EXAMINING THE RATIONALITY OF INFORMATION DISCLOSURE THROUGH MOBILE DEVICES

Completed Research Paper

Mark J. Keith
Marriott School of Management
Brigham Young University
Provo, UT 84604
mark_keith@byu.edu

Samuel C. Thompson
Culverhouse College of Commerce
University of Alabama
Tuscaloosa, AL 35487
scthompson1@crimson.ua.edu

Joanne E. Hale
Culverhouse College of Commerce
University of Alabama
Tuscaloosa, AL 35487
jhale@cba.ua.edu

Chapman Greer
Culverhouse College of Commerce
University of Alabama
Tuscaloosa, AL 35487
cgreer@cba.ua.edu

Abstract

Mobile applications continue to experience explosive growth. Using mobile apps often requires disclosing location data—often along with various other forms of private information. Existing research has implied that consumers are willing to accept privacy risks for relatively smaller benefits and the mobile app context appears to be no different. In other words, consumers do not demonstrate perfect rationality regarding their valuation of risks and benefits regarding mobile app information disclosure. This study employs a theoretical lens based on privacy calculus, but integrated with prospect theory and intertemporal choice to explain how and why this "bounded" rationality occurs in information disclosure decisions through mobile apps. It reports the results of a controlled experiment involving consumers (n=1025) in a range of ages, education, and employment experience based on actual information disclosure. We find that consumers undervalue the probability of risks and have difficulty separating their existing risk exposure from potential new threats.

Keywords: Information privacy, mobile computing, location data, location-based services, privacy calculus, prospect theory, intertemporal choice
Introduction

Mobile devices such as smartphones (iPhone, Android, Blackberry), tablets (iPad, Samsung Galaxy), and e-readers (Kindle, Nook) are enjoying unprecedented rates of adoption. Almost 30 percent of adults in the US now own a tablet (Rainie 2012) since their inception less than three years ago and about half of American adults own smartphones (Smith 2012). These devices create unique combinations of utility in the form of apps providing 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 given the location-based services (LBS) made possible by the device’s global positioning system (GPS). In addition to GPS technology, mobile devices commonly have accelerometers and Bluetooth capability, which provide real-time location information and an estimate 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 device’s user and their location in real time.

Consider, for example, the recent controversy—and subsequent removal from the Apple App Store™—surrounding i-Free’s Girls Around Me app (Mikhaylova 2012). 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, Girls Around Me collected and displayed the girls’ names, personal photos, and most recent location(s). The fine line between “social networking app” and “creepy stalker app” was drawn by its “make contact!” button 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 feature which made the Girls Around Me app possible—GPS technology, push notifications, APIs, Internet connectivity, public personal data—poses only modest risk or none at all. It is unlikely that the creators of any of these technology components had this risk of synthesis in mind. However, the privacy risk of an app like Girls Around Me is certainly non-trivial. If such threatening tools can be legally implemented on mobile devices, it is quite likely that many illegal and less ethical tools have been created and more will follow.

In the above 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 which allow users to “check in;” publicly register their current location for social purposes. With consumers becoming increasingly educated about 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 actual behaviors (Norberg et al. 2007). Prior research has recently begun to examine this question in the mobile app context (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.

The core of this study’s theoretical model is also based on privacy calculus theory. However, privacy calculus is grounded on the premise that decision makers are rational and perceive a linear, utility-based relationship between benefits and risks (Dinev and Hart 2006). We posit that although the mobile device disclosure decision does involve a tradeoff between benefits and risks, this relationship is non-linear in the minds of consumers, as implied by the privacy paradox. Therefore, we also integrate relevant aspects of prospect theory (Kahneman and Tversky 1979) and intertemporal choice (Loewenstein and Prelec 1992) which give greater insight into consumers’ decision making as they trade off the risks versus benefits of disclosing personal and location data through mobile devices.

