Int. J. Human-Computer Studies 71 (2013) 1163–1173

Contents lists available at ScienceDirect

Int. J. Human-Computer Studies

journal homepage: www.elsevier.com/locate/ijhcs

Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior ☆

Mark J. Keith [a,*], Samuel C. Thompson [b], Joanne Hale [b], Paul Benjamin Lowry [c], Chapman Greer [d]

[a] Department of Information Systems, Marriott School of Management, Brigham Young University, Provo, UT 84602, USA
[b] Management Information Systems, Culverhouse College of Commerce, University of Alabama, Tuscaloosa, AL 35487, USA
[c] Department of Information Systems, College of Business, City University of Hong Kong, P7912, Academic Building I, 83 Tat Chee Avenue, Kowloon Tong, Hong Kong, China
[d] Management and Marketing, Culverhouse College of Commerce, University of Alabama, Tuscaloosa, AL 35487, USA

ARTICLE INFO

Article history:
Received 10 October 2012
Received in revised form
10 May 2013
Accepted 28 August 2013
Available online 11 September 2013

Keywords:
Information privacy
Information disclosure
Location data
Mobile devices
Smartphone
Experimental methodology
Privacy calculus

ABSTRACT

The use of mobile applications continues to experience exponential growth. Using mobile apps typically requires the disclosure of location data, which often accompanies requests for various other forms of private information. Existing research on information privacy has implied that consumers are willing to accept privacy risks for relatively negligible benefits, and the offerings of mobile apps based on location-based services (LBS) appear to be no different. However, until now, researchers have struggled to replicate realistic privacy risks within experimental methodologies designed to manipulate independent variables. Moreover, minimal research has successfully captured actual information disclosure over mobile devices based on realistic risk perceptions. The purpose of this study is to propose and test a more realistic experimental methodology designed to replicate real perceptions of privacy risk and capture the effects of actual information disclosure decisions. As with prior research, this study employs a theoretical lens based on privacy calculus. However, we draw more detailed and valid conclusions due to our use of improved methodological rigor. We report the results of a controlled experiment involving consumers ($n=1025$) in a range of ages, levels of education, and employment experience. Based on our methodology, we find that only a weak, albeit significant, relationship exists between information disclosure intentions and actual disclosure. In addition, this relationship is heavily moderated by the consumer practice of disclosing false data. We conclude by discussing the contributions of our methodology and the possibilities for extending it for additional mobile privacy research.

1. Introduction

Mobile devices, such as smartphones, tablets, and e-readers are experiencing unprecedented rates of adoption. Since their inception less than three years ago, almost 30% of adults in the US now own a tablet computer (Rainie, 2012) and about half of American adults own smartphones (Smith, 2012). These devices create unique combinations of utility in the form of applications (a.k.a. *apps*) designed to provide entertainment, productivity tools, Internet access, and more. On the negative side, this blend of features creates exponentially greater privacy risks (Awad and Krishnan, 2006), especially in regard to location-based services (LBS) made possible by the global positioning system (GPS) that are often featured in these devices. In addition to GPS technology, mobile devices commonly have accelerometers and Bluetooth capability, which can provide real time estimates of how many people are near the mobile device. Analyzed separately, this information poses limited risks; however, the primary risk factor associated with these mobile devices is that all of this information can be integrated to precisely identify the user's real-time location.

Consider for example, the recent controversy surrounding i-Free's *Girls Around Me* app (Mikhaylova, 2012), which led to its removal from the Apple App Store™. The app generated a map displaying the locations of single females in close proximity to the user. The availability of publicly shared personal and location data through the application programming interfaces (API) of Foursquare and Facebook allowed *Girls Around Me* to collect and display the names, personal photos, and most recent location(s) of single females. The fine line between "social networking app" and "creepy stalker app" was crossed by its "Make contact!" button,

☆ This paper has been recommended for acceptance by T. Henderson.

* Corresponding author. Tel.: +1 801 361 4403; fax: +1 801 422 0573.
E-mail addresses: mark.keith@gmail.com (M.J. Keith), scthompson1@cba.ua.edu (S.C. Thompson), jhale@cba.ua.edu (J. Hale), paul.lowry.phd@gmail.com (P.B. Lowry), cgreer@cba.ua.edu (C. Greer).

1071-5819/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ijhcs.2013.08.016

which facilitated the user's personal introduction to the female through the push notification feature of the female's Foursquare app.

If examined in isolation, each element that made the *Girls Around Me* app possible—GPS technology, push notifications, APIs, Internet connectivity, public personal data—has potential for only modest risk. It is unlikely that the creators of any of these technology components visualized the risk synergies possible when combined with other components. Consequently, the privacy risk of an app like *Girls Around Me* is certainly noteworthy. If such threatening tools can be legally implemented on mobile devices, it is quite likely that many illegal and unethical tools have or will be created.

In the *Girls Around Me* case, the privacy threat would not exist if consumers did not make their personal and location data publicly available through the *Foursquare* and *Facebook* apps that allow users to "check in" by publicly registering their current location for social purposes. With consumers becoming increasingly educated regarding the privacy risks of social media and mobile apps (Jaiswal, 2010), why do so many people continue to publicly share their personal and real time location data (McCarthy, 2010), particularly since mobile devices compound these risks? In essence, this represents the *privacy paradox*, which refers to the discrepancy between a consumer's stated privacy risk beliefs and their actual behaviors (Norberg et al., 2007). Prior research has examined this question in the context of mobile apps (e.g., Keith et al., 2010; Xu et al., 2010)—primarily through the lens of *privacy calculus theory* (Dinev and Hart, 2006), which frames information disclosure as a tradeoff of benefits and risks. A core complexity in this research exists in providing methodologies appropriate to study the related phenomena. A major limitation, for example, is that the collected data traditionally only involves *intentions* to disclose personal data, not the actual disclosures of personal data (e.g., Keith et al., 2010; Xu et al., 2010)—a difficulty documented in related areas of information privacy research (Joinson et al., 2010).

Therefore, in this paper we execute a methodology and analysis approach that involves actual disclosure—particularly involving the decision to register personal information in a new mobile app and the associated privacy settings regarding location data, credit card storage, and access to Facebook data. To accomplish this, we performed a controlled experiment involving a range of mobile device users ($n=1025$, age = 19–70) using mobile device software. We find that a *privacy paradox* (Acquisti and Grossklags, 2005) exists, in that information disclosure intentions poorly explain actual information disclosure even though it is a statistically significant indicator. In addition, we find that examining actual information disclosure, without understanding the honesty and accuracy of the information provided, may also lead to a misinterpretation of results.

Before introducing our methodology, we explain our chosen information privacy and disclosure context, with the key concepts that we measure. We also briefly note the theoretical basis for the research model that we investigate. We then explain our methodology, data collection approach, and a review of the results. Lastly, we discuss our results in terms of their contributions toward privacy research methodologies, along with the limitations and future research possibilities from our study.

2. Background on privacy context and theory used

2.1. Conceptualizing information privacy and disclosure

In general, information privacy refers to an individual's control over the release of information about themselves (Belanger and Crossler, 2011; Bélanger et al., 2002) including its collection, unauthorized use, improper access, and errors (Smith et al., 1996). Smith et al. (2011) dichotomized the information privacy conceptualizations into those that view it as (1) a desired *state* (Westin, 1967), in which people can vary along a continuum of anonymity versus intimacy with the goal of obtaining anonymity; and (2) those that view it as a *control* (Margulis, 1977), which refers to the limiting of vulnerability during information transactions. Additionally, because information privacy has implications for human well-being in addition to financial security, it can be conceptualized both as a personal *right* (Warren and Brandeis, 1890), making it subject to law enforcement, and as a *commodity* (Davies, 1997), which can be traded and marketed. This latter view has increased in popularity (Jentzsch et al., 2012; Smith et al., 2011) and is the underlying assumption in many studies and theories (e.g., Culnan and Armstrong, 1999; Dinev and Hart, 2006; Laufer and Wolfe, 1977). If information privacy is a commodity, then an individual's decision to disclose versus retain information privacy can be framed as a rational choice (Becker and Murphy, 1988) made by weighing the costs and benefits of disclosure. As a result, the decision to disclose personal information should vary along a linear relationship where changes in the probability and severity of risks should lead to relative changes in an individual's disclosure of personal information (Peter and Tarpey, 1975).

