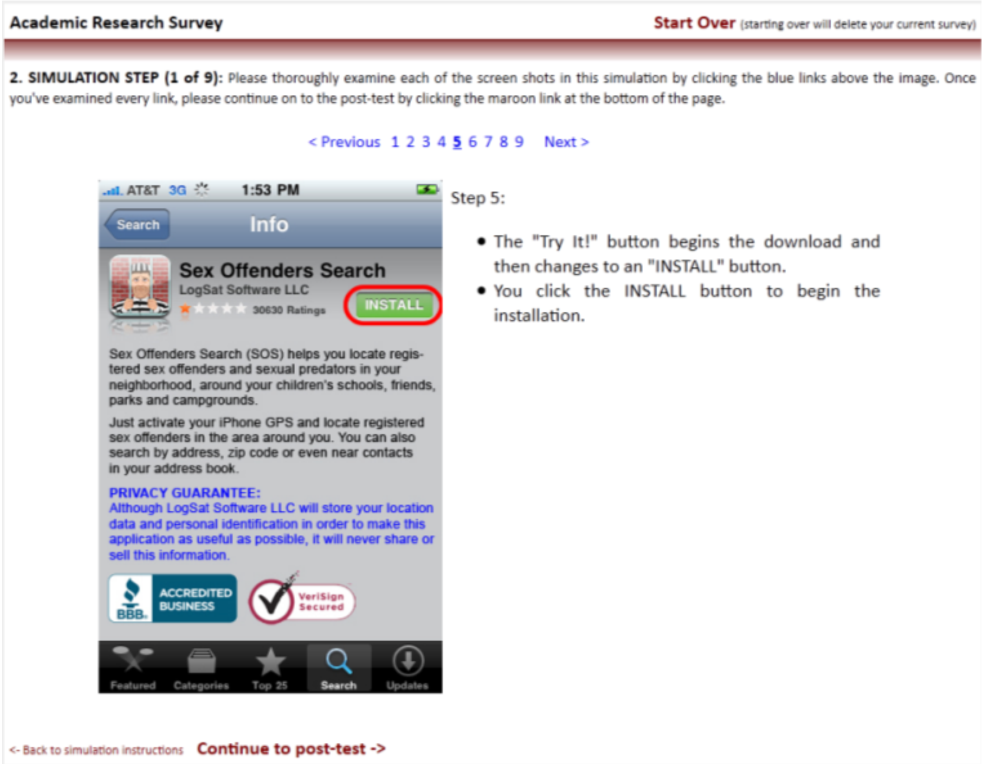
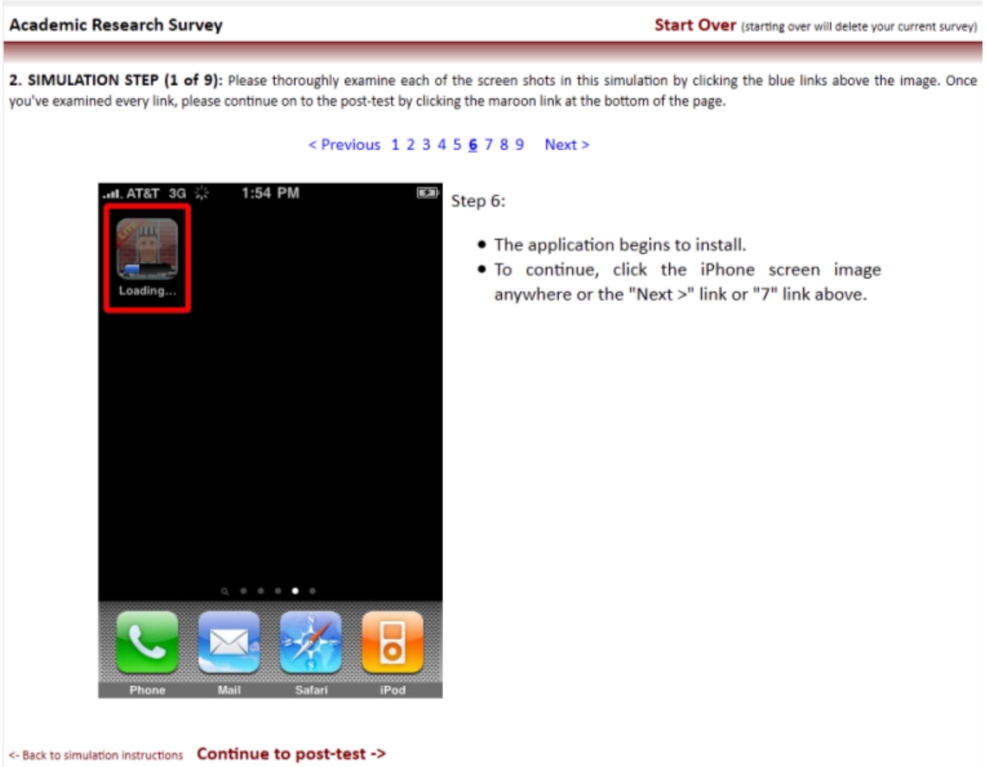
Documentation on Scenarios

