2014 47th Hawaii International Conference on System Science

A Longitudinal Study of Information Privacy on Mobile Devices

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

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

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

Abstract

The real value of mobile applications is heavily dependent on consumers' trust in the privacy of their personal information and location data. However, research has generated few results based on actual information disclosure and even less that is based on longitudinal behavior. The purpose of this study is to execute a unique and authentic field experiment involving real risks and consumer behaviors regarding information disclosure over mobile devices. We compare two theoretical explanations of disclosure decisions: privacy calculus and prospect theory. Our results indicate that consumers are best modeled as "bounded" rational actors concerning their disclosure behavior. Also, actual information disclosure behavior over mobile applications is a more multifaceted issue than research has treated it thus far. For practice, mobile application providers should be aware that increasing the benefits of information disclosure via the app may have the counterintuitive effect of increasing perceived risk and reducing consumer disclosure.

1. Introduction

Information privacy is seeing a considerable increase in interest from academic researchers [1]. This trend is partially due to the emergence and rapid progress of mobile technologies. Smartphones and tablets typically include global positioning systems (GPS), which can be easily accessed from the software development kits (SDK) used to generate "apps" for each mobile platform. Combined with the availability of application programming interfaces (API) for the most popular social networking systems (e.g., Facebook, Twitter, Linkedin, and Pinterest), mobile apps combine personal information, social network data, and real-time location data. Consequently, mobile apps have become a virtual "shopping mall" of information privacy risks by combining the most valuable consumer information in one device.

Because of the incredible usefulness and attractiveness of many mobile apps, consumers are flocking to them with seemingly little regard for the risks. Research has implied that as long as: 1) an app has some sort of stated privacy policy with third- party assurance [2, 3], 2) the app appears to be the favorite among prior app adopters [2], or 3) app consumers believe they are skilled enough [4] or "in control" enough [5] to avoid the privacy risks, they will adopt the app and disclose any requested information.

Perhaps the dominant paradigm for explaining information disclosure is *privacy calculus* [6] which posits a tradeoff of perceived risks and benefits as primary determinants of disclosure. Privacy calculus is useful for explaining rational actors for a particular transaction. However, it doesn't account for the trends in risks and benefits over time or the bounded rationality consumers can exhibit with risk-based decisions [7].

Similarly, there are two limitations commonly found in prior research that may limit their implications. First, with little exception [e.g., 7], most research in the mobile app context has restricted the data collection and theoretical models to include information disclosure *intentions* without gathering actual information disclosure. This is problematic considering the oft observed *privacy paradox* in which actual consumer information disclosure far exceeds stated intentions [8, 9]. Second, there are even fewer *longitudinal* studies of information disclosure over mobile devices. This is also problematic considering that research has shown that consumers exhibit hyperbolic discounting in which future risks and benefits are viewed differently from the immediate term [7, 10]. In addition, privacy-related experience and knowledge are known to affect risk judgments [3, 11]. As a result, information disclosure decisions would logically change over time. Both of the above limitations are understandable considering the nature and difficulty of collecting longitudinal information disclosure data. Further increasing this difficulty, today's mobile apps include a variety of information including personal data, social network data, and location data.

Consequently, the purpose of this study is to design and execute a longitudinal field experiment in which consumers will need to make real disclosure decisions over time based on real privacy risks. To accomplish this, we designed a mobile application (available on iOS and Android smartphones and tablets) called "Findamine." Findamine is a social geo-caching game that requires players to find a series of clues each week leading to interesting locations around their city. Players are incented to refer and track other players using an online social network built into the accompanying app website. Players are also incented to complete an optional player profile and to share their profile data,

978-1-4799-2504-9/14 $31.00 © 2014 IEEE
DOI 10.1109/HICSS.2014.391

app data (including their location), and social network data with as many players as possible. Players are awarded game points that qualify the players for gift cards and prizes for every type of data disclosed. However, players are also given a detailed set of privacy controls allowing them to make conscious choices about exactly which types of information they will share and who they will share it with (e.g., nobody, friends, or all players). To manipulate behavior over time, the level of points awarded for data disclosed was either increased or decreased over time to observe the tradeoff between disclosure risks and benefits over time.

As a result of this design, we can test whether alternative theories, like *prospect theory* [12], can better explain mobile information disclosure. Prospect theory accounts the for the irrational consumer behaviors regarding past experience in new risk decisions. The results reveal support prospect theory. After explaining the experimental design in detail, we expound on these and other interesting findings at the end of the paper.