Conversely, the proposed privacy paradox implies that consumers do not always act rationally regarding to their information disclosure (Acquisti and Grossklags, 2003). In particular, individuals who claim to perceive high amounts of privacy risk and low intention to disclose information still demonstrate relatively higher levels of actual information disclosure (Acquisti and Gross, 2006; Acquisti and Grossklags, 2004; Norberg et al., 2007). However, some researchers argue that the privacy paradox phenomenon is representational of a simple misunderstanding of consumers' preference functions, which are based on their *perceptions* of the cost/benefit tradeoff and not the actual value (McCarthy, 2002). Currently, the privacy paradox cannot be confirmed or denied, because only a limited amount of research has collected information disclosure data to examine this phenomenon (e.g., Acquisti and Grossklags, 2005). This research is further obfuscated by technologies that allow users to reap benefits while disclosing fake, worthless information (Acquisti and Grossklags, 2005). In this case, if measurements do not distinguish between consumers' intentions to disclose *any* information versus *accurate* information, researchers may mistakenly identify the privacy paradox phenomenon in their studies.

In summary, it remains to be seen (1) whether, and to what degree, information disclosure intentions determine actual disclosure; and (2) how the practice of false information disclosure influences this relationship. Our methodology is designed to shed light on these questions.

2.2. Location data disclosure through mobile applications

The concentrated privacy risks associated with smartphones present an interesting framework to study information disclosure decisions due to the unique and emerging nature of the risks. Researchers have yet to understand whether the existing research findings on privacy risk will persist when combined with real-time location data that presents a wide range of threats from simple annoyance to outright personal danger (Junglas and Watson, 2008).

Although several researchers have identified the unique complexities of location data privacy risks (e.g., Barkhuus, 2004; Decker, 2008; Ghosh and Swaminatha, 2001; Jiang and Yao, 2006; Junglas and Watson, 2008; Milne and Rohm, 2003; Rao and Minakakis, 2003; Vihavainen et al., 2009), far fewer studies have empirically examined information disclosure over LBS-based smartphones. Even fewer have manipulated theoretically relevant variables using experiments in order to establish causalities (e.g., Keith et al., 2010; Xu et al., 2010). Studies of *actual* location data disclosure are also notably lacking.

Extant research suggests *general* privacy concerns may (Dinev and Hart, 2006) or may not (Xu and Gupta, 2009) affect intentions

to disclose private information. However, IT-*specific* privacy risk perceptions significantly reduce intentions to disclose information, while perceived IT-specific benefits increase disclosure intentions (Sheng et al., 2008; Xu et al., 2010).

2.3. Theory and hypotheses

Because the primary purpose of this article is methodological, this section provides a truncated discussion of our theory. Many of the empirical LBS privacy studies described above were grounded in privacy calculus (Keith et al., 2010; Xu and Gupta, 2009; Xu et al., 2010). Based on the theories of *reasoned action* (TRA) (Ajzen and Fishbein, 1980) and *planned behavior* (TPB) (Ajzen, 1991), privacy calculus is a "rational" theory that seeks to explain the attitudes, beliefs, intentions, and behaviors of IT consumers when the use of the IT includes the cost of a perceived privacy risk. The term *calculus* refers not to a specific analytical model, but to the cognitive tradeoff among situational constraints (Laufer and Wolfe, 1977)—in this case, anticipated benefits and privacy risks. Unlike TRA and TPB, privacy calculus posits that behavioral intentions and subsequent actions are not only positively affected by expected utility, but negatively affected by the anticipated costs of a potential privacy violation (Culnan and Armstrong, 1999).

Drawing from TRA and TPB, privacy calculus is rooted in *expectancy theory*, which posits that individuals act in ways that they expect will maximize positive outcomes and minimize negative ones (Vroom, 1964). As such, privacy calculus is much like the *expected utility hypothesis* (Friedman and Savage, 1952) from game theory in which individuals bet on outcomes that are a function of the probability and impact of positive or negative occurrences. Individuals are assumed to be "rational" because they make decisions based on a cost/benefit tradeoff and because they are "utility maximizing," meaning that higher benefit outcomes are preferred to lower benefit outcomes (Becker, 1978).

Fig. 1 visualizes our theoretical model based on privacy calculus. Since they have been tested in the context of LBS (Keith et al., 2010; Xu et al., 2010), we do not formally hypothesize the privacy calculus-based relationships in the present study. However, to summarize, each of the arrows in Fig. 1 represents variable relationships posited by privacy calculus theory (Dinev and Hart, 2006). Perceived privacy risks reduce disclosure intentions while perceived benefits of information disclosure increase intentions. An individual's unique level of general privacy concern will increase their context-specific perceived risk and decrease disclosure intentions.

3. Methodology

3.1. Design

To understand information disclosure decisions regarding the location data and personal information used by today's mobile applications, we created a mobile app to be evaluated and used by research participants (explained in detail later). To increase the validity of our methodology, it was necessary to create variation in the participants' perception of the level of mobile app risk. In other words, we did not want our participant sample to perceive the app to be either completely risk-free or risky, which would have caused the theoretical relationships to be mis-specified. This concern is substantial considering that prior research has found evidence that consumers are distinctly dichotomized between those who are quite concerned about privacy risks and those who are not concerned at all (Acquisti and Grossklags, 2003). As a result, a danger exists in that any sample may be skewed toward one attitude or the other. Therefore, to minimize this risk, we designed our experiment to manipulate the heuristics that consumers use to calculate privacy risk along a continuum of possibilities. In particular, we used a $3 \times 2 \times 2$ factorial experimental design for a total of 12 different treatment groups in a manner that varied the participant's perceptions of the probability, impact, and time frame of potential privacy risk violations. The treatments were risk probability (low and high), impact (low and high), and time frame (immediate, near term, and future).

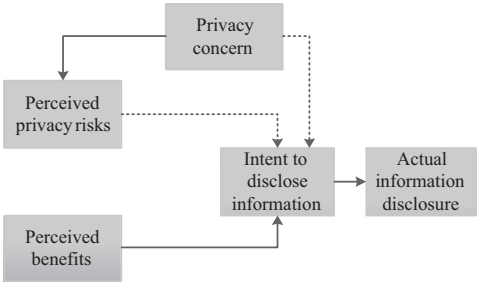

Fig. 1. Privacy calculus core theory.

3.2. Participants

Participants ($n=1025$) were drawn from college students in a large public university as well as a snowball sample including friends and relatives of those students over the age of 30 (about 40% of the sample). Institutional Review Board (IRB) approval was given to collect data and human-subject protocols were followed. We used college students and their larger social networks because they fit well with the app we designed. Snowball sampling was used to find people who had an innate interest and motivation for using apps, as opposed to the contrived or manufactured motivations typical in experimental studies. The students were offered extra credit for their participation and their recruitment of participants over 30 years old, which allowed us to get a more generalizable sample of participants. Additionally, because of the social networking nature of the experiment app, we asked participants to specifically refer friends or family members who would be interested in the type of app they were evaluating. As a control, we required that their referral live no closer than five miles from campus (to prevent roommates from participating as though they were family members over 30 years old). Because the mobile app used in the experiment gathered location data, we were able to verify that the participants referred by students retained in our sample completed the experiment no closer than five miles from campus. Thirty-two results were removed for violating this restriction. Table 1 summarizes participant demographic data.