This study presents the results of a controlled experiment involving a range of mobile device users (n=1025, age=19 to 70) and actual information disclosure; in this case—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. We found that mobile app consumers strongly consider their previous privacy risk exposure (i.e. “How much of my personal information is already stored and shared unethically?”) when making decisions to engage in new forms of privacy risk. These findings indicate why consumers are willing to expose themselves to new risks even when they perceive that those risks are possibly greater than the benefits of disclosure. In addition, we find that consumers demonstrate...
“bounded rationality” (Simon 1982) regarding the immediacy of risks. In other words, risks which are anticipated to manifest themselves in the future are disproportionately discounted relative to immediate risks. Similarly, our results indicate that consumers assign the probability of a risk greater weight than the impact, or actual cost, of the risk. In other words, the real value assigned to a risk is not based on a linear (probability * impact) formula. Contrary to prior research (e.g., Sheehan 2002), perceptions were not affected by age or education. However, consumers with more full-time employment were more likely to disclose data suggesting there may be an increasing trend in the business value of location-based services.

In the remainder of the paper, we review information privacy literature—particularly concerning location data and the mobile device context. We then review privacy calculus, prospect theory, and intertemporal choice theory. Next, we explain the theoretical model tested in this study and outline the hypotheses. We then explain our methodology, data collection approach, and a review of the results. Lastly, we discuss these results including their implications for research and practice, limitations, and future research.

**Conceptualizing Information Privacy and Disclosure**

Although the field of information privacy has been studied for decades, it is a growing concern with the proliferation of information technology and it has accelerated as information becomes increasingly connected (Westin 1967). In general, information privacy refers to an individual’s control over the myriad forms 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).

In their literature review and integration, Smith et al. (2011) dichotomized the information privacy conceptualizations into those which view it as a desired state (Westin 1967), where people can vary along a continuum of anonymity versus intimacy with the goal of obtaining anonymity, and those which view it as a control (Margulis 1977) which refers to the limiting of vulnerability during information transactions. In addition, because information privacy has implications for human well-being and financial security, it can also 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 grown 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) based on 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 proportionate changes in an individual’s disclosure of personal information (Peter and Tarpey 1975).

On the other hand, the observed privacy paradox implies that consumers do not always act rationally in regards 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). In other words, the privacy paradox represents a form of irrational, or bounded-rational decision making (Acquisti and Grossklags 2004; Simon 1982). However, some researchers would argue that the privacy paradox phenomenon simply represents a misunderstanding of consumers’ preference functions which are based on their perceptions of the cost/benefit tradeoff and not actual value (McCarthy 2002). These waters are further muddied in the context of technologies that allow users to reap benefits while disclosing fake, worthless information (Acquisti and Grossklags 2005). In this case, if measurements don’t 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 understood (1) whether consumers make rational information disclosure decisions and what factors influence that decision, and (2) whether they suffer from bounded rationality and what factors consumers do not accurately calculate in their privacy/benefit tradeoff function.

**Location Data Disclosure through Mobile Applications**

The privacy risks in today’s smartphones present an interesting context to study information disclosure
because of the unique and emerging nature of the risks. We have yet to understand whether the existing research findings on privacy risk will continue to hold when combined with real time location data which presents a wide range of threats from simple annoyance (e.g., excessive location-based push notifications) to personal safety (e.g., location data in the hands of violent criminals) (Junglas and Watson 2008).

While many 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), a relatively smaller number of studies have empirically examined information disclosure over LBS-based smartphones, and still fewer have manipulated theoretically relevant variables using experiments in order to establish causalities (e.g., Keith et al. 2010; Xu et al. 2010). Also noticeably lacking are studies of actual location data disclosure whether initial or longitudinal.

Thus far, existing research has found mixed evidence that general privacy concerns affect intentions to disclose private information (Dinev and Hart 2006; Xu and Gupta 2009). However, IT-specific privacy risk perceptions do reduce intentions to disclose information, while perceived IT-specific benefits increase disclosure intentions (Sheng et al. 2008; Xu et al. 2010). In addition, several interesting antecedents of IT-specific risks and benefits have also been examined. For example, the benefits of disclosing location data are influenced by the value derived from location-based personalization (Sheng et al. 2008), monetary rewards such as coupons, bill credits, or actual money (Hann et al. 2002; Xu et al. 2010), network effects and information cascades (Keith et al. 2010), and customer reviews and quality ratings (Keith et al. 2010). On the other hand, perceived LBS risks can be reduced by industry and government regulations (Xu 2010; Xu et al. 2010) and structural assurances (Keith et al. 2010; Xu 2010; Xu et al. 2010). Lastly, individual characteristics such as locus of control (Xu 2010) and personality traits (Junglas et al. 2008) can also affect privacy concerns.