Page 2 The following series of screen shots is for the sex offender locator app only. The other four scenarios followed a nearly identical set of 9 to 10 steps but used the screen shots relevant to each app. Also, notice that each required mouse click is highlighted in red. The participants could click the actual buttons to navigate through the simulation, which further enhanced the realism.	 **Academic Research Survey** **Start Over** (starting over will delete your current survey) **2. SIMULATION STEP (1 of 9):** Please thoroughly examine each of the screen shots in this simulation by clicking the blue links above the image. Once you've examined every link, please continue on to the post-test by clicking the maroon link at the bottom of the page. < Previous 1 2 3 4 5 6 7 8 9 Next > AT&T 3G 4:38 PM Wednesday 24 Messages Calendar Photos Camera YouTube Stocks Maps Weather Voice Memos Notes Clock Calculator Settings iTunes App Store Compass Phone Mail Safari iPod Step 1: Read Carefully!! • iPhone is powered on with pre-installed applications showing. • You click the "App Store" icon to begin searching for a traffic monitoring app. <- Back to simulation instructions **Continue to post-test ->**
Page 3	 **Academic Research Survey** **Start Over** (starting over will delete your current survey) **2. SIMULATION STEP (1 of 9):** Please thoroughly examine each of the screen shots in this simulation by clicking the blue links above the image. Once you've examined every link, please continue on to the post-test by clicking the maroon link at the bottom of the page. < Previous 1 2 3 4 5 6 7 8 9 Next > AT&T 3G 1:52 PM sex offender Q W E R T Y U I O P A S D F G H J K L Z X C V B N M 123 space Search Step 2: Read Carefully!! • You decide to search for apps by keyword and type the terms "sex offender." • Next, you click the "Search" button. <- Back to simulation instructions **Continue to post-test ->**

