The effects of consumer self-regulation and risk immediacy on mobile information disclosure

Completed Research Paper

Introduction

Emerging information privacy risks and behaviors regarding mobile devices and applications have created a clear need for new research. In this context, technical innovations and practical problems are driving the research. Consider the following hypothetical scenario: you are stuck in heavy traffic in a city you are unfamiliar with. You desperately need to exit the freeway and find your way to a conference where you will be speaking. You own a data-enabled smartphone. So, you begin searching on your smartphone for an app to help guide you through the city. Research has demonstrated that the average consumer in this context might both 1) claim outwardly that they are very concerned about the privacy risks of using unknown mobile apps, but also 2) immediately download the first app they find and begin disclosing location data through it in order to satisfy their need for directions (Acquisti et al. 2004).

Although simplistic, this scenario only a portion of all consumers. Others, from either an extreme sense of privacy concern or who simply have greater patience, may choose to stay on the freeway or simply pull over and spend more time searching for the app which best balances the benefits and risks according to their risk preferences. However, research on consumer information disclosure in the mobile app does not account for consumer idiosyncrasies like differences in patience and self-control.

The purpose of this study is to extend existing theory to account for the moderating role of consumer self-regulation on information disclosure behaviors. Our theoretical model is based on a privacy calculus core which models information disclosure behavior as a tradeoff between perceived risks and benefits of the disclosure (Dinev et al. 2006). We extend privacy calculus with self-regulation theory to explain this "bounded rationality" in consumers who tend to disclose information against their "better judgment." In essence, those with greater patience and self-control are less willing to disclose information through apps immediately when first presented with the choice—thus, demonstrating greater rationality. In addition, they are less tempted to disclose information as the time frame of risks is extended further into the future.

Literature review

The body of literature on information privacy and consumer information disclosure is growing rapidly, particularly with the emergence of technologies that are combining various forms of information in a single device (Decker 2008). Smartphones and tablets are the primary source of these new forms of privacy risk. They merge "traditional" consumer information like contacts, web browsing preferences, and email with location data, music, videos, accelerometers, and social networks (Keith et al. 2010). As a result, the level of potential privacy risk has exploded.

Because of this rapid change in technology, the research is still catching up. In particular, there are very few experiments which capture actual consumer disclosure behaviors in a realistic environment with these emerging devices and apps. This is quite a problem since several authors have noted what has been termed the "privacy paradox" which means that consumers typically claim to be very concerned about privacy risks yet are completely willing to disclose their information for seemingly small benefits (Acquisti et al. 2004). However, there are several relevant studies which have begun to examine this phenomenon.

Xu et al. (2010) examines the different level of consumers' disclosure intentions when consumers are asked for information versus voluntarily giving away information. There are other relevant studies that are not directly in the mobile context, yet somewhat related. For example, Lowry et al. (2011) expanded the disclosure literature by accounting for the effects of culture in the context of instant messaging. Their model found a strong relationship between behavior intentions and reported behavior. Hoadley et al. (2010) performed a survey of Facebook users and discovered that consumers can be irrationally influenced by illusions of a loss of control in a study of Facebook users. This study sheds useful light on the potential consumer irrationality

Other studies have collected actual consumer behavior (not reported behavior) in a laboratory setting. For example, Berendt et al. (2005) identifies the difference between consumers' disclosure intentions and actual disclosure in the context of a traditional website store. They found that this intention-to-behavior relationship is very "situational" and not always as strong as theory suggests. Similarly, Norberg et al. (2007) demonstrates the divergence between consumers' privacy disclosure and actual behavior when asked to disclose specific pieces of personal information. Their study strongly validated the existence of the privacy paradox. While these important studies offer more realistic results, the data was collected in a laboratory environment where the participants were likely to perceive low risk.

Other studies have used a field setting to capture more realistic consumer behaviors. For example, Beresford (2010) captures consumers' actual choice between a secured privacy DVD shop and a discounted DVD shop with low privacy control. Consumers were not willing to pay a higher price for the shopping security. In a study perhaps most applicable to our mobile context, Keith et al. (2013) captures consumers' actual disclosure through a mobile app. They recruited participants under the false pretense that they were helping to "beta" test an upcoming mobile app and were given the "opportunity" to register to use the app for free as a reward for their help. They found that disclosure intentions were a significant predictor of actual disclosure but the effect size was quite small. In these studies, disclosure data was captured in a field experiment setting where participants were more likely to perceive real risks.

In summary, there is increasingly literature on consumer disclosure (including many studies not reviewed here for space limitations) and the methodologies are improving. However, there is still an important gap in this literature. Thus far, very few studies, and only one in the mobile app context, 1) incorporates a field setting so that participants perceive a real risk, and 2) captures actual information disclosure rather than intentions or reported disclosure only.