Theoretical Framework and Hypotheses

**Privacy Calculus**

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 which 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 to the 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 affected not only positively by expected utility, but also negatively affected by the anticipated costs of a potential privacy violation (Culnan and Armstrong 1999).

Figure 1 visualizes our theoretical model based on privacy calculus. Since the privacy calculus-based relationships have been tested in the LBS context (Keith et al. 2010; Xu et al. 2010), we do not formally hypothesize them in the present study.
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). In this way, 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). However, the observed privacy paradox suggests that individuals do not always act rationally regarding the real costs of privacy risks. Therefore, we discuss alternative explanations below.

**Prospect Theory**

Prospect theory was formed as an extension to the expected utility hypothesis in order to explain the routinely-observed violations of that theory (Kahneman and Tversky 1979) and has received support in a many relevant contexts (Ho et al. 2006; Smith et al. 1999; Tversky and Kahneman 1992). Prospect theory describes how individuals evaluate a set of decision alternatives based on personal heuristics, and then act or choose rationally based on the higher-valued outcome. However, the decision heuristics used to evaluate alternatives can demonstrate bounded rationality (Simon 1982) because an individual’s preferences do not follow a linear relationship where real value equals the probability * impact.

According to prospect theory, an individual’s reference point is strongly factored into their evaluation heuristics whereas in expected utility theory, individuals are indifferent to reference points (Kahneman and Tversky 1979). In particular, individuals who perceive themselves as being in a “gain” position relative to a prior reference point make risk-averse decisions whereas individuals in a “loss” position take risk-seeking behaviors. For example, Kahneman and Tversky (1979) discovered that subjects preferred a 100% chance of gaining $500 over a 50% chance of gaining $1000 when the real value of both options are equal. This was reversed in a loss scenario as individuals preferred a 50% chance of losing $1000 over a 100% chance of losing $500.

This phenomenon has interesting implications for the decision to share sensitive data over mobile devices that involve interdependent gains (in the form of utility) and losses (in the form of privacy risk). When evaluating a new mobile app, consumers are expected to take their **existing** risks and benefits into consideration. For example, if a consumer believes that their location data and personal information are already stored by unethical parties, they will perceive less new risk from adopting an app which shares common risks. This would cause the consumer to act in risk-seeking ways (i.e. by disclosing information and adopting the app) in order to achieve a balance with their prior reference point. In summary, a consumer’s frame of reference will affect their intention to disclose information such that a high level of
existing risk will increase disclosure intentions while a high level of existing benefits will decrease intentions. On the other hand, the degree to which a consumer believes that they already possess benefits of the new app will decrease their intention to adopt the app, disclose information, and reap the benefits.

\[ H1: \text{(Risk Reference)} \] Existing risks decrease the perceived risks of future disclosure and, therefore, decrease intent to disclose information through future mobile apps.

\[ H2: \text{(Benefit Reference)} \] Existing benefits decrease the perceived benefits of future disclosure and, therefore, decrease intent to disclose information through future mobile apps.

If the benefit and cost of disclosing information over a mobile device could be quantified and was equal (e.g., $10 of utility, $10 of risk), consumers would perceive a net benefit of disclosure if those values were based on a 100% chance of gaining the $10 utility and a 50% chance of losing $20 from a breach of privacy. In reality, when a potential consumer is faced with a mobile app adoption decision, it is much easier for them to gauge the probability that they will reap the mobile app benefits (e.g. through ratings, screen shots, and reviews found in the Apple App Store™ or Android Marketplace) than the probability that their disclosed data will be compromised. This would explain why even small benefits, if they are considered certain, are enough to offset potentially very large costs—if they are considered sufficiently unlikely. Therefore, we hypothesize the following:

\[ H3: \text{(Probability)} \] The perceived probability of privacy risks increases perceived privacy risk.

\[ H4: \text{(Probability Moderation)} \] The perceived probability of privacy risks increases the negative effect of perceived privacy risk on intention to disclose information.

\[ H5: \text{(Impact)} \] The perceived impact of privacy risks increases perceived privacy risk.

\[ H6: \text{(Impact Moderation)} \] The perceived impact of privacy risks increases the negative effect of perceived privacy risk on intention to disclose information.