3.3. Tool, task, and procedures

We created a realistic and in-depth experiment that allowed us to both manipulate and capture the participant perceptions of risk probability and impact while maintaining a high degree of

Table 1
Demographic statistics.

Age	31.9 $\bar{x}$ (13.5σ)	Employment	35% with 5+ years
Gender	44% male	Smartphone user	87%
Education	27% college graduates	LBS Apps	83% use 15 or more LBS apps
Ethnicity	82% Caucasian, 7% African American, 6% Asian, 2% Hispanic, 3% Other		

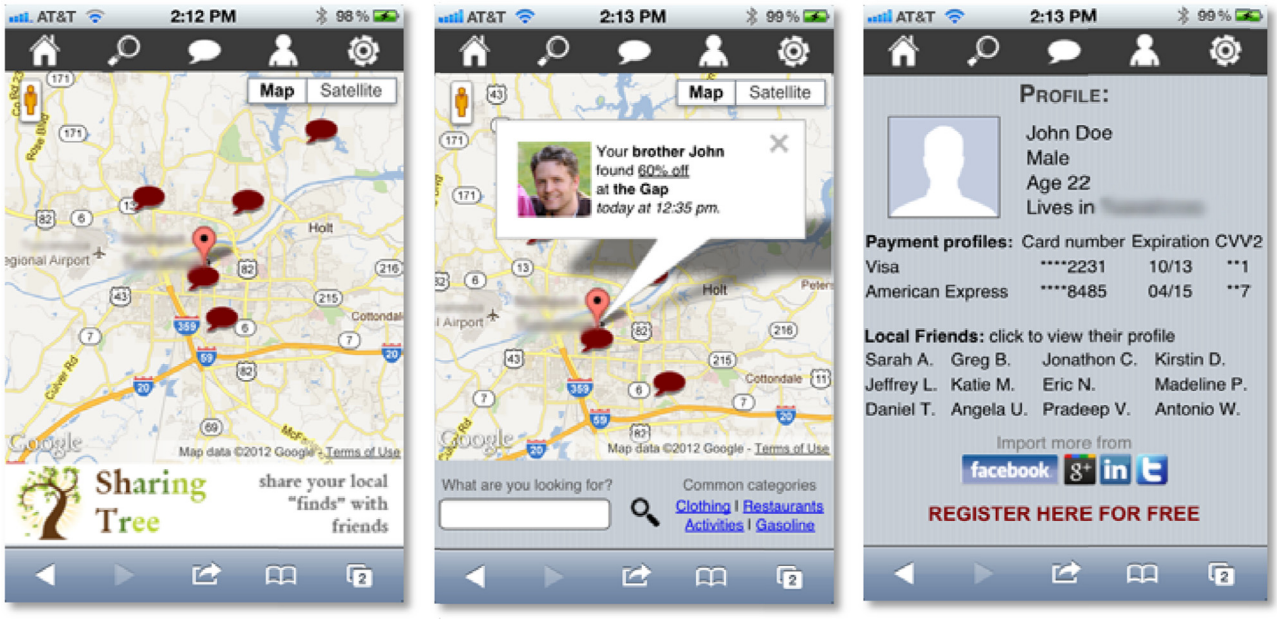

Fig. 2. Screenshots of sharing tree app.

relevance. To ensure our model was tested rigorously, and to increase likelihood of generalizable results, participants were recruited under the misleading pretense that they were needed to help analyze and test a new mobile app being readied for market. With IRB approval, participants were led to believe that "Sharing Tree" was a production app and the researchers had been hired to help perform market research and "alpha" testing prior to its release. Participants were told that in return for their participation, they would be given the opportunity to continue using the app for free after it reached the market, but they must become registered users immediately. However, their only mandatory requirement was to evaluate it in trial mode, which did not require registration. As a result, we analyzed *initial* actual information disclosure for those who registered willingly.

We created a prototype of an HTML5-based mobile application that was formatted to fit the majority of mobile device screen sizes. This app was designed to incorporate some of the major benefits and privacy risks commonly found in most LBS apps, including location-sensitivity, social networking, financial, and personal data. The stated purpose of the app was to allow users to share local shopping deals, gas prices, activities, or other interests with friends and family in the user's area. For example, if a user finds a great deal on clothing from the local Gap™ retail store, they can share that information with only their intended friends and family members before the limited stock runs out (see Fig. 2). In addition, this app (similar to paid mobile apps) would not include advertisements or sponsored locations, so that all shared data would be relevant and based on the word-of-mouth recommendations of those they care about.

Sharing Tree's LBSs allowed the user to view a map of their current location with markers of useful sites generated by friends and family members. The list of friends and family members in the user's social network could be imported automatically from Facebook. In addition to storing the user's social network, Sharing Tree also allows the user to store credit card information to pay for shopping deals available online. Furthermore, the user could store detailed profile information, which would allow the app to suggest personally relevant points of interest in the user's local area. The app included a settings screen that allowed the user to specify four *on* or *off* privacy settings: (1) use of the app's LBS, (2) location data sharing, (3) storage of credit card data, and (4) sharing the user's profile with *anyone*, *friends only*, or *nobody*. The app was designed to be partially functional—representative of a trial version before a user had registered to use it. Therefore, while the LBS were truly functional and showed the user's real time location, the "shares" and social network data provided in "trial mode" were fictional and the user could not store credit cards, friends, or personal information. To facilitate the participant's review of the app, we created an online survey and instructions to capture the user's overall perceptions of the app.

Table 2
Treatments, groups, and sample size.

	Probability	Impact	Time period
High	$n=516$ 60–70%	$n=520$ $400–$500	$n=336$ "6–12 months"
Medium	N/A	N/A	$n=357$ "1–2 weeks"
Low	$n=509$ 5–7%	$n=505$ $10-$20	$n=332$ "next few minutes"

To increase experimental control and the quality of the results, participants were led through the following five steps:

- **Step 1.** Each participant, on their smartphone, navigated to the website where the experimental instructions and survey was hosted. After reading an IRB cover letter that had been modified to deceive participants into believing they were helping an external marketing firm to pre-test an upcoming mobile app, they were given a short pretest to measure their mobile computing self-efficacy and privacy concerns.
- **Step 2.** Using a randomized, counterbalanced approach, participants were randomly assigned by the web application to one of 12 different treatments (2 levels of probability *2 levels of impact *3 levels of time period—see Table 2) so that each participant viewed an article of one particular treatment. To accomplish this, an algorithm was written to measure the current number of participants in each treatment group, sorted the groups by the count of completed surveys, and then randomly assigned the next user to one of the groups with the lowest count. This assured both random and equal

Fig. 3. Screenshots of news story on a mobile browser.