Theory and Hypothesis

Privacy Calculus

Most researchers have adopted a core theoretical model based on privacy calculus adapted by Dinev & Hart (2006) for the e-commerce context (visualized in Figure 1). Privacy calculus explains the effect of perceived benefit and risks that inhibits and facilitates consumer's intention to disclose personal information. In other words, privacy calculus explains the consumer's behavior based on the cumulative effect of the inhibitors and driver set. If the effect of the driver set outweighs the effect of the inhibitors set, consumer will be involved in the online transaction. However, if the effect of the inhibitor set outweighs the effect of the drivers set, consumer will avoid the transaction.

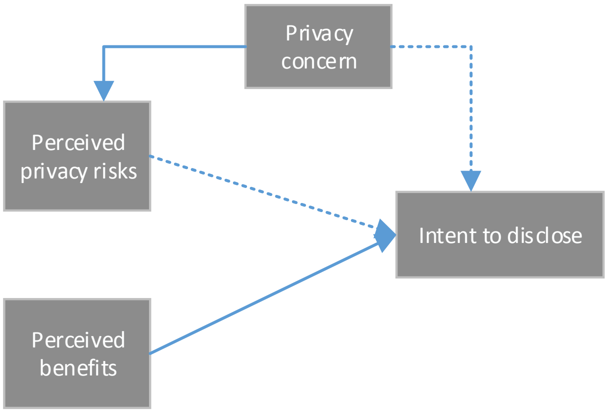


Figure 1. Privacy Calculus theory adapted from (Dinev and Hart 2006)

Privacy calculus is based on the assumption that consumers are rational decision makers. This means that they are fully capable of evaluating the true value of disclosure risks and benefits. In the mobile app market, this means that consumers will evaluate the cost and benefit of the app and then decide whether to purchase/download the app. The cost is giving up personal privacy and accepting some level of future risk associated with the disclosure. The benefit is the utility that the app creates.

While privacy calculus theory is a proven core model for information disclosure, it is unlikely to fully explain risk decisions in the mobile context by itself. For example, it is well-known that mobile app consumers are often completely unaware of exactly how much data is being gathered from them and sold to third parties (Seriot 2010). The mobile context is even more severe in this regard than traditional “desktop-based” e-commerce because of the potential loss of location data (Keith et al. 2010; Xu et al. 2010). As a result, mobile consumers cannot be rational decision makers. On the other hand, the provider is incented to hide all privacy risks. It is against their interest to help the consumer rationally evaluate risks. A more self-regulated and/or informed consumer would be more likely to recognize this fact and be patient as they search for the best app to meet their needs (Babin et al. 1995). However, existing research has not accounted for the role of consumer self-regulation in the mobile app context as it has in more traditional marketing “impulse buying” contexts (Rookh 1987).

Second, the risks of information disclosure over mobile apps do not happen at the same time as the benefits. In particular, they will manifest themselves at some point in the future (although usually completely without the consumer’s knowledge). For example, if a consumer downloads an app and registers with the app provider, they will immediately begin getting the benefits of this app. However, once they’ve allowed the app to begin collecting location data, this data is then recorded over time. As more data is collected, their level of privacy risk increases. Because it is difficult for the consumer to even know how much data is being collected, it will be even more difficult for them to judge the long term risks. As a result, it is quite possible for a consumer to miss-calculate the initial benefit/risk tradeoff. Therefore, we incorporate theory on self-regulation below.

Self-Regulation

Self–regulation is the ability to delay immediate action for spontaneous desires (Mischel et al. 1972) and includes impulse control which is the management of short-term desires (Ainslie 1975). This theory has been used extensively in the marketing literature to explain consumer impulse buying behavior (Rookh 1987). This research helps to establish why self-regulation is more relevant in the mobile context than traditional e-commerce. When using mobile devices, consumers are “in the moment” of their needs and wants making them more susceptible to emotional impulse decisions (Ainslie 1975). Self-regulation plays a major role in the evaluating process between spontaneous need and immediate actions. There are two types of self-regulation typically studied in the literature: 1) patience or “delay of gratification”, and 2) action control.

Patience is the ability to delay immediate small reward for a larger reward in the future (Mischel et al. 1972). Patience is related to the similar concepts of delayed gratification (Mischel et al. 1972), impulse control (Ainslie 1975), and willpower (Metcalfe et al. 1999). Patience is an internal characteristic that has been correlated to greater cognitive and social competence in life (Mischel et al. 1989).