**Intertemporal Choice**

*Intertemporal choice* (Loewenstein and Prelec 1992) is a direct extension of prospect theory based on observations of decision makers using non-linear discount rates when making choices under conditions of uncertainty with outcomes that vary by timeframe. Intertemporal choice theory posits that decision makers overweight immediate and short term prospects while underweighting longer term prospects. As with prospect theory, individual perceptions of the time discounted value are exaggerated and do not follow real values.

*Hyperbolic discounting* (Laibson 1997) is an example of intertemporal choice based on an irrational bias called “temporal myopia” (Ainslie 1975) illustrated by the sentiment “eat, drink, and be merry, for tomorrow we may die.” In other words, in the presence of uncertainty, individuals tend to excessively discount future costs and benefits versus immediate ones. This tendency has been demonstrated repeatedly in financial risk decisions (Henderson and Langford 1998; Laibson 1997) and has been suggested in the information privacy context (Acquisti 2004; Acquisti and Grossklags 2003) with preliminary evidence in the traditional e-commerce context (Acquisti and Grossklags 2005). In the present context, this phenomenon means that individuals will underweight mobile device privacy risks which are perceived to have impacts further in the future. Therefore, we hypothesize:

\[ H7: \text{(Time)} \] The perceived time distance of privacy risk affects perceived privacy risk.

\[ H8: \text{(Time Moderation)} \] The perceived time distance of privacy risk interacts with the negative effect of perceived privacy risk on intention to disclose information.

**Methodology**

**Design and Participants**

To test these hypotheses, we used a 3 x 2 x 2 factorial experimental design for a total of 12 different groups. The treatments were risk probability (low and high), impact (low and high), and time frame (immediate, near term, and future). 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). The students were offered extra credit for their participation and their recruitment of participants over 30 years old. Institutional Review Board (IRB) approval was given to collect data and standard human-subjects protocols were followed. Table 1 summarizes participant demographic data.

<table>
<thead>
<tr>
<th>Table 1. Demographic Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age 31.9 (\bar{x}(13.5 \text{ s}))</td>
</tr>
<tr>
<td>Gender 44% male</td>
</tr>
<tr>
<td>Education 27% college graduates</td>
</tr>
<tr>
<td>Ethnicity 82% Caucasian, 7% African American, 6% Asian, 2% Hispanic, 3% Other</td>
</tr>
</tbody>
</table>

**Tool, Task, and Procedures**

Rather than perform a traditional economic experiment where participants are asked to choose between two oppositely framed hypothetical scenarios (Kahneman and Tversky 1979; Tversky and Kahneman 1981), we created a realistic and in-depth experiment which allowed us to manipulate the participant perceptions of risk probability and impact while maintaining a high degree of relevance.

To test our hypotheses, 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 this app, called “Sharing Tree,” was a production app and that the researchers had been hired to help perform market research and user testing prior to its release. They were told that because of their participation, they would be given the opportunity to continue using the app for free after it reached the market, if they became registered users now. Their only mandatory requirement was to evaluate it in trial mode, which does not require registration. As a result, we are analyzing initial disclosure.

We created a prototype of an HTML5-based mobile application which 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, social network, 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 the 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 Figure 2). In addition, this app would not include annoying 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.

![Figure 2. Screenshots of Sharing Tree App](image)

The LBS of Sharing Tree allowed the user to view a map of their current location with markers of useful sites generated by friends and family members in the user’s social network (which could be automatically imported from Facebook). In addition to storing the user’s social network, Sharing Tree also allows the
user to store credit card information in order to pay for shopping deals available online. Additionally, 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 fully functional and could show the user’s current location, the “shares” and social network data it provided in “trial mode” were fictional and the user could not actually store credit cards, lists of friends, or personal information. To facilitate the participant’s review of the app, we created an online survey and instruction set to capture the user’s perceptions regarding the app. The steps included:

1. Participants navigated to the online survey and instructions on their mobile device browser
2. After reading a message explaining the purpose of the mobile app review, participants were randomly assigned to one of the 12 treatment groups and responded to a set of pre-test questions regarding their mobile device self-efficacy, general privacy concern, and perceived existing risk exposure.
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 smart phones. In this step, we manipulated these variables in the article depending on the participant’s group assignment.