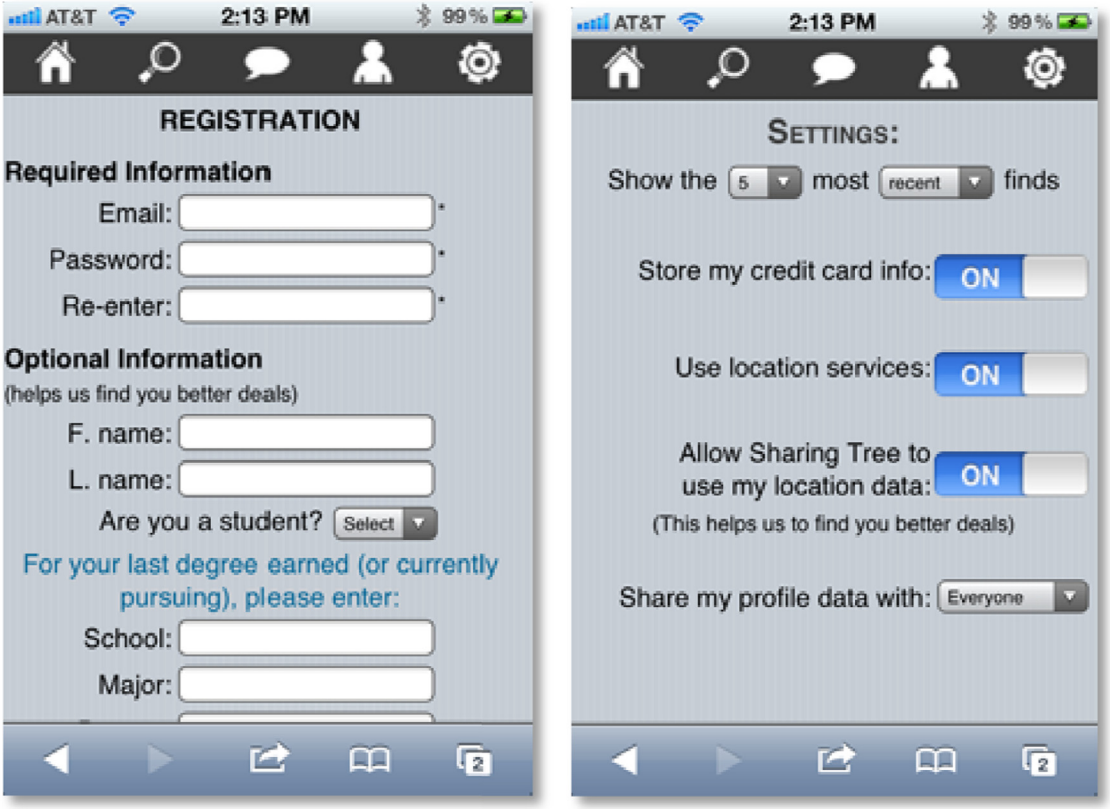

Fig. 4. Sharing tree app registration and settings screenshots.

assignment to treatments. The minor differences between treatment group sample sizes summarized in Table 2 are the result of removing incomplete or invalid data submissions.

- **Step 3.** Next, the participants were asked to read a short mockup of a news article where a "mobile privacy expert" was interviewed about the *probability*, *impact*, and *time frame* of privacy breaches over smartphones. In this step, we manipulated these variables in the article depending on the participant's group assignment. The source of the news story was also manipulated to reduce any credibility bias (Grewal et al., 1994). As a result, each participant was assigned to one of four news sources (USA Today, NetworkWorld.com, [University name] newspaper, or control [no story]), two probabilities (*low* 5–7% or *high* 60–70%), two impacts (*low* $10–$20 or *high* $400–$500), and three time periods (*short* next few minutes, *medium* 1–2 weeks, or *long* 6–12 months) (see Fig. 3, which depicts one example based on the NetworkWorld treatment). All participants, including those who did not receive the news story, were

Table 3
Measurement model statistics.

Construct	$\bar{x}$	σ	1	2	3	4	5	6	7	8	9	10
1. Actual disclosure	6.2%	20.7%										
2. Privacy settings: use location services (0=no, 1=yes)	85.8%	35.0%	.048									
3. Privacy settings: store credit card (0=no, 1=yes)	58.0%	48.4%	−.070	.450								
4. Privacy settings: share profile (0=nobody, 1=friends only, 2=everyone)	1.56	.66	−.061	.368	.560							
5. Intent to disclose	3.26	1.63	.124	.170	.160	.126						
6. Perceived privacy risk: location data risk	3.90	1.48	−.085	−.234	−.002	−.043	−.343					
7. Perceived privacy risk: personal information risk	4.40	1.37	−.135	−.191	−.098	−.051	−.475	.700				
8. Perceived benefit: personalization	5.09	1.15	.097	.103	−.030	−.010	.299	−.177	−.175			
9. Perceived benefit: locatability	5.06	1.17	.040	.139	−.016	.006	.259	−.173	−.138	.737		
10. Privacy concern	4.85	1.40	−.067	−.077	.023	−.057	−.153	.326	.297	−.047	−.049	
11. Privacy risk awareness	4.18	1.57	−.046	−.113	−.007	.013	−.122	.329	.294	−.060	−.060	.291

Notes: All measures based on Likert-type scales where 1=Strongly disagree and 7=Strongly agree.

Table 4
Summary of path coefficients and relationship significance results for Fig. 7.

Relationship	β	*t*	Significant
Privacy risk awareness→perceived privacy risks	.26	8.52	Yes
Privacy concern→perceived privacy risks	.26	7.50	Yes
Privacy concern→actual registration information disclosed	−.03	1.34	No
Privacy concern→privacy settings	−.02	1.04	Yes
Perceived privacy risks→actual registration information disclosed	−.04	1.69	Yes
Perceived privacy risks→privacy settings	−.22	5.83	Yes
Perceived benefits→actual registration information disclosed	.00	.04	No
Perceived benefits→privacy settings	.12	2.61	Yes
Honesty/accuracy of information disclosed→actual registration information disclosed	.66	23.71	Yes
Employment→actual registration information disclosed	.03	1.53	Marginally
Employment→privacy settings	−.01	.35	No

then asked to answer survey items indicating their *perceived* probability, impact, and time frame of mobile app privacy risks in general. These measures were used as manipulation checks. Consequently, the control group (no story) did not have significantly different risk perceptions than the three groups which read a news article—indicating a minimal priming effect. However, as indicated later, the probability, impact, and time period manipulations did create significant differences in risk perceptions and a normal distribution across the participant sample.

- **Step 4.** Next, the participants were given a link to the app (see Fig. 2) and asked to follow a set of review instructions, which included (see Fig. 4) the following tasks:
  (a) view each screen of the Sharing Tree app and test out all functionality,
  (b) visit the registration screen and decide what information to disclose and
  (c) visit the settings screen and adjust privacy settings to individual preferences.
- **Step 5.** After viewing each of the app's screens, participants were given a post-test survey that included all remaining measures. Importantly, the participants were asked at this point to specify which of the data they provided, if any, were accurate and honest. They were not asked to provide real data if they had previously disclosed false data. Moreover, participants were assured that their extra credit had already been earned in full, and could not be taken away, even if all of the information provided was false (per IRB regulations). Therefore, although participants could easily lie about the accuracy of their disclosed data, they would have little incentive to do so.

3.4. Measures

Prior survey items were used to measure the privacy calculus related variables of general concern for privacy (Malhotra et al., 2004), perceived benefits (Xu et al., 2010), perceived privacy risks (Keith et al., 2010), intent to disclose (Xu et al., 2010), and awareness of privacy risks (Xu et al., 2010) with minor modifications. Perceived privacy risks were expanded for this study to include both privacy risks to location data (three items) as well as risks to personal information (three items). Similarly, items measuring perceived benefits were modeled to include both personalization- and locatability-based benefits (Xu et al., 2010). As a result, perceived privacy risks and perceived benefits were each modeled as second order formative constructs with first order reflective sub-constructs, similar to research on trust with mobile commerce Vance et al., 2008). Table 3 summarizes measurement model statistics for each construct. Table 4 lists each path coefficient.