Patience is relevant to our context because of the privacy risk involved in information disclosure. If there were no risk, patience would be less relevant when predicting initial information disclosure because there would be no initial cost to delay. However, mobile apps do involve risk which requires consumers to make a decision as to whether the upfront mobile app benefits are greater than future risks. A patient consumer is not as likely to reduce their perceived risk just because it manifests itself further into the future. Similarly, a patient person is less likely to artificially discount the risks because they desire instant gratification. Therefore,

> *H1: The effect of perceived risk immediacy on actual information disclosure is reduced when consumers possess greater patience*

H2: The effect of perceived risk on actual information disclosure is increased when consumers possess greater patience

Action-control is the ability to form goals prior to an action and to stay with the goal during the action process (Babin et al. 1995). Action theorist's dichotomize people as being either "action" oriented or "state" oriented" (Kuhl 1985). Action oriented people form relatively firm intentions before performing an action. They are less susceptible to competing influences which may distract them from a goal (Babin et al. 1995). On the other hand, state-oriented people are more influenced by social and emotional influences that can be either internal or external. As a result, state-oriented individuals have weakened intentions and are more susceptible to both spontaneous behavior with negative consequences as well as a delay of activities with positive outcomes. Therefore, state-oriented individuals are deemed as "low" self-regulators. Therefore:

H3: The effect of perceived risk immediacy on actual information disclosure is increased when consumers exhibit greater action-control

H4: The effect of perceived risk on actual information disclosure is decreased when consumers exhibit greater action-control

To be clear, our theoretical model is based on a core of privacy calculus theory (Dinev et al. 2006). However, we extend it with core constructs from intertemporal choice theory (Loewenstein et al. 1992) and self-regulation theory (Ainslie 1975; Mischel et al. 1972). Figure 2 visualizes our theoretical model.

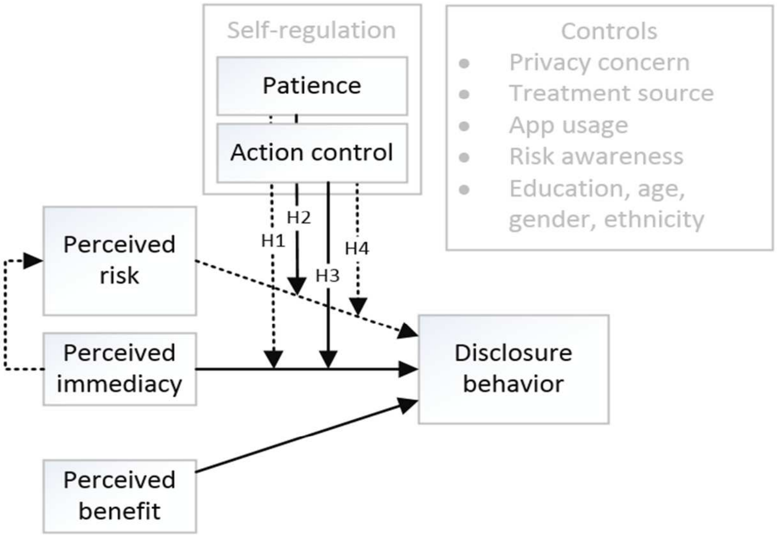


Figure 2. Theoretical Model

The core relationships in the privacy calculus model have been validated in both the e-commerce (Dinev et al. 2006) and mobile app contexts (Keith et al. 2010; Keith et al. 2013; Keith et al. 2012; Xu et al. 2010). In addition, the effect of perceived immediacy on perceived risk was examined previously (Keith et al. 2012). Therefore, we do not formally hypothesize them here. However, perceived immediacy is a relevant control variable that is likely to interact with consumer self-regulation.

Methodology

We adopted an experiment based on the methodology used by Keith et al. (2013) designed to measure valid consumer information disclosure behaviors in the mobile app context. In particular, we had participants evaluate and test a real, forthcoming mobile app in "beta" stage and then decide (1) whether to register to use the app in the future and (2) how much of their personal profile information to disclosure during the registration process.

The overall participant sample (n=441) was drawn from multiple sources (1) college students in a business school course (n=206), (2) their friends and relatives over the age of 30 (n=137), and (3) Amazon Mechanical Turk (n=100). Table 2 summarizes participant demographic data.

Apps currently used (non-system apps)	27.2 $\bar{x}$ (16.83 σ)
Age	26.6 $\bar{x}$ (5.74 σ)
Smartphone user	89.9%
Apple iPhone user	58.6% (of previous)
Gender (male / female)	58.3% / 41.7%