![Figure 3. Screenshots of News Story on a Mobile Browser](image)

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 to 12 months) (See Figure 3). All participants (including those who did not receive the news story) were 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.

4. Next, the participants were given a link to the app (See Figure 2) and asked to follow a set of review instructions which included:
   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
   c. Visit the settings screen and adjust privacy settings to individual preferences
5. Lastly, the participants were given a post-test survey which included all remaining measures.

**Measures**

Prior survey items were used to measure mobile computing self-efficacy (Keith et al. 2011), general privacy concern (Malhotra et al. 2004), perceived benefits (Xu et al. 2010), perceived 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, perceived benefits, and perceived prior privacy risks 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).

The remaining measures were developed new in this study, although based on prior research and theoretical definitions. The items measuring prior/existing privacy risks and prior benefits were based on previous items (Keith et al. 2010; Xu et al. 2010), but modified to reflect existing risk exposure and benefits. New items were created to measure perceived probability, impact, and time frame of smartphone-based privacy risks in general.

Actual information disclosure was measured by capturing a true/false value representing the participant’s decision to disclose each type of optional registration information (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).

Validity and 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 they tried to skip the story, they were politely asked to spend more time studying the news article. In addition to stating their perceived smartphone privacy risk probability, impact, and time frame, participants had to complete a multiple choice “quiz” which tested their recall of the security expert’s statements regarding the probability, impact, and time frame of smartphone privacy breaches. All questions had to be answered correctly before proceeding, with the participants allowed to review the story multiple times. Based on one-way ANOVAs comparing the means of the perceived probability, impact, and time frame items across groups, we found that participants perceived a significant difference between the high (mean = 4.6) and low (mean = 3.6) probabilities, high (mean = 5.0) and low (mean = 4.0) impacts, and high (mean = 4.1), medium (mean = 3.3), and low (mean = 2.7) time frames. During the actual review of the Sharing Tree app, the system recorded whether each participant clicked on all five of the app’s tab links and did not allow them to proceed with the survey until they reviewed each screen.

Data Analysis and Results

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). 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).

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 formative constructs and the significant additions to existing theory (Chin et al. 2003; Fornell and Bookstein 1982). All measurement items were standardized and Chin et al.’s (2003) product-indicator approach was used for measuring the exploratory interaction effects. In the model tested, the risk-related manipulation check scores for probability, impact, and time frame were used in place of group indicators because they reflected the participants perceptions based on the treatments (c.f., Komiak and Benbasat 2006).
Figure 4 summarizes the hypothesis testing in our theoretical model. The path coefficients (betas $\beta$s) are indicated on the paths between constructs along with the significance which was estimated using a bootstrap technique with 300 resamples. The explanatory power of the model is assessed through the $R^2$ scores (i.e. the amount of variance accounted for) and the latent variable paths.

**Table 2. Measurement Model Statistics**

<table>
<thead>
<tr>
<th>Construct</th>
<th>$\bar{x}$</th>
<th>$\sigma$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Intent to disclose</td>
<td>3.3</td>
<td>1.6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Perceived privacy risk</td>
<td>4.1</td>
<td>1.4</td>
<td>-0.49</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Perceived benefits</td>
<td>5.1</td>
<td>1.2</td>
<td>0.30</td>
<td>-0.19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Existing privacy risk</td>
<td>4.1</td>
<td>1.4</td>
<td>0.05</td>
<td>0.13</td>
<td>0.06</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Existing benefits</td>
<td>4.2</td>
<td>1.6</td>
<td>-0.19</td>
<td>0.29</td>
<td>-0.25</td>
<td>0.03</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Probability of new risks</td>
<td>4.1</td>
<td>1.5</td>
<td>-0.10</td>
<td>0.38</td>
<td>0.01</td>
<td>0.20</td>
<td>0.06</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Impact of new risks</td>
<td>4.5</td>
<td>1.5</td>
<td>-0.06</td>
<td>0.31</td>
<td>0.06</td>
<td>0.13</td>
<td>0.04</td>
<td>0.44</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Time frame of new risks</td>
<td>3.3</td>
<td>1.4</td>
<td>0.09</td>
<td>0.07</td>
<td>-0.01</td>
<td>0.01</td>
<td>0.07</td>
<td>-0.03</td>
<td>-0.03</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. Privacy risk awareness</td>
<td>4.2</td>
<td>1.6</td>
<td>-0.12</td>
<td>0.33</td>
<td>-0.06</td>
<td>0.14</td>
<td>0.19</td>
<td>0.27</td>
<td>0.22</td>
<td>0.01</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10. Mobile self-efficacy</td>
<td>5.9</td>
<td>1.0</td>
<td>0.10</td>
<td>-0.07</td>
<td>0.12</td>
<td>0.13</td>
<td>0.07</td>
<td>0.00</td>
<td>0.04</td>
<td>-0.05</td>
<td>0.08</td>
<td></td>
</tr>
<tr>
<td>11. Privacy concern</td>
<td>4.8</td>
<td>1.4</td>
<td>-0.16</td>
<td>0.33</td>
<td>-0.05</td>
<td>0.34</td>
<td>0.06</td>
<td>0.32</td>
<td>0.27</td>
<td>0.00</td>
<td>0.29</td>
<td>0.01</td>
</tr>
</tbody>
</table>