Prior survey items were used to measure the control variable mobile computing self-efficacy (Keith et al., 2011). New items were created to measure perceived probability, impact, and time frame of smartphone-based privacy risks. However, these measures were only used as manipulation checks to assess the validity of the mock news story manipulation. These measures are not used in the theoretical model and, therefore, not assessed for convergent and discriminant validity along with the theoretical constructs.

Actual information disclosure was measured by capturing a true/false value representing the participant's decision to disclose each type of registration information (email address, password, first name, last name, home address, phone number, level of education, employment experience, age, gender, ethnicity, marital status, income) and actual device settings (Turn location services on/off? Store credit card data? Share personal profile with: nobody/friends only/anyone). Several control variables were measured in addition to self-efficacy, general privacy concern, and awareness of privacy risks, including whether or not the participant was a smartphone user, age, ethnicity, employment, and education background (asked separately from the Sharing Tree app registration page).

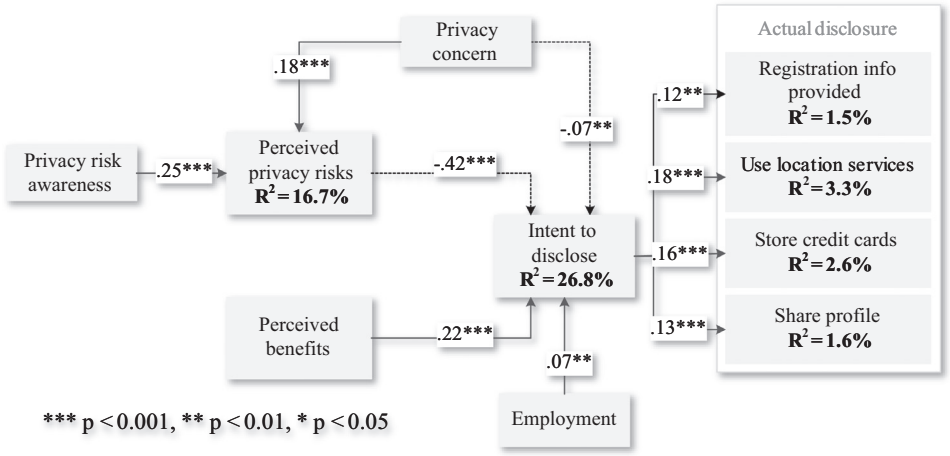

Fig. 5. PLS analysis results.

3.5. Validity manipulation checks

Several checks were either included in the system or analyzed *post-hoc* to ensure that the manipulations of the independent variables were valid and understood by the participants. First, the system did not allow participants to continue past the news story mockup unless they had spent at least two minutes on the page. If participants tried to skip the story, they were politely asked to spend more time studying the news article. Although the 2-min time requirement does not ensure that the participants actually read the article, we did confirm that they understood the most important information from it. This was accomplished by requiring participants to complete a multiple choice "quiz" that tested their recall of the security expert's statements regarding the probability, impact, and time frame of smart phone privacy breaches. Participants were allowed to review the story in order to answer all questions correctly before proceeding.

The latent construct measures for probability, impact, and time frame served as manipulation checks to verify the validity of our mock news story manipulation. These Likert-type scales ranged from 1 (strongly disagree) to 7 (strongly agree). To check for valid manipulations, we tested for statistically significant differences in the latent construct averages of these items. Using one-way ANOVAs to compare the averages between groups, we confirmed that the high probability condition was perceived as greater than the low probability condition ($\bar{x}=4.63>3.6$, one-way ANOVA, $F_{(1,\ 1023)}=126.70$, $p<.001$); the high impact condition was perceived as greater than the low impact condition ($\bar{x}=5.00>4.04$, one-way ANOVA, $F_{(1,\ 1023)}=112.98$, $p<.001$); the long time period condition was perceived as longer than the medium time period ($\bar{x}=4.04>3.31$, contrast $t_{1022}=6.23$, $p<.001$); and the medium time period was perceived as longer than the short time period condition ($\bar{x}=3.31>2.68$, contrast $t_{1022}=7.31$, $p<.001$). In summary, our manipulations are a valid technique for varying the perceived probability, impact, and time frame of privacy violation risk.

Another technical control was an app browsing history check that assured that participants visited every screen of the mobile app before they could proceed to the post-experiment survey. If participants attempted to click the "Next" button before visiting every page of the app, they were given a polite message asking that they visit the specific screens that they had not already visited. As a final control, each participant's experimental session was timed. All participants who spent less than five minutes on the entire procedure were removed from the data. The average was just over 22 min. In summary, our technical controls ensured that participants spent a reasonable amount of time in order to correctly complete each step of the experiment, including gaining an understanding of the security expert's opinion regarding the probability, impact, and time frame of risks.

4. Data analysis and results

4.1. Pre-analysis, factorial validity, and reliabilities

Pre-analysis was performed to analyze whether the measures were formative and/or reflective, test the convergent and discriminant validity of the reflective measures, test for multicollinearity, ensure reliabilities, and check for common methods bias (CMB). These analyses are extensively explained in Appendix 1. The results indicated acceptable factorial validity and minimal multicollinearity or CMB based on the standards for IS research (Gefen and Straub, 2005; Liang et al., 2007; Pavlou et al., 2007; Straub et al., 2004).

4.2. Results of hypothesis testing

We analyzed our path model using PLS SEM based on SmartPLS 2.0.M3 (Ringle et al., 2005). Despite the large sample size, we chose PLS based on our use of a mixed model of formative and reflective constructs (Chin et al., 2003; Fornell and Bookstein, 1982). All measurement items were standardized. Fig. 5 summarizes the hypothesis testing. The path coefficients (betas βs) are indicated on the paths between constructs along with the significance that was estimated using a bootstrap technique featuring 300 resamples. The explanatory power of the model is assessed through the R^2 scores (i.e., the amount of variance accounted for in the model) and the latent variable paths. Age, education, gender, ethnicity, news source, and mobile self-efficacy were not found to be significant and, therefore, not included in this diagram.

Fig. 6 depicts a revised PLS analysis model that bypasses the intention to disclose construct by analyzing the effect of perceived privacy risks and benefits directly on actual information disclosure. The purpose of this model is to discover whether the weak relationship between disclosure intentions and actual disclosure also exists between perceived privacy risks and benefits and actual disclosure. In this model, the various privacy control settings that indicate the participant's preferred level of information disclosure during the app's run time are combined into a single formative construct labeled *privacy settings*. Finally, Fig. 7 depicts the improvement in the R^2 value for the actual registration disclosure variable when the honesty and accuracy of the information disclosed is included in the model.

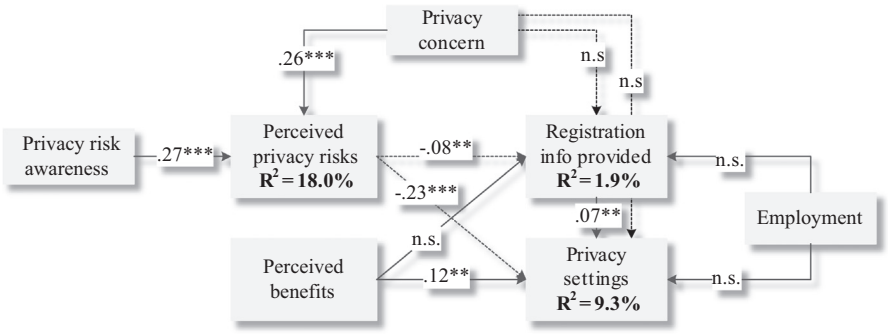

Fig. 6. PLS analysis results without intent to disclose.