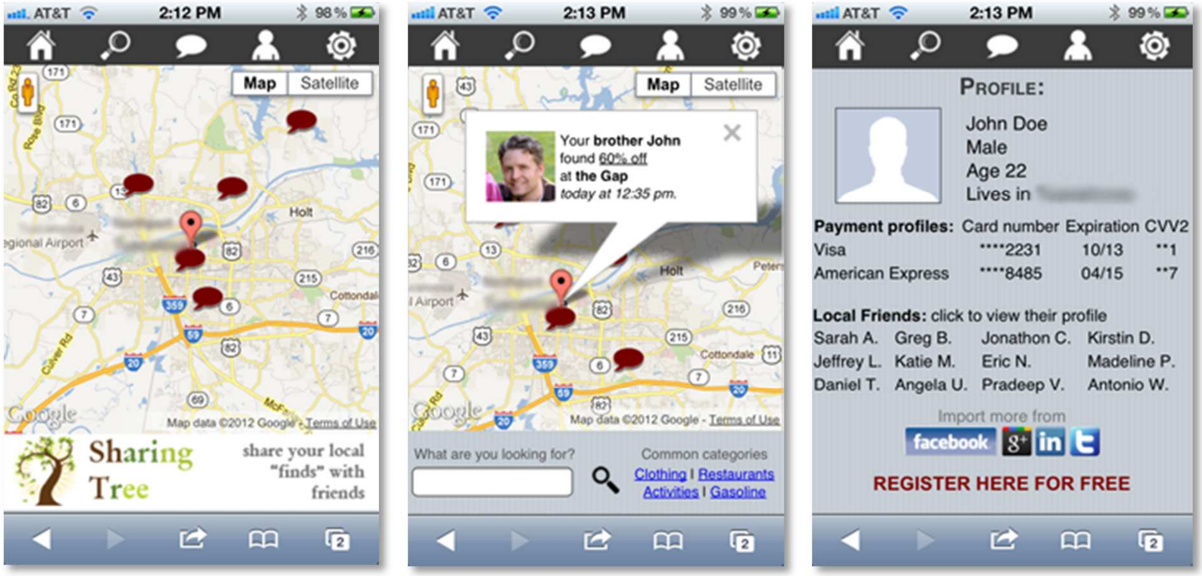
Table 2. Demographic Statistics

Tool, Task, and Procedures

Research artifact

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 deceived to believe that this app, called "Sharing Tree," was a forthcoming app in beta testing phase and that the researchers had been hired to help perform market research and consumer 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.

Sharing Tree was designed to incorporate some of the major benefits and privacy risks commonly found in most 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 consumer's area (See Figure 2). In addition, this app would not sponsored locations, so that all shared data would be based on the word-of-mouth recommendations of those they care about.



Your brother John found 60% off at the Gap today at 12:35 pm.

PROFILE:

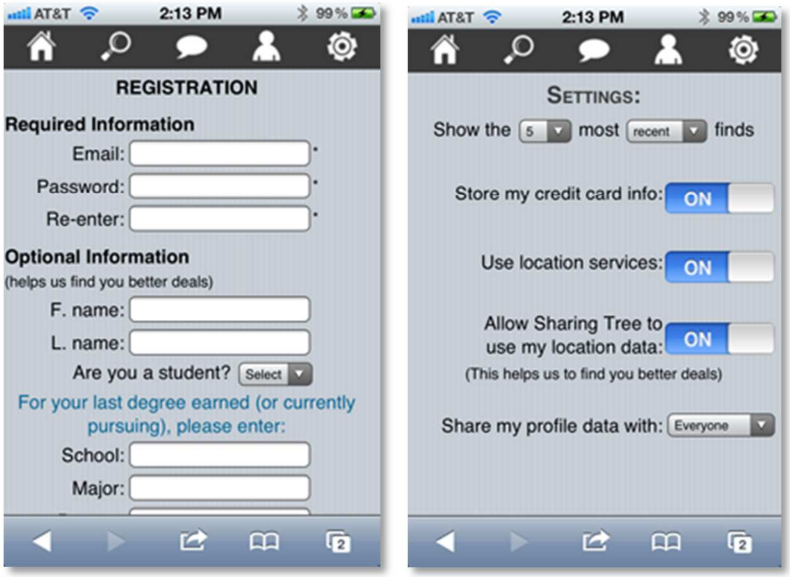
John Doe
Male
Age 22
Lives in [redacted]

Payment profiles:	Card number	Expiration	CVV2
Visa	****2231	10/13	**1
American Express	****8485	04/15	**7

Local Friends: click to view their profile

Sarah A.	Greg B.	Jonathon C.	Kirstin D.
Jeffrey L.	Katie M.	Eric N.	Madeline P.
Daniel T.	Angela U.	Pradeep V.	Antonio W.

Import more from



REGISTRATION

Required Information

Email: *

Password: *

Re-enter: *

Optional Information

(helps us find you better deals)

F. name:

L. name:

Are you a student? Select

For your last degree earned (or currently pursuing), please enter:

School:

Major:

SETTINGS:

Show the 5 most recent finds

Store my credit card info: ON

Use location services: ON

Allow Sharing Tree to use my location data: ON

(This helps us to find you better deals)