2. Literature Review

In general, *information privacy* refers to an individual's control over the myriad forms of information about themselves [13, 14] including its collection, unauthorized use, improper access, and errors [11]. Information privacy has a long and interesting research stream which is well-documented in recent literature reviews [1, 13]. Its definition depends on its conceptualization. Smith et al. [1] summarizes these conceptualizations as information privacy as: (1) a *state* [15]—something you currently have (or don't have); (2) a *control* [16]—something to be limited during transactions; (3) a *right* [17]—something the law entitles you to; and most recently 4) a *commodity* [18]—something that can be traded.

As discussed, the progress of mobile device technologies and popularity of social networking applications have combined to increase privacy risks. Because of the emerging nature of this problem, the research in this area only beginning to mature and much is found in recent conference proceedings. However, there are key findings worth noting.

First, a recent review of the fledgling research on mobile location privacy behaviors [19] indicates that consumers prefer privacy on mobile devices. Although this finding may seem obvious, it is important because consumers have shown a relative unwillingness to pay for privacy in other contexts [20]. Moreover, because mobile consumers prefer privacy, they are rational, making this context suitable to theories that assume consumer rationality.

Second, even though the ethics and intentions of mobile app providers cannot be verified (as evidenced in [21]), consumers have proven to be more than willing to adopt and pay for mobile apps. To justify increased privacy risk, consumers rely on some combination of external signals, internal self-assessments, or "sunk cost" beliefs. For example, privacy promises, seals, or third party statements about the reliability of an app provider can significantly reduce perceived risk [2, 3, 22]. Concurrently, consumers may believe that they are firmly in control of the risky situation regardless of the asymmetries of information between themselves and the app provider [5] or that their self-efficacy with mobile devices will allow them to prevent unauthorized access to their data [4]. More recently, research has also shown that, much like gamblers sunk in a "loss" position, mobile app consumers are willing to take greater risks if they believe their personal information is already "lost" [7]. Therefore, they readily adopt apps to gain the benefits, believing they cannot be placed in greater risk.

Lastly, a qualitative analysis of consumer focus groups and business managers [19] has revealed that both the costs and benefits of information disclosure over mobile devices are more multifaceted than prior research has considered. The decision to adopt a mobile application involves not only location data risks, but also personal information risks, and often social network information risks and others. Similarly, the benefits are also diverse including improvements in personal productivity, well-being, and entertainment. Although no single study can or should examine all forms of benefits at once, some types (e.g. entertainment) have not been examined in research at all. Additionally, most research studies (with limited exception [7]) focus on only one form of privacy risk.

3. Theoretical Model and Hypotheses

Several theories have been used to explain privacy concerns and perceived privacy risks. However, privacy calculus has been the dominate paradigm for explaining the formation of disclosure intentions [2, 3, 7, 19].

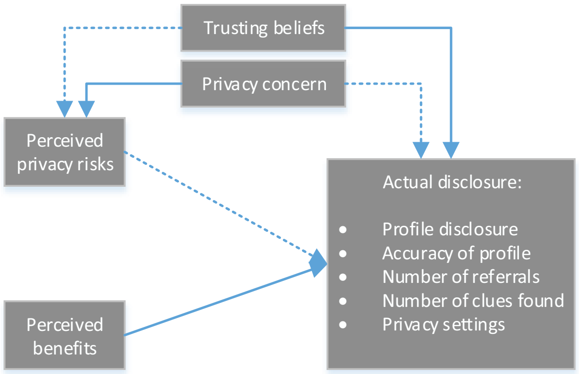


Figure 1. Privacy Calculus Model

Privacy calculus in the e-commerce context explains information disclosure as a tradeoff between the perceived benefits and context-specific risks [6]. Also, the formation of perceived risks and disclosure intentions are determined by an individual's general privacy concerns with the environment.

3.1. Privacy Calculus Hypotheses

Because the nomological relationships in privacy calculus theory have been posited [6] and tested numerous times [2, 3, 7, 19], we do not formally hypothesize them here—although we test them in our study as a theoretical baseline. Importantly, we extend privacy calculus by accounting for changes in disclosure benefits and risks over time.

Privacy calculus is based on the assumption that consumers are *rational* [7]—meaning they can estimate the benefits and risks of information disclosure with some degree of accuracy and then make decisions based on a linear relationship, or tradeoff, between them. This assumption also implies that privacy calculus adopts the conceptualization of privacy as a commodity. That is, consumers can place a monetary value behind both the costs and benefits, thus making it possible to evaluate a perceived net gain/loss. Consequently, risks and benefits are independent of each other. They are calculated separately, yet both are used in the disclosure equation. Thus, if privacy calculus holds true as prior research has evidenced [2, 3, 7, 19], then increases in benefits over time should have no effect on perceived risk, yet also cause greater information disclosure:

H1: As information disclosure benefits increase, app consumers will perceive less mobile app risk.