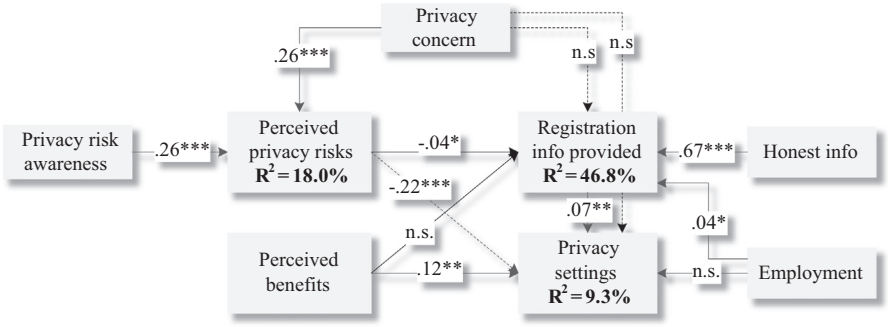

Fig. 7. PLS analysis results without intent and including honesty.

5. Discussion

5.1. Summary of results

As expected from prior privacy calculus research (Dinev and Hart, 2006; Keith et al., 2010; Xu et al., 2010), Fig. 5 demonstrates that an increase in perceived privacy risk from a new mobile app decreases an individual's intent to disclose information through the app significantly, while perceived benefits increase this intention. In contrast to prior research (Keith et al., 2010; Xu et al., 2010), our results suggest that perceived privacy risks play a larger role than perceived benefits in determining disclosure intentions, of which 26.8% were explained in our model.

Although this study exclusively examines initial information disclosure, it builds upon prior privacy calculus research by demonstrating that information disclosure intention positively influences various forms of actual information disclosure. However, it should be noted that the effect sizes (registration information provided $R^2=1.5\%$, share location data $R^2=3.3\%$, store credit card info $R^2=2.6\%$, share profile info $R^2=1.6\%$) are quite small, even compared to very conservative studies of actual IS usage (e.g., Szajna (1996)) in traditional technology acceptance literature (see review of literature in Turner et al. (2010)).

This finding suggests that a privacy paradox may exist in our context; in that disclosure intentions are a poor indicator of actual disclosure. However, the paradox suggested by prior research (Acquisti and Gross, 2006) is that consumers disclose information even when claiming they do not intend to. The descriptive data from our study indicates the opposite: consumers who did intend to disclose information actually did not. In particular, the average cumulative benefit ($\bar{x}=5.07$) exceeded the average cumulative risk ($\bar{x}=4.25$), resulting in an average disclosure intention ($\bar{x}=3.25$) just below the midpoint of "Neither agree nor disagree" with disclosing. The actual registration information disclosed averaged only 6% per participant, with only about 10% of all participants (103 total) actually registering. Concerning privacy settings, over 85% chose to disclose location data, 58% chose to store credit card information, and participants favored keeping the profile information totally unrestricted (i.e., would share with anyone regardless of whether they know the person, $\bar{x}=1.56$). Interestingly, the results were somewhat more conservative for those who actually chose to register. Although more chose to share location data ($\bar{x}=92.2\%$), fewer chose to make their profile public ($\bar{x}=1.40$), and fewer were willing to store their credit card profiles ($\bar{x}=45.6\%$). In summary, our observed paradox using mobile apps appears to contradict the prevailing notion that consumers indicate a preference for privacy but realistically engage in risky privacy behavior.

Figs. 6 and 7 provide additional insight. Perceived benefits and risks are a more efficient way of predicting the actual privacy settings decided upon, as the R^2 value of the cumulative privacy settings increased from a maximum of 3.3% (for using location services) to 9.3% overall. Similarly, when accounting for the accuracy and honesty of the registration information provided, R^2 increased dramatically from 1.9% to 46.8%. This finding helps explain the weak relationship between disclosure intentions and actual disclosure. Consumers who do not intend to disclose real information may actually disclose false information—at least in a mobile app context. In our data, about 40% of participants who registered provided a least some false information. The validity of this alternative explanation is dependent on the assumption that participants chose to disclose in the post-test survey when false information was provided.

Lastly, contrary to privacy calculus theory, a consumer's general privacy concern did not have any effect on their actual registration information disclosed. However, this finding agrees with recent literature in the mobile location data context (Keith et al., 2011; Xu et al., 2010). One explanation might be that specific risk contexts can overshadow general risk concerns. Also, in the present case, consumers had the option of restricting social network access to their profile information via their privacy settings. Thus, another explanation may be that consumers' general privacy concerns were pacified by their ability to adjust privacy settings.

Another unexpected finding was that the perceived benefits of information disclosure did not affect the level of registration

information disclosed while it did cause consumers to select riskier privacy settings. A simple explanation for this finding would be that consumers did not see any additional benefits after registering to use the app from entering optional registration information. That is, the participants were willing to register in order to find deals and activities, but were not ready to share their identities—at least initially.

5.2. Key methodological contributions

Although our experiment was not a full field study, we were able to obtain a high degree of realism while maintaining "laboratory-like" control. Our theory-driven methodological approach demonstrated several practical contributions to mobile app privacy research, such as the following:

- Conducted a novel experiment to more realistically test the privacy paradox in users' disclosure of their personal information. By creating a real app that dynamically showed shopping deals, activities, and entertainment options near their current, real-time location, the experiment moves beyond a simulation methodology, which lacks realism.
- Provided a realistic (albeit false) motivation with a trial version of an application to create a more believable setting for the users to provide feedback, which allowed for a better determination of actual disclosures.
- Leveraged snowball sampling to find people who had a natural interest and motivation for using the app, as opposed to artificial motivations typical in experimental studies. Also, allowed a more generalizable sample than merely using students. The collection of real-time location data also allowed us to minimize the risk that participants were replicating their own data or using convenience referrals rather than true smartphone users over the age of 30.
- Gathered both intentions and actual disclosure behavior. Actual disclosure was also captured in two realistic forms: (1) actual registration information provided, and (2) privacy settings chosen for use after the experiment was complete.
- Chose a realistic and understandable task involving news that was also carefully monitored to assure proper manipulations.
- Distinguished between consumers' intentions to disclose *any* information versus *accurate* information. Researchers may mistakenly identify the privacy paradox phenomenon in their studies if their experimental design does not assess the accuracy of data provided.
- Leveraged path modeling via PLS to better test the nomological network, and to accommodate both reflective and formative measures.
- Analyzed the data rigorously, including testing for convergent and discriminant validity of the reflective measures, multicollinearity, reliabilities, and common methods bias.

From these methodological contributions, our results offer practical and research implications that could not otherwise be supported from a simulation, laboratory experiment, or survey. For example, we demonstrate that the privacy paradox phenomenon is reduced when accounting for the honesty and accuracy of disclosed information. When participants claim that they do not intend to disclose information, it is quite possible that their intention is to not disclose accurate information. In this case, they could still disclose false information to gain the benefits. It is thus essential to differentiate between intentions to disclose *any* data versus *accurate* data.

Another interesting finding is that although consumer age has typically been positively correlated to online privacy concerns (Paine et al., 2007); age played no significant role in the decision to disclose personal information or location data over mobile devices. Rather, only the number of years of full-time employment was a significant indicator of disclosure intentions, but not actual disclosure.

Additionally, a *post-hoc* analysis of actual data disclosure revealed that participants were less likely to reveal their address than information about their school, work, demographics, or even birthday—indicating that consumers (at least college students) might be becoming more aware of the dangers of disclosing a reliable location. Ironically, almost all participants, including those who chose not to register, were willing to click "ok" when asked if the Sharing Tree app could collect their real-time location data. Perhaps a new form of privacy paradox is emerging in regards to location data: consumers might recognize the dangers of disclosing their home address yet do not understand the ease of determining this and other information from summaries of location data. Alternatively, the variance may be due to benefits rather than risks. Participants might have believed that revealing their location information is more likely to benefit them in a social networking context, while revealing their address would not.