Share my profile data with: Everyone

Figure 3. Screenshots of Sharing Tree App

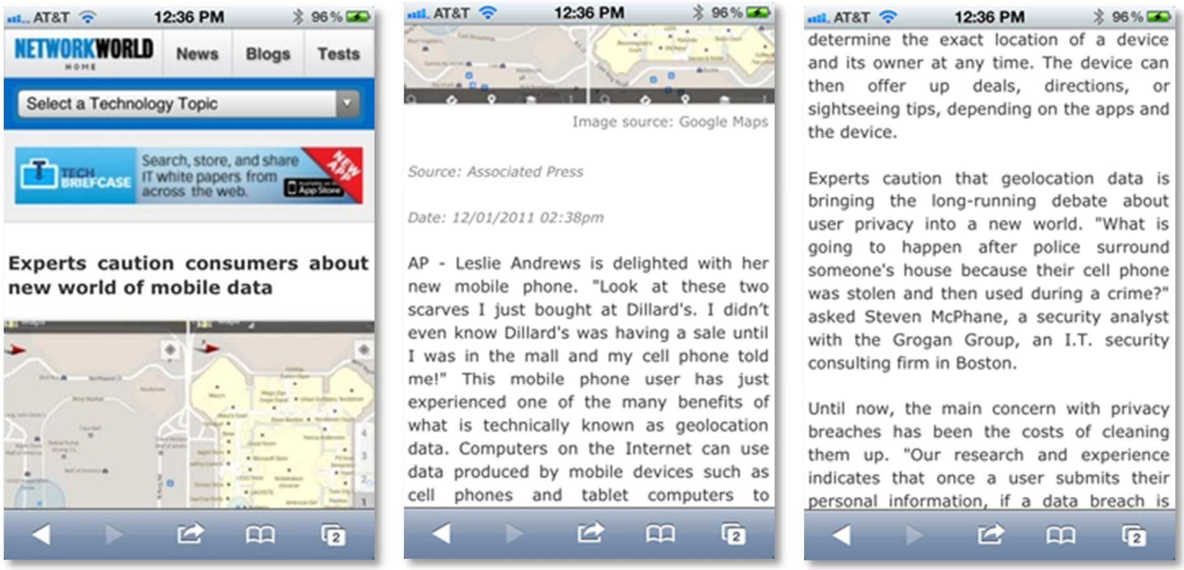
The location-based services (LBS) of Sharing Tree were fully functional and allowed the consumer to view a map of their current location with markers of useful sites generated by friends and family members in the consumer's social network (which could be automatically imported from Facebook).

Manipulations

A research participant's level of self-regulation cannot be manipulated. Rather, their perceived level of risk immediacy was manipulated. This was accomplished by requiring the participants to read a mock news article written by a supposed expert on the exact nature of mobile privacy risks before they reviewed the actual mobile app.

Twelve versions of the mock news article were created with two manipulations (3 x 4 factorial design) varying across them. First, three levels of privacy risk immediacy were included meaning that the "expert" states that mobile privacy exploits are likely to occur in either 1) immediately when the data is collected, 2) sometime in the first 24 hours, or 3) sometime in the first month. In order to validate this manipulation, a latent construct measure of the perceived risk immediacy was measured for each participant. These items were used to verify that the participants actually perceived differences in immediacy based on the experimental manipulation. One-way ANOVAs indicate that there was a significant difference between Treatments 1 and 3 ($p < 0.001$).

Second, the mock news story was created to appear from four different sources (networkworld.com, USAtoday.com, university newspaper, no story) in order to reduce the potential for source credibility bias (Chaiken et al. 1994) (see Figure 3).


AT&T 12:36 PM 96 %
NETWORKWORLD HOME
News
Blogs
Tests
Select a Technology Topic
TECH BRIEFCASE Search, store, and share IT white papers from across the web.
NEW APP
App Store

Experts caution consumers about new world of mobile data

Image source: Google Maps

Source: Associated Press

Date: 12/01/2011 02:38pm

AP - Leslie Andrews is delighted with her new mobile phone. "Look at these two scarves I just bought at Dillard's. I didn't even know Dillard's was having a sale until I was in the mall and my cell phone told me!" This mobile phone user has just experienced one of the many benefits of what is technically known as geolocation data. Computers on the Internet can use data produced by mobile devices such as cell phones and tablet computers to determine the exact location of a device and its owner at any time. The device can then offer up deals, directions, or sightseeing tips, depending on the apps and the device.

Experts caution that geolocation data is bringing the long-running debate about user privacy into a new world. "What is going to happen after police surround someone's house because their cell phone was stolen and then used during a crime?" asked Steven McPhane, a security analyst with the Grogan Group, an I.T. security consulting firm in Boston.