H2: As information disclosure benefits increase, app consumers will disclose more information.

3.2. Prospect Theory Hypotheses

Although privacy calculus theory has proven to be a strong predictor of disclosure intentions, it has two limitations that we address. First, privacy calculus is intended to explain a cross-section of privacy beliefs and behaviors. A consumer's *current* risk and benefit assessment is what determines their *current* information disclosure. However, the risks and benefits of a given information technology (IT) are often changing, implying that a privacy calculus model might not be a good indicator of future behavior. For example, a news report of a serious security breach would certainly change users' risk perceptions. Similarly, if mobile app provider were to offer new incentives or functionality, then past information disclosure levels would be a poor indicator of future consumer behavior.

Privacy calculus assumes that consumers are rational and base disclosure decisions on a linear relationship between the risks and benefits of disclosure. Nevertheless, a recent study demonstrated in the mobile app context that this assumption is only partially valid [7]. Consumers tend to overweight the probability of risks, while underweighting the impact or cost of risks [7]. As a result, we propose *prospect theory* [12] as a useful lens to modify the privacy calculus model. A key proposition of prospect theory is that individuals strongly consider reference points when making risk decisions. For example, if a gambler is "up" from their original financial position, they will take fewer risks whereas they will take greater risks if they are "down" in order to catch up to their original position. However, the actual risk (probability * impact) does not change.

Prospect theory can help inform the first limitation we described. If the benefits of information disclosure are increasing over time, consumers are in a "gain" position from their original reference point. Thus, they will be more risk averse. Conversely, if the benefits of information disclosure are decreasing over time, consumers will be in a "loss" position and willing to accept greater risks to return to the net gain/loss position they once had. This proposition is supported by recent research [7] that found consumers' perception of their level of prior risk exposure (i.e., the extent to which their personal information was already held by marketing companies) significantly increased their intention to disclose information again. Similarly, the level of prior benefits held significantly affected consumers future disclosure decisions. Therefore:

H3: As information disclosure benefits increase, app consumers will perceive more mobile app risk.

H4: As information disclosure benefits increase, app consumers will disclose less information.

In summary, we examine whether changes in information disclosure benefits over time are better explained by privacy calculus or prospect theory.

4. Methodology

As noted, we created a mobile app with an accompanying website to test the hypotheses. Five hundred and sixty-eight undergraduates at a large private university in the western United States participated during the spring semester of 2013.

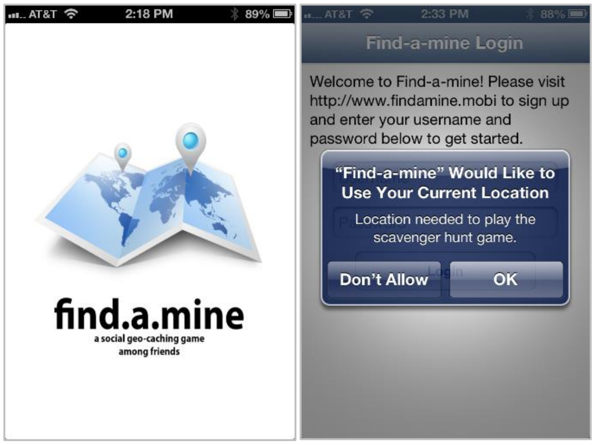
The mobile phone application (called "findamine" or "find.a.mine" it the Apple App Store™ and Google Play™) was a geo-caching game. Each week (for 12 weeks), participants received three new clues on their phone or tablet (iOS and Android supported) through the mobile app. They earned points by deciphering the clue, travelling to the location, and taking a picture of the location through the mobile app. If they were correct, they earned points. Participants also earned points by sharing demographic information and uploading a photo on the personal profile they created on the website and by referring friends to join.

We provided weekly and end-of-game incentives to encourage play. Each week, we awarded 3-15 gift cards ($10 Visa or $11 campus gift card) to the participants who were first to find all of that week's locations. At the end of the game, the two participants with the most total points won a Samsung Galaxy Tab II™. We also held a random drawing, based on points earned, to award a third Samsung Galaxy Tab II™.