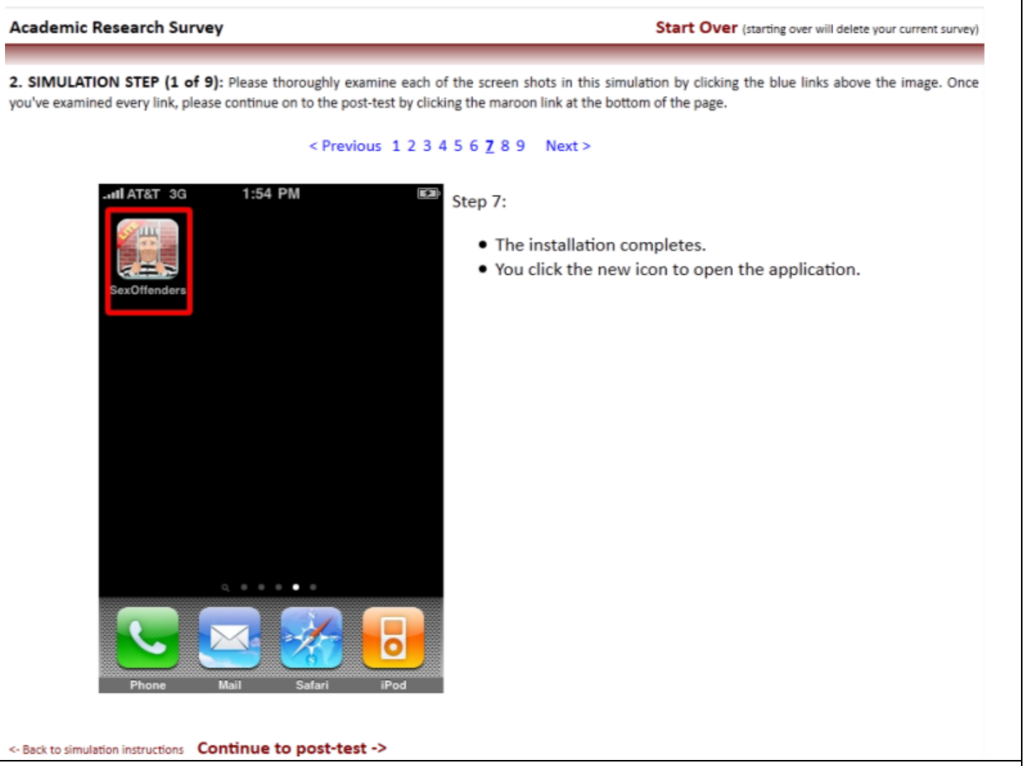
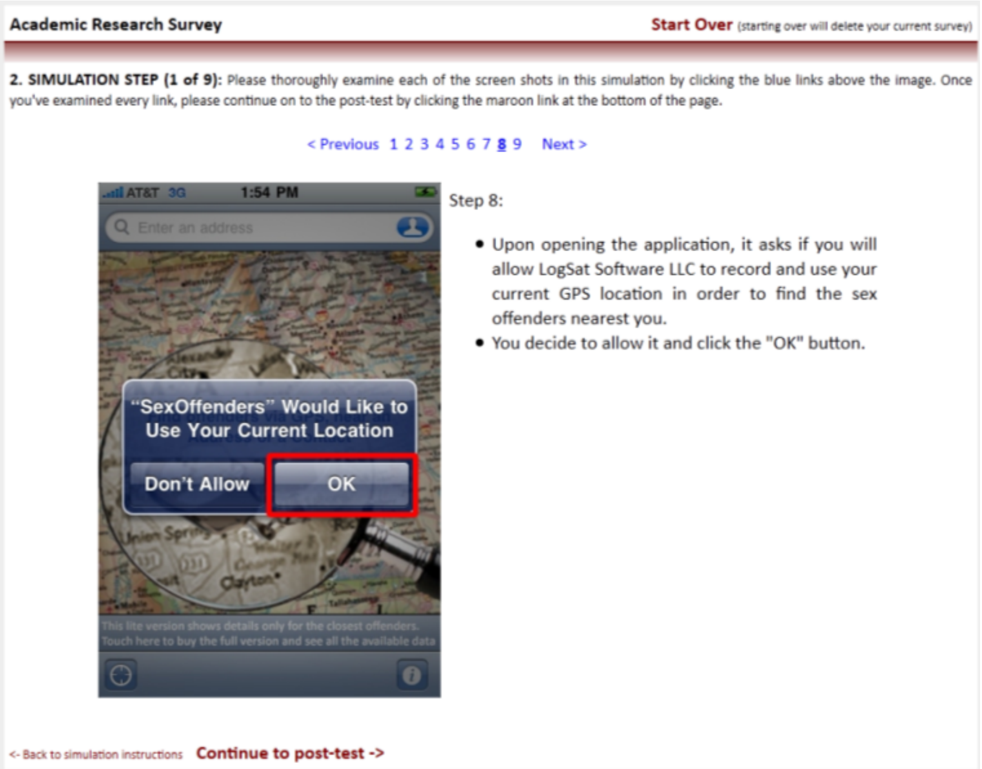
Documentation on Scenarios

Page 4	 Academic Research Survey Start Over (starting over will delete your current survey) **2. SIMULATION STEP (1 of 9):** Please thoroughly examine each of the screen shots in this simulation by clicking the blue links above the image. Once you've examined every link, please continue on to the post-test by clicking the maroon link at the bottom of the page. < Previous 1 2 3 4 5 6 7 8 9 Next > AT&T 3G 1:52 PM sex offender ThinAir Wireless Offender Locator 1002 Ratings LogSat Software LLC Sex Offenders Search 29121 Ratings Kaulcom GmbH CIS Fingerprint Sca... 30 Ratings Public Engines, Inc. CrimeReports 2396 Ratings Life360 Sex Offender Monitor 117 Ratings Featured Categories Top 25 Search Updates Step 3: Read Carefully! • Your search returned several options. • You decide to select "Sex Offenders Search". <- Back to simulation instructions **Continue to post-test ->**
Page 5 This is the step which highlights the experimental manipulations. Notice that the simulation draws their attention to the three variables (quality rating, network size, and privacy assurance) equally.	 Academic Research Survey Start Over (starting over will delete your current survey) **2. SIMULATION STEP (1 of 9):** Please thoroughly examine each of the screen shots in this simulation by clicking the blue links above the image. Once you've examined every link, please continue on to the post-test by clicking the maroon link at the bottom of the page. < Previous 1 2 3 4 5 6 7 8 9 Next > AT&T 3G 1:53 PM Search Info Sex Offenders Search LogSat Software LLC 30630 Ratings Try It! Sex Offenders Search (SOS) helps you locate registered sex offenders and sexual predators in your neighborhood, around your children's schools, friends, parks and campgrounds. Just activate your iPhone GPS and locate registered sex offenders in the area around you. You can also search by address, zip code or even near contacts in your address book. PRIVACY GUARANTEE: Although LogSat Software LLC will store your location data and personal identification in order to make this application as useful as possible, it will never share or sell this information. BBB ACCREDITED BUSINESS VeriSign Secured Featured Categories Top 25 Search Updates Step 4: Read Carefully!! This is the most important screen!! • After clicking on the application, you get a more detailed description. • Ask yourself the following questions and make a mental note of the answers: ○ What quality rating has this app received (number of stars out of 5)? ○ How many people have used and rated this app (very many [e.g. more than 100]? or very few [e.g. less than 100]?)? ○ Are there any privacy icons or seals in the description? ○ Is there a written privacy promise/guarantee? ○ If so, does it explicitly promise to keep my identity separate (i.e. not store it) from my location data? • Because the application appears to meet your needs, you decide to click the "Try It!" button which will allow you to download and use the application for a 2-week trial period. After that, you can decide whether or not to purchase it.