Until now, the main concern with privacy breaches has been the costs of cleaning them up. "Our research and experience indicates that once a user submits their personal information, if a data breach is

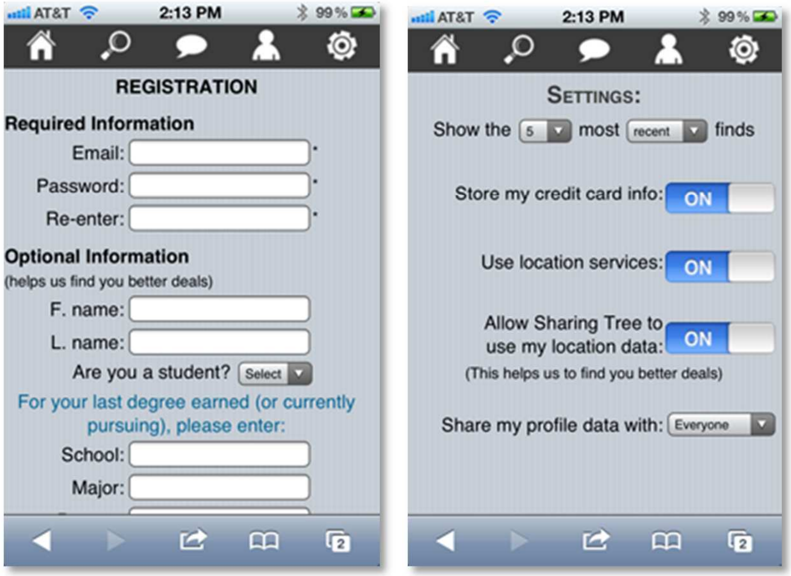
Figure 4. Screenshots of Mock News Story in a Mobile Browser

Procedures

The study procedures included:

1. Each participant, on their smartphone, navigated to the website where the experimental instructions and survey was hosted. They were given a short pretest to measure their self-efficacy and privacy concerns.

2. Next, the participants were asked to read the mock news report and required to correctly answer a quiz question proving they had read the article



REGISTRATION

Required Information

Email: *

Password: *

Re-enter: *

Optional Information

(helps us find you better deals)

F. name:

L. name:

Are you a student? Select

For your last degree earned (or currently pursuing), please enter:

School:

Major:

SETTINGS:

Show the 5 most recent finds

Store my credit card info: ON

Use location services: ON

Allow Sharing Tree to use my location data: ON

(This helps us to find you better deals)

Share my profile data with: Everyone

Figure 5. Sharing Tree App Registration and Settings

3. Next, the participants were given a link to the app 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 (see Figure 5)

4. 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.

Measures

Prior survey items were used to measure privacy concern (Xu et al. 2012), perceived benefits (Xu et al. 2010), perceived privacy risks (Keith et al. 2013), intent to disclose (Dinev et al. 2006), mobile computing self-efficacy (Keith et al. 2011), perceived risk immediacy (Keith et al. 2012), and privacy risk awareness (Xu et al. 2010). Perceived privacy risks include both privacy risks to location data as well as risks to personal information. Similarly, perceived benefits was 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.

Action control was collected based on prior research (Babin et al. 1995; Kuhl 1985). It includes 20 short hypothetical scenarios. Each scenario contains two responses. Participants are asked to select which response they would choose for each scenario. One response is coded as action control while the other is state control. The items measuring patience were created unique for this study but based on prior research (Mischel et al. 1972).

Actual disclosure was measured by 1) 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), 2) the stated level of accuracy of the information provided, and 3) the 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 and privacy awareness, including whether or not the participant was a smartphone user, number of apps regularly used, age, gender, ethnicity, employment, and education background (asked separately from the Sharing Tree app registration page). Lastly, the news story source was also included as a control.

Results

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 et al. 2005; Liang et al. 2007; Pavlou et al. 2007; Straub et al. 2004).

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 as well as several non-normal variable distributions (Chin et al. 2003; Fornell et al. 1982). All measurement items were standardized. Figure 1 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 R2 scores (i.e., the amount of variance accounted for in the model) and the latent variable paths.