As seen in the example in Figure 2b&c, if players could not decipher the clue, they could use the "hot/cold" meter which indicated how geographically close they were to the target clue. Upon finding the clue, players pressed the "Found It!" button which prompted them to take a photograph through the app. After the photograph was submitted, participants could login to the mobile website and view their points on the leaderboard. Figure 3 shows the website leaderboard.

a. Splash screen

b. Location data disclosure



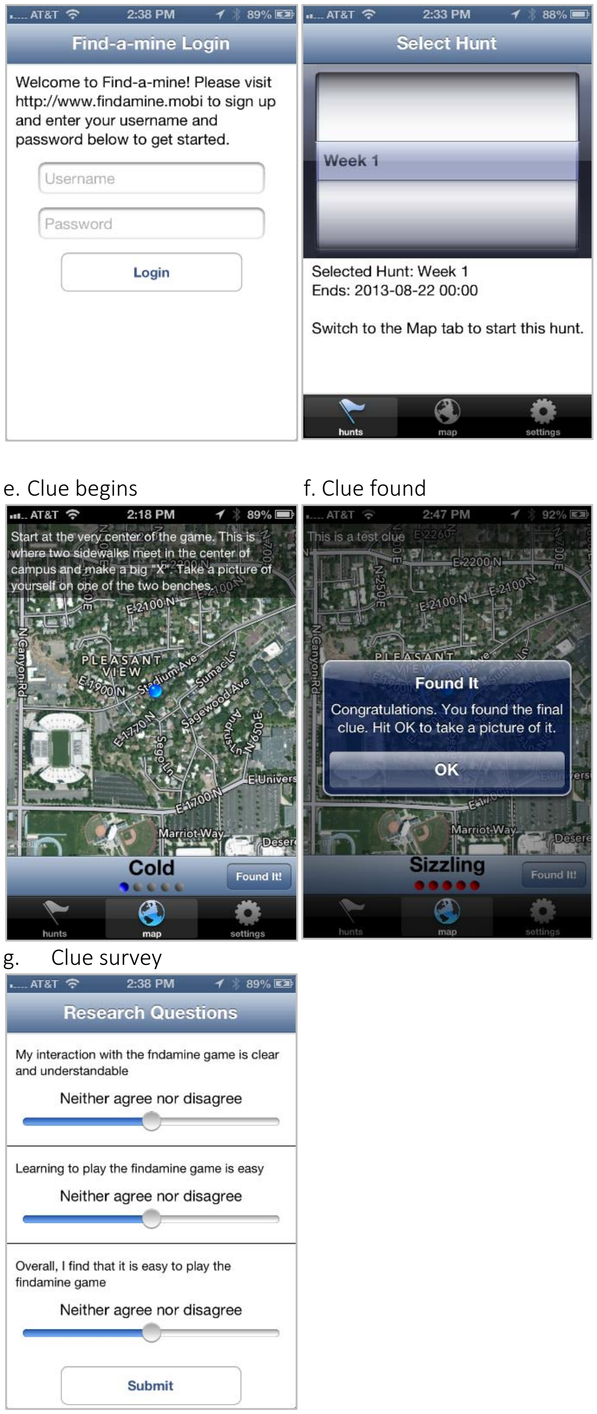
Welcome to Find-a-mine! Please visit http://www.findamine.mobi to sign up and enter your username and password below to get started.

"Find-a-mine" Would Like to Use Your Current Location

Location needed to play the scavenger hunt game.

c. Login screen

d. Clue selection



Welcome to Find-a-mine! Please visit http://www.findamine.mobi to sign up and enter your username and password below to get started.

Selected Hunt: Week 1
Ends: 2013-08-22 00:00

Switch to the Map tab to start this hunt.

Start at the very center of the game. This is where two sidewalks meet in the center of campus and make a big "X". Take a picture of yourself on one of the two benches.

This is a test clue

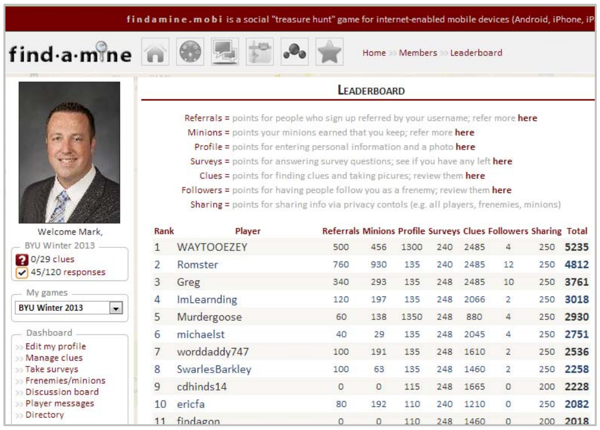
Congratulations. You found the final clue. Hit OK to take a picture of it.