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

**Discussion**

Table 3 summarizes the hypothesis results. We found strong support for the heuristics posited by prospect theory (probability and impact of risks) and intertemporal choice (time frame of risks) with significant impact on risk perceptions. In particular, an individual’s perceived privacy risk regarding the personal and location data disclosed over mobile devices is impacted foremost by the probability of risk occurrence (H3), then by the potential cost/impact of risk (H5), and lastly the length of time before the risk may be realized (H7). However, although the time frame of risks has the least effect on perceived risks, it significantly moderates the effect of risk perceptions on disclosure intentions (H8) while probability (H4) and impact (H6) do not. However, it is important to note that the direct effect of time frame on perceived privacy risks (H7) and its interaction with risks on intent to disclose (H8) are both significant in the opposite direction from hypothesized. The implications of this result are discussed later.

Interestingly, perceived existing risks did not significantly impact the perception of new risks incurred by
As expected from prior privacy calculus research (Dinev and Hart 2006; Xu et al. 2010), an increase in perceived privacy risk from a new mobile app significantly decreases an individual’s intent to disclose information through the app, while perceived benefits increase that intention. Although this study examines only initial information disclosure, it does build 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 (optional information $R^2 = 1.5\%$, 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).

The perceptions of risk heuristics measured in this study (probability, impact, and time frame) performed reasonably well in explaining perceptions of new mobile app privacy risks ($R^2 = 25.0\%$) considering that several known factors were not measured or manipulated in the scope of this study like privacy seals and statements (Keith et al. 2010; Xu et al. 2010), network effects and rating systems (Keith et al. 2010), and user interface characteristics (Vance et al. 2008). Lastly, our privacy calculus based model explained 30.3 percent of the variance in disclosure intentions.

**Implications for Research and Theory**

This research has several important implications for research and theory on information disclosure through mobile devices given its ground-breaking departures from traditional privacy calculus theory and
research. In general, our research supports the notion that the forms of information privacy relevant to mobile apps can be characterized as a commodity (Davies 1997)—to a degree. Although consumers demonstrate a certain level of economic rationality regarding the costs and benefits of information disclosure through mobile apps, we find that prospect theory and intertemporal choice provides greater insight into the departures from rationality expected by privacy calculus.

For example, after accounting for an individual’s reference point, perceived new risk plays a much larger role (β = 0.73) than perceived benefits (β = 0.19) in determining disclosure intentions while prior research (e.g., Keith et al. 2010; Xu et al. 2010) has shown that perceived benefits are the stronger predictor. This finding agrees with prospect theory that losses loom much larger than gains; although a small, but certain, gain can overshadow a large, but unlikely, loss. This finding also agrees with the observed privacy paradox in that consumers perceive great risks in disclosure, but do so even for relatively small benefits. Regarding the prospect theory concepts of reference points and loss aversion, it is interesting to note that while existing benefits clearly reduced the perceived benefits of new LBS apps, existing risk does not reduce the perceived risk of new apps. However, existing risks are important since they directly increased participants disclosure intentions (β = 0.08, p < 0.01). As a result, while it is relatively easy for consumers to quantify or operationalize benefits, it is relatively difficult to subtract existing privacy risks from the new risks of a new app. In this situation, prospect theory would predict that the consumer will choose to adopt the app and disclose information because individuals tend to overweight highly probable gain outcomes and underweight low probability loss outcomes—directly explaining why relatively higher privacy risks are so easily ignored for relatively smaller benefits. This was supported in our data in that probability (β = 0.22) was stronger than the financial impact (β = 0.13) of a loss in predicting risk perceptions—demonstrating that mobile app consumers do not use a linear value function when analyzing the risks associated with mobile app privacy risks.