Finally, our research design also has implications related to academic research on information privacy. We deceived participants, which allowed us to collect the most accurate disclosure data possible. This deception may raise justifiable concerns about the ethics of this type of research. Indeed, information privacy researchers face their own "privacy paradox" in that the only way to accurately capture human risk-taking behavior is to subject participants to risk—whether real or superficial. Traditionally, it has been difficult to collect valid data concerning perceived information privacy in experimental designs that are intended to manipulate privacy-related independent variables. This is a rather serious methodology limitation affecting research on information privacy. In our case, the risk that participants perceived was not real, however we took steps to cause participants to perceive the risk as real. The information disclosed in our experiment is not as risky as, for example, actual personal financial data. Therefore, our findings may change if the level of risk were to increase.

In summary, this study represents a step toward resolving what might be newly termed as the *privacy research paradox* by gathering human behavior data based on real risk perceptions. Our findings are, however, still limited by (1) the low level of risk involved with the information we captured, and (2) the focus on initial information disclosure rather than longitudinal disclosure.

5.3. Limitations and future research opportunities

Our research has several limitations that present useful opportunities for future research. Perhaps most importantly, the danger of not including actual behaviors (Turner et al., 2010) appears to be amplified in the information disclosure context. In particular, while our R^2 results for explaining disclosure intentions compare well to prior research (Keith et al., 2010; Xu et al., 2010), the beta coefficients measuring the impact of disclosure intentions on actual disclosure (optional information β=.12, location data sharing β=.18, credit card info storage β=.16, profile info sharing β=.13) are much smaller than those found in prior m-commerce research when analyzing the effect of mobile transaction intentions on actual use (e.g., β=.48 in Wu and Wang, 2005). In short, the relationship between disclosure intentions and actual information disclosure is much weaker than the relationship between e-commerce adoption intentions and actual usage.

We recommend some potential explanations for this finding to be explored in future research. The simplest explanation might be that participants intended to disclose *some* information, but not each of the types measured in this study. Similarly, consumers can easily turn location services on or off at any time once they

transition from trial to full usage. As a result, some participants might have intended to keep location services turned off whenever they are not needed. Based on the ability of consumers to withhold location data and/or disclose false optional information, a particularly interesting research question would be to answer why any consumer would provide real information at all if either (1) doing so is not required, or (2) the validity of the information cannot be verified. Lastly, our experimental design might have led to the weak relationship between disclosure intentions and behaviors. In particular, because the participants were being asked to review the app at a time when they were not in a real need for its services, they were less likely to register and disclose data.

Another limitation of our research, and the privacy calculus model in general, is its focus on the initial transaction level that does not account for a consumer's long term intentions or disclosure behavior. Privacy calculus might be better modeled as a sub-theory within a larger framework aiming to elucidate how long term information disclosure relationships form. For example, *social exchange theory* (Blau, 1964), which increasingly is used in socio-technical contexts (Posey et al., 2010), explains how perceived costs and benefit decisions are made as part of an exchange *relationship*—rather than as an isolated transaction. In this case, a consumer may disclose significant levels of personal information in a transaction with little initial benefit, perhaps even viewing it as a long-term investment. Future research will explore these social exchange theory based explanations through longitudinal experiments with active application use over time.

Moreover, because our sample was based on university students and their close friends and relatives over 30 years old, it is likely biased towards a more highly educated population than is representative of all smartphone users. This may explain the lack of support for a relationship between education and disclosure intention. Consequently, performing research with older and less education participants could be a useful future research endeavor.

Concerning our experimental design, it is quite possible that by asking pre-test questions regarding the participant's self-efficacy and privacy concern profile, we primed them to be overly cautious about their privacy concerns. However, they did not know they were participating in an academic research study, which should decrease such potential priming. Similarly, the news story reading manipulation, although necessary to manipulate a wide range of perceived privacy risk, might have influenced participants to be more cautious of their privacy than normal. Future experiments can evaluate this possibility by either moving the pre-test questions to post-experiment or capturing them in a separate data collection. A Solomon four-group design could also address this issue in a more controlled laboratory setting.

The experimental nature of the trial app usage limits the study's external validity. Participants were directed to try the app, rather than searching for it in response to a specific need. Further, the information shared and responses provided were done so in anticipation of future expected individual and social network use that was not realized. The "shares" and social network data provided by the app in "trial mode" were fictional and the user could not store credit cards, friends, or personal information.

Finally, the core of this study's theoretical model is also built upon privacy calculus theory. However, privacy calculus is grounded on the premise that decision makers are rational individuals who perceive a linear, utility-based relationship between benefits and risks (Dinev and Hart, 2006). Although our research clearly demonstrates that the mobile device disclosure decision involves a tradeoff between benefits and risks, it is possible that this relationship is non-linear in the minds of consumers, as is implied by the privacy paradox. Consequently, future research should strive to integrate relevant aspects from other behavioral economics theories that can account for the bounded rationality demonstrated by consumer information disclosure. For example, integrating aspects of *prospect theory* (Kahneman and Tversky, 1979) could provide greater insight into consumers' decision making as they exchange the risks versus benefits of disclosing personal and location data through mobile devices. Prospect theory suggests that consumers may take into consideration their current risk profile when making decisions regarding new risks; for example, consumers who believe that their most critical personal information is already stored and shared illicitly among companies may not be as concerned about disclosing more information in the future because they already occupy a "loss position" (i.e., "What do I have to lose?").

6. Conclusion

While still maintaining a high degree of experimental control and internal validity, this study demonstrates a methodology for gathering realistic perceptions concerning perceived privacy risks. More specifically, our methodology induced an environment in which participants perceived actual risk rather than hypothetical risk resulting in the collection of realistic actual information disclosure decisions. As a result, the increased realism allowed us to generate stronger practical and theoretical conclusions.

For example, this research demonstrates that only a weak, albeit significant, relationship exists between mobile device information disclosure intentions and actual information disclosure. Consequently, studies that do not account for actual disclosure may draw inaccurate conclusions and recommendations. Additionally, the conceptualization of information disclosure intention is muddied by the potential for consumers to provide inaccurate information while still reaping the benefits of the mobile app, which serves to underscore the importance of distinguishing between a consumer's intentions to provide accurate information versus any information in general.

Appendix A. Supplementary material

Supplementary data associated with this article can be found in the online version at http://dx.doi.org/10.1016/j.ijhcs.2013.08.016.

References

Acquisti, A., Gross, R., 2006. Imagined communities: awareness, information sharing, and privacy on the facebook. In: Danezis, G., Golle, P. (Eds.), Privacy Enhancing Technologies. Springer, Berlin/Heidelberg, pp. 36–58.
Acquisti, A., Grossklags, J., 2003. Losses, Gains, and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behavior. In: Proceedings of the 2nd Annual Workshop on "Economics and Information Security", UC Berkeley, Berkeley, CA.
Acquisti, A., Grossklags, J., 2004. Privacy attitudes and privacy behavior. In: Camp, L., Lewis, S. (Eds.), Economics of Information Security. Springer, US, pp. 165–178.
Acquisti, A., Grossklags, J., 2005. Privacy and rationality in individual decision making. IEEE Security and Privacy 3, 26–33.
Ajzen, I., 1991. The theory of planned behavior. Organizational Behavior and Human Decision Processes 50, 179–211.
Ajzen, I., Fishbein, M., 1980. Understanding attitudes and predicting social behavior. Prentice Hall, Englewood-Cliffs, NJ, USA.
Awad, N.F., Krishnan, M.S., 2006. The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. MIS Quarterly 30, 13–28.
Barkhuus, L., 2004. Privacy in Location-based Services: Concern vs. Coolness. In: Proceedings of the Mobile HCI 2004 Workshop: Location System Privacy and Control, Glasgow, UK.
Becker, G.S., 1978. The Economic Approach to Human Behavior. University of Chicago Press, Chicago.
Becker, G.S., Murphy, K.M., 1988. A theory of rational addiction. Journal of Political Economy 96, 675–700.
Belanger, F., Crossler, R.E., 2011. Privacy in the digital age: a review of information privacy research in information systems. MIS Quarterly 35, 1017–1041.