My interaction with the fndamine game is clear and understandable

Learning to play the findamine game is easy

Overall, I find that it is easy to play the findamine game

Figure 2. Mobile and Screen Shots



findamine.mobi is a social "treasure hunt" game for internet-enabled mobile devices (Android, iPhone, iP

LEADERBOARD

Referrals = points for people who sign up referred by your username; refer more here
Minions = points your minions earned that you keep; refer more here
Profile = points for entering personal information and a photo here
Surveys = points for answering survey questions; see if you have any left here
Clues = points for finding clues and taking picures; review them here
Followers = points for having people follow you as a frenemy; review them here
Sharing = points for sharing info via privacy contols (e.g. all players, frenemies, minions)

Rank	Player	Referrals	Minions	Profile	Surveys	Clues	Followers	Sharing	Total
1	WAYTOOEZEY	500	456	1300	240	2485	4	250	5235
2	Romster	760	930	135	240	2485	12	250	4812
3	Greg	340	293	135	248	2485	10	250	3761
4	ImLearnding	120	197	135	248	2066	2	250	3018
5	Murdergoose	60	138	1350	248	880	4	250	2930
6	michaelst	40	29	135	248	2045	4	250	2751
7	worddaddy747	100	191	135	248	1610	2	250	2536
8	SwarlesBarkley	100	63	135	248	1460	2	250	2258
9	cdhinds14	0	0	115	248	1665	0	200	2228
10	ericfa	80	192	110	240	1210	0	250	2082
11	findagon	0	0	110	248	1460	0	200	2018

Figure 3. Game Leaderboard (website view)

4.1. Ensuring Experimental Validity

To generate valid and realistic information disclosure behaviors, participants needed to perceive actual personal risk and fear of disclosing information. This was accomplished in multiple ways. First, we obtained IRB approval to *not* require participants' informed consent because informed consequent automatically elevants' participants awareness of risk and the artificial nature of data collection. Rather, participants were recruited under the false pretense that a local mobile app business wanted to pilot test a new geo-caching app at their university. As a result, there was no priming effect on participants and they participants were less susceptible to social desirability bias. Moreover, they were told that the friends and family members they referred to the app did not have to be university students or employees.

Second, the context of the app was chosen to replicate several relevant forms of information privacy and encourage consistent disclosure. For example, by choosing an app design with weekly incentives, participants were motivated to play by more than just extra credit. Because it was a geo-caching app, there was a clear need to collect location data, which presents personal safety risks [19]. The social network aspect of the app created both additional enjoyment as well as creating vertical and horizontal personal information privacy risks [23]. The website included a player directory and social network (consisting of "frenemies" and "minions"[1]). Players could search through and explore the app directory, which allowed them to view any player profile and app data that had been made public (like traditional social network apps) and add them to their social network. Thus, participants' personal information could legitimately be made publicly available—unless they set their privacy settings to restrict their data to "friends only" or "nobody."

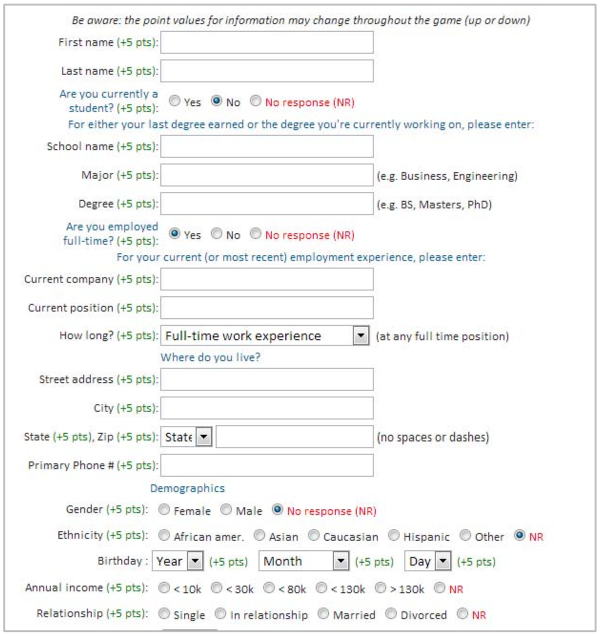
Third, the findamine app architecture needed to match those that are most potentially dangerous to consumers. In particular, the game was made possible by a native mobile app, a cross-platform website, and web services that connected the mobile app to the external database. When the app was introduced to participants, they were given a brief explanation of how the mobile app and website worked together with the same data. Consequently, participants were aware that the mobile app was capable of sending personal information to remote servers.