Documentation on Scenarios

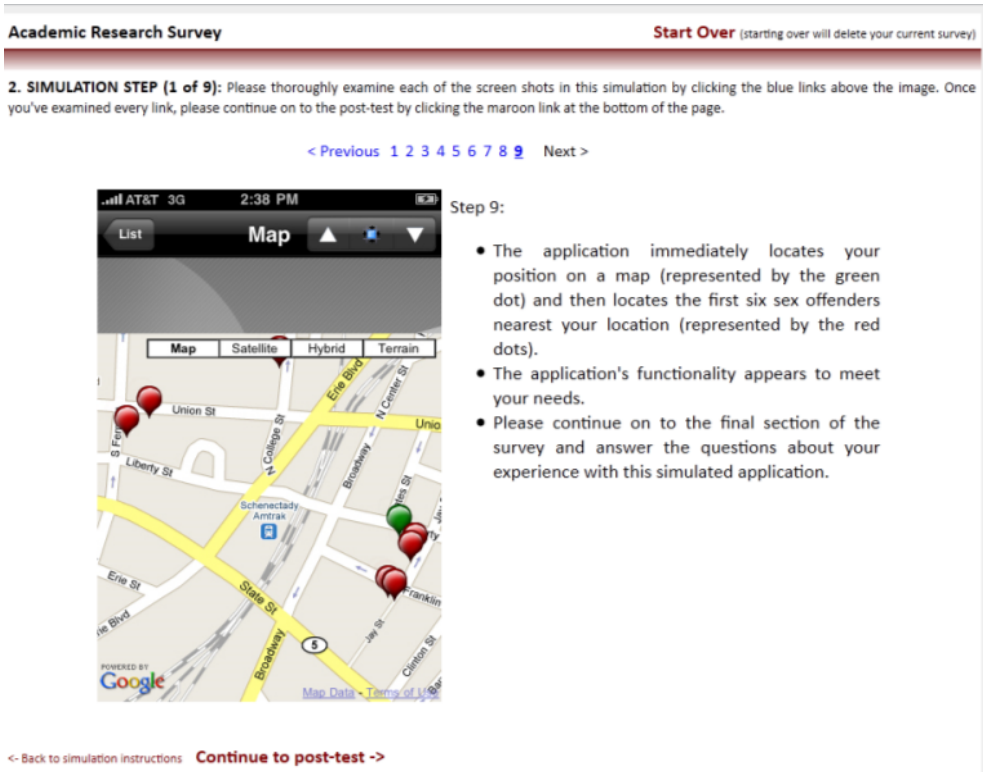
Page 6	 **Academic Research Survey** **Start Over** (starting over will delete your current survey) **2. SIMULATION STEP (1 of 9):** Please thoroughly examine each of the screen shots in this simulation by clicking the blue links above the image. Once you've examined every link, please continue on to the post-test by clicking the maroon link at the bottom of the page. < Previous 1 2 3 4 5 6 7 8 9 Next > Sex Offenders Search LogSat Software LLC 30630 Ratings INSTALL Sex Offenders Search (SOS) helps you locate registered sex offenders and sexual predators in your neighborhood, around your children's schools, friends, parks and campgrounds. Just activate your iPhone GPS and locate registered sex offenders in the area around you. You can also search by address, zip code or even near contacts in your address book. PRIVACY GUARANTEE: Although LogSat Software LLC will store your location data and personal identification in order to make this application as useful as possible, it will never share or sell this information. BBB. ACCREDITED BUSINESS VeriSign Secured Featured Categories Top 25 Search Updates Step 5: • The "Try It!" button begins the download and then changes to an "INSTALL" button. • You click the INSTALL button to begin the installation. <- Back to simulation instructions **Continue to post-test ->**
Page 7	 **Academic Research Survey** **Start Over** (starting over will delete your current survey) **2. SIMULATION STEP (1 of 9):** Please thoroughly examine each of the screen shots in this simulation by clicking the blue links above the image. Once you've examined every link, please continue on to the post-test by clicking the maroon link at the bottom of the page. < Previous 1 2 3 4 5 6 7 8 9 Next > Step 6: • The application begins to install. • To continue, click the iPhone screen image anywhere or the "Next >" link or "7" link above. <- Back to simulation instructions **Continue to post-test ->**