Bélanger, F., Hiller, J.S., Smith, W.J., 2002. Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. Journal of Strategic Information Systems 11, 245–270.
Blau, P.M., 1964. Exchange and Power in Social Life. Wiley, New York.
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, 189–217.
Culnan, M.J., Armstrong, P.K., 1999. Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. Organization Science 10, 104–115.
Davies, S., 1997. Re-engineering the right to privacy: how privacy has been transformed from a right to a commodity. In: Agre, P., Rotenberg, M. (Eds.), Technology and Privacy: The New Landscape. MIT Press.
Decker, M., 2008. Location Privacy—An Overview. In: Proceedings of the 7th International Conference on Mobile Business, ICMB '08, pp. 221–230.
Dinev, T., Hart, P., 2006. An extended privacy calculus model for e-commerce transactions. Information Systems Research 17, 61–80.
Fornell, C., Bookstein, F.L., 1982. Two structural equation models: Lisrel and PLS applied to consumer exit-voice theory. Journal of Marketing Research 19, 440–452.
Friedman, M., Savage, L.J., 1952. The expected-utility hypothesis and the measurability of utility. Journal of Political Economy 60, 463–474.
Gefen, D., Straub, D.W., 2005. A practical guide to factorial validity using pls-graph: tutorial and annotated example. Communications of the AIS 16, 91–109.
Ghosh, A.K., Swaminatha, T.M., 2001. Software security and privacy risks in mobile e-commerce. Communications of the ACM 44, 51–57.
Grewal, D., Gotlieb, J., Marmorstein, H., 1994. The moderating effects of message framing and source credibility on the price-perceived risk relationship. Journal of Consumer Research 21, 145–153.
Jaiswal, J., 2010. Location-aware Mobile Applications, Privacy Concerns and Best Practices, ⟨http://www.truste.com/resources/#/Whitepapers⟩. pp. 9.
Jentzsch, N., Preibusch, S., Harasser, A., 2012. Study on Monetising Privacy: An Economic Model for Pricing Personal Information. European Network and Information Security Agency (ENISA), Published, pp. 1–76.
Jiang, B., Yao, X., 2006. Location-based services and GIS in perspective. Computers, Environment and Urban Systems 30, 712–725.
Joinson, A.N., Reips, U.D., Buchanan, T., Schofield, C.B.P., 2010. Privacy, trust, and self-disclosure online. Human–Computer Interaction 25, 1–24.
Junglas, I., Watson, R., 2008. Location-based services. Communications of the ACM 51, 65–69.
Kahneman, D., Tversky, A., 1979. Prospect theory: an analysis of decision under risk. Econometrica 47, 263–291.
Keith, M.J., Babb, J.S., Furner, C.P., Abdullat, A., 2010. Privacy Assurance and Network Effects in the Adoption of Location-based Services: An Iphone Experiment In: Proceedings of the International Conference on Information Systems (ICIS '10), St. Louis, MI, pp. 237.
Keith, M.J., Babb, J.S., Furner, C.P., Abdullat, A., 2011. The Role of Mobile Self-efficacy in the Adoption of Location-Based Applications: An Iphone Experiment. In: Proceedings of the Hawaii International Conference on System Sciences (HICSS '11), Kauai, HI.
Laufer, R.S., Wolfe, M., 1977. Privacy as a concept and a social issue: a multidimensional developmental theory. Journal of Social (33), 22–42.
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, 59–87.
Malhotra, N.K., Kim, S.S., Agarwal, J., 2004. Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. Information Systems Research 15, 336–355.
Margulis, S.T., 1977. Conceptions of privacy: current status and next steps. Journal of Social (33), 5–21.
McCarthy, B., 2002. New economics of sociological criminology. Annual Review of Sociology 28, 417–442.
McCarthy, C., 2010. Who Will be Facebook's Next 500 Million?, July 21, 2010. ⟨http://news.cnet.com/8301-13577_3-20011158-36.html⟩ (accessed 09.05.13).
Mikhaylova, L., 2012. Girls Around me as a Mirror of Social Networking, April 5, 2012. ⟨http://www.examiner.com/article/girls-around-me-as-a-mirror-of-social-networking⟩ (accessed 09.05.13).
Milne, G.R., Rohm, A.J., 2003. The 411 on mobile privacy. Marketing Management 12, 40–45.
Norberg, P.A., Horne, D.R., Horne, D.A., 2007. The privacy paradox: personal information disclosure intentions versus behaviors. The Journal of Consumer Affairs 41, 100–126.
Paine, C., Reips, U.D., Stieger, S., Joinson, A., Buchanan, T., 2007. Internet users' perceptions of 'privacy concerns' and 'privacy actions'. International Journal of Human–Computer Studies 65, 526–536.
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, 105–136.
Peter, J.P., Tarpey Sr., L.X., 1975. A comparative analysis of three consumer decision strategies. Journal of Consumer Research 2, 29–37.
Posey, C., Lowry, P.B., Roberts, T.L., Ellis, S., 2010. The culture-influenced 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, 181–195.
Rainie, L., 2012. Tablet and e-Book Reader Ownership Nearly Double Over the Holiday Gift-giving Period, Pew Internet. Pew Research Center.
Rao, B., Minakakis, L., 2003. Evolution of mobile location-based services. Communications of the ACM 46, 61–65.
Ringle, C.M., Wende, S., Will, S., 2005. Smartpls 2.0 (m3) beta, Hamburg, Germany.
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, 344–376.
Smith, A., 2012. Nearly half of American adults are smartphone owners, Pew Internet. Pew Research Center.
Smith, H.J., Dinev, T., Xu, H., 2011. Information privacy research: an interdisciplinary review. MIS Quarterly 35, 989–1015.
Smith, H.J., Milberg, S.J., Burke, S.J., 1996. Information privacy: measuring individual's concerns about organizational practices. MIS Quarterly 20, 167–196.
Straub, D.W., Boudreau, M.C., Gefen, D., 2004. Validation guidelines for IS positivist research. Communications of the AIS 13, 380–427.
Szajna, B., 1996. Empirical evaluation of the revised technology acceptance model. Management Science 42, 85–92.
Turner, M., Kitchenham, B., Brereton, P., Charters, S., Budgen, D., 2010. Does the technology acceptance model predict actual use? A systematic literature review. Information and Software Technology 52, 463–479.
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, 73–100.
Vihavainen, S., Oulasvirta, A., Sarvas, R., 2009. "I can't lie anymore!": The Implications of Location Automation for Mobile Social Applications. In: Proceedings of the Sixth International MobiQuitous Conference, Toronto, ON, July 13–16. pp. 1–10.
Vroom, V.H., 1964. Work and Motivation. Wiley, New York.
Warren, S.V., Brandeis, L.D., 1890. The right to privacy. Harvard Law Review 4, 193–220.
Westin, A.F., 1967. Privacy and Freedom. Atheneum, New York.
Wu, J.H., Wang, S.C., 2005. What drives mobile commerce?: an empirical evaluation of the revised technology acceptance model. Information and Management 42, 719–729.
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, 137–149.
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, 135–174.