4.2. Experimental Manipulation

To understand how information disclosure behaviors change over time, we decided to manipulate the benefits of disclosure. As noted, participants were incented to disclose their profile data and personal photo by giving them points, which earned prizes, for each piece of information. At the beginning of the experiment, all participants were offered 35 points for each piece of information they disclosed. However, over the next three months until the final day, half of the participants were randomly assigned to have a gradual point reduction while the other half's points were increased over time. By the end of the experiment, one group was offered 65 points for each piece of information and the other group was offered 5 points. Participants knew their points were constantly changing because they frequently checked the leaderboard. They were also warned that point values would change during the course of the experiment[2]. Figure 4 depicts a screen shot from a participant in the "decreasing" condition on the last day of the game. Participants were allowed to either submit or delete the profile data stored by this form at any time during the game. In this figure, no data has been entered. However, the participant could earn five points for each piece of information if they chose to submit it.

[1] *Frenemies* were other players that could be added to a participant's personal network. By adding them to your network, you could monitor their points, track their clue progress, and share selected data with them. *Minions* were other players a participant had personally invited to play the game. Players also earned a percentage of their minions' points toward their own point total.

[2] However, players were not told that some would see an increase in points while others had a decrease—only that points would change in general and that they should review them frequently.



Be aware: the point values for information may change throughout the game (up or down)

First name (+5 pts):

Last name (+5 pts):

Are you currently a student? (+5 pts): ○ Yes ● No ○ No response (NR)

For either your last degree earned or the degree you're currently working on, please enter:

School name (+5 pts):

Major (+5 pts): (e.g. Business, Engineering)

Degree (+5 pts): (e.g. BS, Masters, PhD)

Are you employed full-time? (+5 pts): ● Yes ○ No ○ No response (NR)

For your current (or most recent) employment experience, please enter:

Current company (+5 pts):

Current position (+5 pts):

How long? (+5 pts): Full-time work experience (at any full time position)

Where do you live?

Street address (+5 pts):

City (+5 pts):

State (+5 pts), Zip (+5 pts): State (no spaces or dashes)

Primary Phone # (+5 pts):

Demographics

Gender (+5 pts): ○ Female ○ Male ● No response (NR)

Ethnicity (+5 pts): ○ African amer. ○ Asian ○ Caucasian ○ Hispanic ○ Other ● NR

Birthday : Year (+5 pts) Month (+5 pts) Day (+5 pts)

Annual income (+5 pts): ○ < 10k ○ < 30k ○ < 80k ○ < 130k ○ > 130k ○ NR

Relationship (+5 pts): ○ Single ○ In relationship ○ Married ○ Divorced ○ NR

Figure 4. Example of Profile Points

4.3. Measures

Because of our research design, we were able to capture a variety of objective measures for overall game play and information disclosure. Six of them are included in this study representing three types of information which can be disclosed over mobile apps:

I. *Personal information*

1. Percent of overall profile information disclosed (0.0 to 1.0)
2. Accuracy of profile information entered (1=nothing was accurate, 6=everything was accurate)[3]
3. Privacy setting (0=nobody, 1=minions only, 2=frenemies and minions, 3=all players)

II. *Location data*

3. Number of game clues found

III. *Social network information*

4. Number of referrals (required submitting friends' email addresses)

IV. *Controls*

5. Number of updates to profile data
6. Number of website logins

In addition to the game measures, we collected latent construct measures of *perceived disclosure risk* (modeled as a second order formative construct consisting of both *location data risk* and *personal information risk*) and *perceived disclosure benefits* (modeled as a second order formative construct consisting of both *locatability* and *personalization*). These measures were based on prior relevant research [3, 7]. We also measured general *privacy concern* using a new and better-targeted instrument for mobile privacy [24]. Lastly, we included *trusting beliefs* which is an important determinant of perceived risk privacy calculus theory [6] and trusting behaviors such as information disclosure [25].

To capture these latent measures during the most relevant moments during game play, and to minimize the potential for common methods bias (CMB), we designed the findamine app to allow a few survey questions (typically 3-5) to be collected from the app as soon as a player selects a clue and before the map was displayed. Figure 2d shows an example screen shot of one survey. This screen is displayed before the screen shot in Figure 2b. Once the player answers the questions, they can proceed with the clue. During the game, not all clues had questions assigned to them. The items measured for this study were collected during the last few clues of the game after participants had had a couple of months of experience with the game—giving adequate time for players to form experience-based perceptions. In this way, we were able to capture perceptions *during* the moments those perceptions were relevant in the minds of players—as opposed to before or after the game when those beliefs would be only hypothetical.