Documentation on Scenarios

Page 8	 **Academic Research Survey** **Start Over** (starting over will delete your current survey) **2. SIMULATION STEP (1 of 9):** Please thoroughly examine each of the screen shots in this simulation by clicking the blue links above the image. Once you've examined every link, please continue on to the post-test by clicking the maroon link at the bottom of the page. < Previous 1 2 3 4 5 6 7 8 9 Next > AT&T 3G 1:54 PM SexOffenders Phone Mail Safari iPod Step 7: • The installation completes. • You click the new icon to open the application. <- Back to simulation instructions **Continue to post-test ->**
Page 9	 **Academic Research Survey** **Start Over** (starting over will delete your current survey) **2. SIMULATION STEP (1 of 9):** Please thoroughly examine each of the screen shots in this simulation by clicking the blue links above the image. Once you've examined every link, please continue on to the post-test by clicking the maroon link at the bottom of the page. < Previous 1 2 3 4 5 6 7 8 9 Next > AT&T 3G 1:54 PM Enter an address "SexOffenders" Would Like to Use Your Current Location Don't Allow OK This lite version shows details only for the closest offenders. Touch here to buy the full version and see all the available data Step 8: • Upon opening the application, it asks if you will allow LogSat Software LLC to record and use your current GPS location in order to find the sex offenders nearest you. • You decide to allow it and click the "OK" button. <- Back to simulation instructions **Continue to post-test ->**

Documentation on Scenarios

<table>
<tr>
<td><strong>Page 10</strong></td>
<td>



Academic Research Survey **Start Over** (starting over will delete your current survey)

2. SIMULATION STEP (1 of 9): Please thoroughly examine each of the screen shots in this simulation by clicking the blue links above the image. Once you've examined every link, please continue on to the post-test by clicking the maroon link at the bottom of the page.

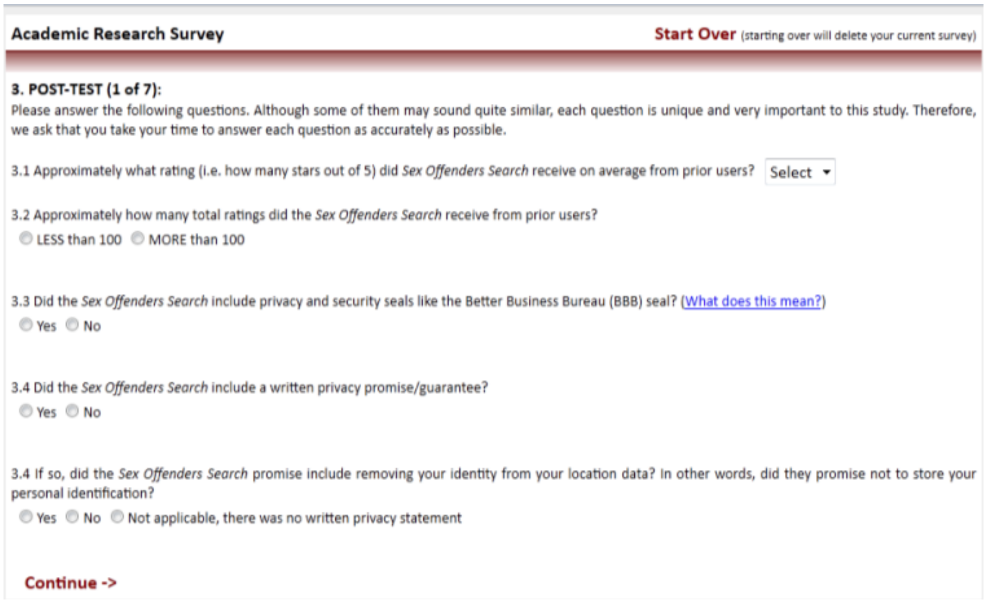
< Previous 1 2 3 4 5 6 7 8 9 Next >

Step 9:

- The application immediately locates your position on a map (represented by the green dot) and then locates the first six sex offenders nearest your location (represented by the red dots).
- The application's functionality appears to meet your needs.
- Please continue on to the final section of the survey and answer the questions about your experience with this simulated application.

<- Back to simulation instructions **Continue to post-test ->**

</td>
</tr>
<tr>
<td><strong>Page 11</strong>
Manipulation checks</td>
<td>



Academic Research Survey **Start Over** (starting over will delete your current survey)

3. POST-TEST (1 of 7):
Please answer the following questions. Although some of them may sound quite similar, each question is unique and very important to this study. Therefore, we ask that you take your time to answer each question as accurately as possible.

3.1 Approximately what rating (i.e. how many stars out of 5) did *Sex Offenders Search* receive on average from prior users? Select ▾

3.2 Approximately how many total ratings did the *Sex Offenders Search* receive from prior users?
○ LESS than 100 ○ MORE than 100

3.3 Did the *Sex Offenders Search* include privacy and security seals like the Better Business Bureau (BBB) seal? (What does this mean?)
○ Yes ○ No

3.4 Did the *Sex Offenders Search* include a written privacy promise/guarantee?
○ Yes ○ No

3.4 If so, did the *Sex Offenders Search* promise include removing your identity from your location data? In other words, did they promise not to store your personal identification?
○ Yes ○ No ○ Not applicable, there was no written privacy statement

Continue ->

</td>
</tr>
<tr>
<td><strong>Post-test</strong></td>
<td>After answering the manipulation check questions and clicking the “Continue ->” button above, the participates were administered each of the post-test questions listed in the Appendix 1</td>
</tr>
</table>

About the Authors

Dr. Mark J. Keith is an associate professor of information systems at Brigham Young University. His research interests concern information privacy and security, mobile computing, HCI, and systems development. His research has also appeared in *Information Systems Research*, *Journal of Management Information Systems*, *Journal of the Association for Information Systems*, *Decision Science*s, *Information Systems Journal*, *International Journal of Human-Computer Studies*, *Decision Support Systems*, and other leader journals and conference proceedings.

Dr. Jeffry Babb is an Associate Professor in the Computer Information and Decision Management department in the College of Business at West Texas A&M University. His research interests are in information privacy and team learning in the use of agile methods. His work has appeared in the *Information Systems Journal* and *IEEE Software*, among others. He is currently the Senior Editor for the Information Systems Education Journal.

Dr. Christopher P. Furner has served as an Assistant Professor of Management Information Systems in the College of Business at East Carolina University since August 2013. His research interests include mobile computing issues including mobile commerce, mobile app stickiness and mobile self-efficacy. Dr. Furner also studies cultural determinants of individual level information systems outcomes, such as knowledge management system effectiveness, media choice and purchase intention in an e-commerce setting.

Dr. Amjad Abdullat serves as the associate dean of undergraduate programs and professor of computer information Systems in the College of Business at West Texas A&M University. Dr. Abdullat research focus on database, strategic information systems, mobile computing and privacy issues.

Dr. Paul Benjamin Lowry is a Full Professor of Information Systems at the Faculty of Business and Economics, at the University of Hong Kong. He received his Ph.D. in Management Information Systems from the University of Arizona and an MBA from the Marriott School of Management. He has published 90+ journal articles in *MIS Quarterly, Information System Research, J. of Management Information Systems, J. of the AIS, Information Systems J., European J. of Information Systems, IJHCS, JASIST, I&M, CACM, DSS*, and many others. He is the co-editor-in-Chief of *AIS-Transactions on HCI*. He is an SE at *J. of the* AIS and *Decision Sciences*. He serves as an AE at *Information Systems J.*, *European J. of IS,* and *Information & Management.* He has also served as an ICIS, ECIS, and PACIS track chair in various security/privacy tracks. His research interests include organizational and behavioral security/privacy issues; HCI and decision sciences; e-commerce and supply chains; and scientometrics.

Transactions on Human – Computer Interaction