In addition, intertemporal choice plays a significant role as consumers consider the time frame of risks. However, our results did not perfectly reflect the hyperbolic discounting effect. In particular, although as risks were perceived to happen later into the future led participants to increase their disclosure intentions (β = 0.13, p < 0.001), those later risks actually increased the perceived risks of new apps (β = 0.08, p < 0.01) and reinforced the negative effect of those perceived risks on disclosure intention (β = 0.20, p < 0.001). A post-hoc analysis of only those participants in the control group (i.e. those who were not manipulated with the mock up news story) also demonstrated the reinforcing interaction effect, but no significant direct effect of time frame on perceived new risks. This implies that most consumers currently don’t consider a temporal dynamic when calculating the new risks, but risks that take place further into the future can strengthen the negative effect of risks perceptions on disclosure intention. Perhaps this finding can be explained by understanding the nature of short-term versus long-term risks. In particular, recent research has demonstrated that consumers perceive a variety of risks involved with LBS (Thompson et al. 2012). Some are short-term in nature while others are long term. For example, short term risks may be associated with annoyances like spam email, push notifications, etc. whereas long term risks are more likely to be identity theft or home intrusion. In that case, the potential for long term risks like identity theft would certainly be taken more seriously than short term risks like push notifications. Another explanation for this finding may be that participants believed that the longer their information is held in the wrong hands, the more likely that it could be repeatedly shared or sold to malevolent parties.

One last explanation for the above reversed finding may simply be that our experimental design was not believable to participants. Those who received the short term risk manipulation (i.e., they read the security expert’s testimony that most privacy intrusions happen immediately when the information is disclosed) may have believed that it is impossible that privacy costs could be incurred immediately and discounted the risk altogether. Consequently, although our research supports the notion that information privacy can be considered a commodity, there are boundaries of this perspective and researchers should be wary of assuming a fully-economic perspective.

Our results imply that decisions to disclose personal and location data through mobile apps is better modeled with bounded rationality theories (e.g. prospect and intertemporal choice) than privacy calculus alone which assumes a rational, linear tradeoff between privacy risks and disclosure benefits.

**Implications for Practice**

Previous privacy risk exposure (i.e. “How much of my personal information is already stored and shared...
unethically?”) does not impact a mobile app consumer’s perception of risk exposure when evaluating a new mobile app. This finding implies that it is difficult for consumers to conceptually separate existing risk exposure from the risks of a new app, suggesting that each new app will be evaluated on its own merits. However, this study indicates mobile app consumers clearly consider their previous privacy risk exposure when making information disclosure decisions (β = 0.08, p < 0.01). Taken together, if consumers are convinced they are sufficiently exposed in general, there is no point in denying themselves the benefits of a new app—even though they can’t be sure that the new app’s risks are no different from their prior risk exposure. Perhaps this would change if more app platforms, like Android, notified consumers of each type of information collected.

In evaluating risks, the perceived probability that a consumer’s information may be stored and used unethically is weighted higher than the cost and time before such loss may occur. Thus, communications to urge information privacy protection should emphasize the real rates of data theft and remind consumers who may feel inclined to focus only on larger probabilities that the smaller probabilities from using multiple apps do accumulate; eventually luck runs out. Consumers should be aware of their tendency to underweight the real probabilities of privacy breaches and consider the real cost. Similarly, consumers should be made aware of their penchant for hyperbolic discounting and realize that a future privacy breach still has real costs.

In contrast, ethical app developers must promote the steps taken to protect against data theft and track and promote successful mitigation practices. Although our results demonstrate that consumers tend to underweight risk probabilities, they are still risk-averse in their beliefs and behaviors. As a result, if app developers implement techniques that reduce a consumer’s perceived risk probability (e.g., stating exactly which types of information are being collected), they should be able to gain market share from developers who cannot reduce the consumer’s perceived risk probability.