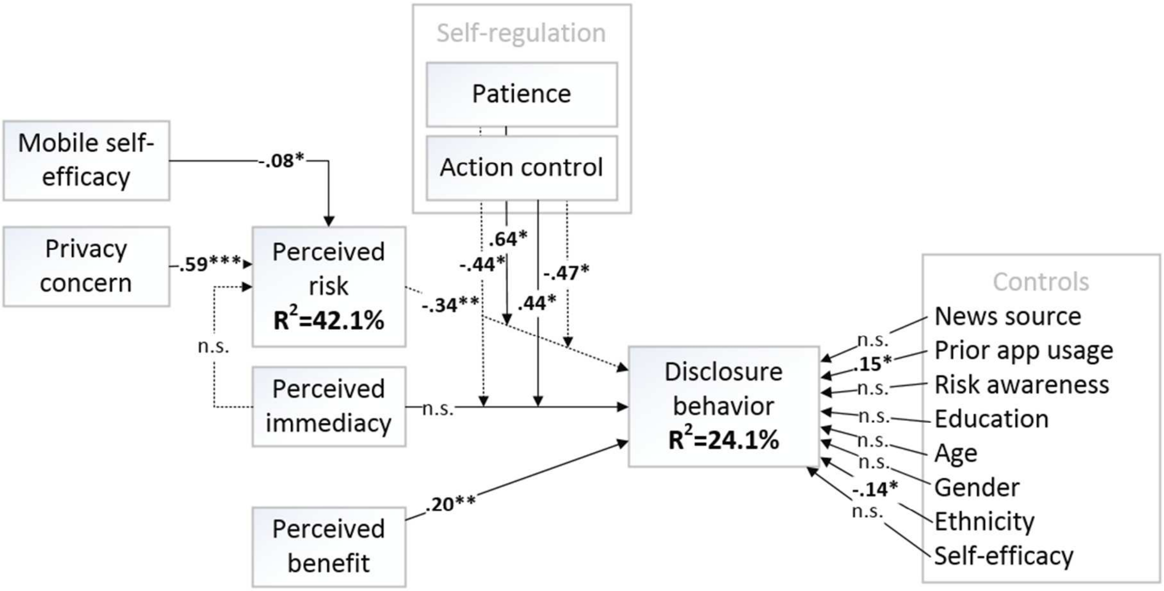


Figure 6. PLS Analysis Results

Discussion

Based on the results of Study 1, each of the hypotheses have been confirmed so far. Patience reduced the effect (β = -0.44, p < 0.05) of perceived risk on actual disclosure (H1) and increased the effect (β = 0.64, p < 0.05) of perceived risk immediacy on actual disclosure (H2). As hypothesized, action control increased the effect (β = 0.44, p < 0.05) of perceived risk on actual disclosure (H3) and decreased the effect (β = -0.47, p < 0.05) of perceived risk immediacy on actual disclosure.

Although not hypothesized, there were several other relationships of interest to note. Even with the new interaction effects, there was still a significant direct effect of perceived risk (β = -0.34, p < 0.01) and perceived benefit (β = 0.20, p < 0.01) on actual disclosure. Although more general measures of privacy concern have occasionally not been significant in prior privacy calculus studies (Keith et al. 2010; Xu et al. 2010), we found a very strong effect of privacy concern on perceived risk (β = 0.59, p < 0.001). This is likely due to using an improved instrument developed specifically for mobile devices and applications (Xu et al. 2012). In addition, mobile self-efficacy had a negative effect on perceived risk (β = -0.08, p < 0.05). Among the other control variables, only ethnicity (β = -0.14, p < 0.05) and prior app usage (β = 0.15, p < 0.05) had significant effects on actual information disclosure. News story source, risk awareness, education, age, and mobile self-efficacy had no effect on actual disclosure.

Implications

There are several interesting and useful implications of this study for future researchers and practitioners based on Study 1. It should be noted that the R squared value in this study for actual disclosure (24.1%) was much higher than the similar methodology used in Keith et al. (2013) (from 2.4% to 7.8%), implying that privacy calculus can be enhanced by accounting for consumer characteristics such as self-regulation. Overall, we find support for our self-regulation based model.

For self-regulation research, these results demonstrate that being action-oriented does not always have positive results as found in prior studies. In our context, action-oriented individuals artificially perceive less risk and disclosure more information because of their intense focus on accomplishing a task. These types of consumers should be wary in the mobile app context because accomplishing their goal will also include a potential risk in addition to a utility or benefit.

Similarly, being patient helps consumers cope with the difficulties in evaluating the immediacy of privacy risks. As stated previously, consumers are known to overly discount future costs (Henderson et al. 1998) causing them to accept relatively small initial benefits for much larger future costs. Being able to delay gratification allows some consumers to manage impulses and make smarter decisions regarding their information disclosure over mobile apps.

Moreover, these results will help app providers to better design privacy statements. Privacy statements should clearly inform consumers about the exact nature of the application risks and when these risks will take place. By making consumers more aware of the benefits and risks, app providers may help consumers to make more rational choices based on their level of self-regulation (Keith et al., 2012).

Limitations and Future Research

There are still certain limitations of this study. For example, this study captures only a cross-sectional snapshot of disclosure behavior. It is likely that many participants did not disclose simply because they were hurrying through the study. Similarly, even though the study was set up to deceive participants into believing there were real risks, it is possible that some perceived the controlled nature of the study and disclosed more data than they normally would.

Lastly, we argue about that consumers are not fully rational and there are valuation of mobile app risk which has been established in recent research (Keith et al. 2012). It is likely that greater education and awareness of privacy risk could change consumer behavior overtime. Although we control privacy awareness using minimal two-item measure, future research should expand the construct of privacy risk education and study its influence over time.

Conclusion

In summary, this study finds support for an expanded privacy calculus model which incorporates consumer self-regulation characteristics like patience and action control. We build on the information privacy literature by using improved experimental methodology for capturing actual consumer behavior over time. In particular, this research has benefited from the design of technical artifact that allows for both control manipulation as well as external validity and relevance in the artifact context.

References

Acquisti, A., and Grossklags, J. 2004. "Privacy Attitudes and Privacy Behavior," in Economics of Information Security, L. Camp and S. Lewis (eds.), Springer US, pp. 165-178.