5. Results

5.1. Measurement Validity

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 CMB. For brevity, the details are not reported here. However, the results indicated acceptable factorial validity and minimal multicollinearity or CMB based on the standards for IS research [26-29].

5.2. Hypothesis Testing

To analyze the results, we analyzed a path model with the PLS SEM technique using SmartPLS 2.0.M3 [30]. This was appropriate because we needed to test multiple paths in the same model, two of the constructs were second-order formatives, and PLS does not depend on normal distributions or interval scales [31, 32]—making it ideal for our measures of actual behavior.

[3] To account for the potential of entering inaccurate information into the profile data, participants were asked one final question at the end of the experiment after all prizes had been awarded: Which of the profile data you submitted was inaccurate?

Table 1 summarizes descriptive statistics of the players and their game play. About two-thirds (68%) of participants were male. Although participants could refer any friend to play the game they wanted to in order earn points, it originated in an information systems course which was dominantly male.

Table 1. Descriptive Statistics

	Male (n=402)	Female (n=166)
Age (years)	$\bar{x}$ = 23.46	$\bar{x}$ = 20.91
Points accumulated	$\bar{x}$ = 1569	$\bar{x}$ = 1425
Weekly prizes won	55 (76.4%)	17 (23.6%)
Friends recruited	162 ($\bar{x}$ = 0.61)	25 ($\bar{x}$ = 0.30)
Number of website sessions:	Total $\bar{x}$ = 9.90 Mobile $\bar{x}$ = 3.90	Total $\bar{x}$ = 4.79 Mobile $\bar{x}$ = 1.43

Table 2. Means, Std. Deviation, and Correlations

Var.	$\bar{x}$	s	1	2	3	4	6	7	8	9	10	11	12
1 Acc	5.5	1.0											
2 Ben	4.1	1.3	.02										
3 Clu	2.2	6.0	.10	-.12									
4 DTR	2.9	1.3	-.22	.27	-.14								
6 Dis	0.7	0.3	.05	-.02	.10	-.23							
7 Log	8.4	11.0	-.04	.02	.26	-.12	.20						
8 PC	4.5	1.1	-.15	.06	.01	.38	-.25	-.01					
9 Ref	0.3	2.2	.04	-.03	.09	-.08	.12	.81	.00				
10 Risk	3.5	1.4	-.18	.32	-.07	.54	-.14	-.06	.35	-.13			
11 TRU	5.1	1.0	-.01	-.08	.06	-.45	.24	.07	-.14	.11	-.33		
12 Upd	0.1	0.3	-.08	.05	.14	-.09	.20	.22	.03	.16	.00	.13	
13 PrS	1.8	0.7	-.03	.00	.12	-.14	.38	.41	-.19	.32	.00	.18	.26

Note: Acc = *acc*uracy of profile data submitted, Ben = perceived *ben*efits of disclosing data to findamine, Clu = total *clu*es found (i.e. amount of location data disclosed), Dir = the randomly assigned *dir*ection of change in benefits, Dis = amount of profile data *dis*closed, Log = the total number of times the participant logged into the findamine website, PC = privacy concern, Ref = number of people referred to play findamine, Risk = perceived privacy risk of disclosing data to findamine, TRU = trusting beliefs in findamine provider, Upd = number of updates to profile data, PrS = level of privacy settings (higher means more sharing)

Table 2 summarizes the variable means, standard deviations, and construct correlations. Table 3 summarizes the path coefficients for the PLS model. The t-statistics were generated from running a number of bootstrap procedures equal to the number of samples (n=569). R^2 values represent the amount of total variance accounted for by the exogenous variables.