Fundamentally, those who care about preserving the privacy of personal information and location data, such as organizational security officers, government regulators, ethical app producers, and consumers themselves, must find ways to help users recognize their tendencies to irrationally underweight the probabilities of risk and overweight the certainties of benefits as well as having the patience to relinquish immediate benefits that come with future costs.

Contrary to prior research (e.g., Sheehan 2002), privacy risk perceptions were not affected by age or education. However, consumers with more full-time employment experience were actually more likely to disclose data (β = 0.05, p < 0.05). Since those with more full-time employment experience also tend to be older and more educated, it would seem that these consumers would actually be less likely to disclose. This finding suggests that there may be an increasing trend in the perceived business value of LBS.

Lastly, our research design also has implications for academic research on information privacy. In our study, we deceived participants in order 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 only perceived. It seems that valid data and perceived information privacy cannot both be achieved in an experimental design which is intended to establish causality. This is a rather serious limitation to research on information privacy. In our case, the risk which participants perceived was not real, but we took steps to cause participants to perceive the risk as real1. However, the information disclosed in our experiment is not as risky as, for example, 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 termed as the “privacy research paradox” in that we gathered human behavior data based on real risk perceptions. However, our findings are still limited by 1) the low level of risk involved with the information we captured, 2) the focus on initial information disclosure rather than longitudinal disclosure. Additional limitations and research opportunities are discussed next.

 Limitations and Future Research Opportunities

1 Per IRB regulations, we informed participants (post-hoc) that they had, in fact, participated in an experiment and that they had the right to have their data removed.
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-squared 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 $\beta = 0.12$, location data sharing $\beta = 0.18$, credit card info storage $\beta = 0.16$, profile info sharing $\beta = 0.13$) are much smaller than those found in prior m-commerce research when analyzing the effect of mobile transaction intentions on actual use (e.g., $\beta = 0.48$ 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 may be that participants intended to disclose some information, but not each of the types we measured. Another practice which is likely affecting our results is that of providing false information. Although the participant could not provide false location data, they could enter any personal data they would like in the optional fields. Future research would be useful in differentiating between intentions to disclose real versus false information. A particularly interesting research question along these lines 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.

Another limitation of our research and the privacy calculus model in general, is its focus on the initial transaction level which doesn’t account for a consumer’s long term intentions. Privacy calculus might be better modeled as a sub-theory within a larger framework explaining how long term information disclosure relationships form. For example, social exchange theory (Blau 1964) 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, viewing it as a long-term investment.

Concerning our experimental design, it is quite possible that by asking pre-test questions about the participant’s self-efficacy and privacy concern profile, we primed them to be overly cautious about their privacy concerns—even though they did not know they were participating in an academic research study. Similarly, the news story reading manipulation—although necessary to test our independent variables—was likely to have influenced participants to be more privacy cautious than they would normally be. Now that the above theoretical model has established causality, future experiments should forgo the pre-test questions and manipulation in order to capture more realistic information disclosure decisions.

Lastly, 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. In particular, the positive effect of full time employment on disclosure intentions may be phenomenon that exists only within a well-educated population and not within the entire population of smartphone users.

**Conclusion**

This research demonstrates that mobile app disclosure intentions and behaviors do not exhibit linear, “rational” outcomes, but are subject to the heuristics modeled by prospect theory and intertemporal choice. In particular, we find that when conceptualizing the risks of mobile app information disclosure, individuals over-emphasize and underweight the probability of risks. In addition, they are unable to fully distinguish between their existing privacy risks and those presented by a new mobile app. However, consumer perceptions of their existing risks lead them to be more likely to disclose information. This creates a very dangerous situation because it is easier for individuals to assess the immediate benefits rather than the longer-term risks they will incur from using a new app. This phenomenon, coupled with a tendency to over-discount the present value of future risks, can lead consumers to disclose personal information and location data even though the real benefits of disclosure are smaller than the costs of privacy risk. This research is a further step toward explaining the decision process and heuristics consumers use to calculate the risk/benefit tradeoff involved with information disclosure through mobile devices and applications.
References