Ainslie, G. 1975. "Specious reward: A behavioral theory of impulsiveness and impulse control," Psychological Bulletin (82:4), pp 463-496.

Ajzen, I. 1991. "The theory of planned behavior," Organizational Behavior and Human Decision Processes (50:2) Dec, pp 179-211.

Babin, B. J., and Darden, W. R. 1995. "Consumer self-regulation in a retail environment," Journal of Retailing (71:1) Spr, pp 47-70.

Berendt, B., G, O., #252, nther, and Spiekermann, S. 2005. "Privacy in e-commerce: stated preferences vs. actual behavior," Commun. ACM (48:4), pp 101-106.

Beresford, A. R., Kübler, D., and Preibusch, S. 2010. "Unwillingness to Pay for Privacy: A Field Experiment."

Chaiken, S., and Maheswaran, D. 1994. "Heuristic processing can bias systematic processing: effects of source credibility, argument ambiguity, and task importance on attitude judgment," Journal of personality and social psychology (66:3), p 460.

Chin, W. W., Marcolin, B. L., and Newsted, P. R. 2003. "A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study," Information Systems Research (14:2), pp 189-217.

Decker, M. Year. "Location Privacy-An Overview," Mobile Business, 2008. ICMB '08. 7th International Conference on2008, pp. 221-230.

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

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

Gefen, D., and Straub, D. W. 2005. "A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example," Communications of the AIS (16:5), pp 91-109.

Henderson, N., and Langford, I. 1998. "Cross-disciplinary evidence for hyperbolic social discount rates," Management Science (44:11) Nov, pp 1493-1500.

Hoadley, C. M., Xu, H., Lee, J. J., and Rosson, M. B. 2010. "Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry," Electronic Commerce Research and Applications (9:1), pp 50-60.

Kahneman, D., and Tversky, A. 1979. "Prospect Theory: An Analysis of Decision under Risk," Econometrica (47:2), pp 263-291.

Keith, M. J., Babb, J. S., Furner, C. P., and Abdullat, A. 2010. "Privacy Assurance and Network Effects in the Adoption of Location-Based Services: An iPhone Experiment," in Proceedings of the International Conference on Information Systems (ICIS '10): St. Louis, MI, p. 237.

Keith, M. J., Babb, J. S., Furner, C. P., and 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: Kauai, HI.

Keith, M. J., Thompson, S. C., Hale, J., Benjamin Lowry, P., and Greer, C. 2013. "Information Disclosure on Mobile Devices: Re-examining Privacy Calculus with Actual User Behavior," International Journal of Human-Computer Studies (71:12), pp 1163–1173.

Keith, M. J., Thompson, S. C., Hale, J., and Greer, C. 2012. "Examining the Rationality of Information Disclosure through Mobile Devices," in International Conference on Information Systems (ICIS '12): Orlando, FL.

Kuhl, J. 1985. "Volitional mediators of cognition-behavior consistency: Self-regulatory processes and action versus state orientation," in Action control, Springer, pp. 101-128.

Laibson, D. 1997. "Golden eggs and hyperbolic discounting," Quarterly Journal of Economics (112:2) May, pp 443-477.

Loewenstein, G., and Prelec, D. 1992. "Anomalies in Intertemporal Choice: Evidence and an Interpretation," Quarterly Journal of Economics (107:2), pp 573-597.

Metcalfe, J., and Mischel, W. 1999. "A hot/cool-system analysis of delay of gratification: dynamics of willpower," Psychological review (106:1), p 3.

Mischel, W., Ebbesen, E. B., and Raskoff Zeiss, A. 1972. "Cognitive and attentional mechanisms in delay of gratification," Journal of personality and social psychology (21:2), p 204.

Mischel, W., Shoda, Y., and Rodriguez, M. I. 1989. "Delay of gratification in children," Science (244:4907), pp 933-938.

Norberg, P. A., Horne, D. R., and Horne, D. A. 2007. "The privacy paradox: Personal information disclosure intentions versus behaviors," The Journal of Consumer Affairs (41:1) Sum, pp 100-126.

Ringle, C. M., Wende, S., and Will, S. 2005. "SmartPLS 2.0 (M3) Beta," Hamburg, Germany.

Rookh, D. W. 1987. "The buying impulse," The Journal of Consumer Research (14:2), pp 189-199.

Seriot, N. Year. "iPhone privacy," Black Hat DC 2010, Black Hat, Arlington, VA, USA, 2010, p. 30.

Xu, H., Gupta, S., Rosson, M. B., and Carroll, J. M. 2012. "Measuring mobile users' concerns for information privacy," in International Conference on Information Systmes: Orlando, FL.

Xu, H., Teo, H. H., Tan, B. C. Y., and Agarwal, R. 2010. "The role of push-pull technology in privacy calculus: The case of location-based services," Journal of Management Information Systems (26:3), pp 135-174.