Table 3. PLS Path Coefficients and R^2 Values

Path coefficient		*t*-stat
Perceived risk *(R^2 = 37.4%)*		
Direction of change -> perceived risk	0.10	2.79**
Trust -> perceived risk	-0.28	6.21***
Privacy concern -> perceived risk	0.33	7.40***
Perceived benefits *(R^2 = 19.7%)*		
Direction of change -> perceived benefits	0.09	1.88*
Profile disclosure *(R^2 = 25.2%)*		
Direction of change -> profile disclosure	0.10	2.92**
Perceived benefits -> profile disclosure	0.01	0.28
Perceived risk -> profile disclosure	-0.01	0.14
Trust -> profile disclosure	0.19	4.29***
Privacy concern -> profile disclosure	-0.21	5.09***
Updates to profile -> profile disclosure	0.19	6.11***
Updates to profile * accuracy -> profile disclosure	-0.82	2.97**
Accuracy of profile disclosure *(R^2 = 20.5%)*		
Direction of change -> accuracy (after accounting for trust interaction)	0.18 (-0.76)	5.07*** (4.23)***
Direction of change * trust -> accuracy	0.97	6.37***
Perceived benefits -> accuracy	0.04	1.05
Perceived risk -> accuracy	-0.20	3.32***
Trust -> accuracy	-0.08	1.60
Privacy concern -> accuracy	-0.10	2.27*
Privacy settings -> accuracy	-0.07	1.41
Clues found *(i.e,. location data disclosed) (R^2 = 5.2%)*		
Direction of change -> clues found	-0.09	2.00*
Perceived benefits -> clues found	0.06	1.31
Perceived risk -> clues found	-0.08	1.45
Trust -> clues found	-0.02	0.38
Privacy concern -> clues found	0.08	1.56
Referrals *(i.e., social network data disclosed) (R^2 = 14.7%)*		
Direction of change -> referrals	-0.11	2.98**
Perceived benefits -> referrals	0.08	1.83*
Perceived risk -> referrals	-0.12	4.16***
Trust -> referrals	0.02	0.53
Privacy concern -> referrals	0.07	1.57

Notes: *** p < 0.001, ** p < 0.01, * p < 0.05, † p < 0.10; the direct path coefficients were calculated *before* including interaction effects

6. Discussion

Table 4 summarizes the hypothesis testing results. Perhaps most importantly, when the disclosure benefits increased over time, consumers perceived greater risks (β=0.10, *p*<0.01); thus, supporting H3 rather than H1.

Table 4. Hypothesis Testing Results

Hypotheses		Confirmed
Privacy calculus		
H1: As information disclosure benefits increase, consumers will perceive no change in mobile app risk		No
H2: As information disclosure benefits increase, consumers will disclose more information	*Personal data*	Yes*
	Location data	No
	Social network data	No
Prospect theory		
H3: As information disclosure benefits increase, consumers will perceive greater mobile app risk		Yes
H4: As information disclosure benefits increase, consumers will disclose less information	*Personal data*	No*
	Location data	Yes
	Social network data	Yes

Overall, the effect of changing profile data disclosure benefits supports H4 over H2. However, at first glance, it appears that the opposite is true for personal data. Technically, as benefits increased over time, participants disclosed *more* information (β=0.10,

p<0.01). Similarly, the information they did choose to disclose was *more* accurate (β=0.18, p<0.001). However, the profile data is the one type of information which can be disclosed inaccurately. Therefore, a post-hoc interaction effect was tested. Typically, when participants updated their profile, they did so in order to disclosure more information (β=0.19, p<0.001) and, hence, gain more points. However, they typically did so with *in*accurate information (β=-0.82, p<0.001). In other words, the increase in benefits only served to increase the disclosure of false data.

Concerning the other forms of disclosure, Participants completed fewer clues (β=-0.09, p<0.05) (thus, disclosing less location data) and referred fewer friends (β=-0.11, p<0.01) as the benefits for information disclosure increased.

In summary, the prospect theory hypotheses (H3 and H4) were best-supported. However, there are other interesting differences between our findings and prior research worth highlighting. For example, it is clear that trust plays a significant role in determining perceived risk and information disclosure although it has been omitted from some of the prior research [2, 3, 7]. In fact, perceived risks and benefits—the traditional independent variables in privacy calculus theory—become insignificant after accounting for trust when predicting profile disclosure and clues found. Although, perceived risk is clearly more important in predicting the number of referrals (β=-0.20, p<0.001) and privacy settings (β=-0.12, p<0.001).

Lastly, it is also worth noting that privacy concern was a significant predictor of profile disclosure (β=-0.21, p<0.001) and profile accuracy (β=-0.10, p<0.05), but not for clues or referrals.

6.1. Implications for Research

Our research evidence supports prospect theory as a better explanation of the effect of changes in disclosure benefits on perceived risks than does the privacy calculus model. Consumers appear to be considering their original reference point of benefits when making risk decisions regardless of the fact that real risk has not changed. They become risk averse when they are in a "gain" position and risk seeking when in a "loss" position. That is, consumers appear to behave with "bounded" rationality because their level of risk aversion changes based on the direction of their change from a given reference point.

Further supporting prospect theory, consumers actually disclosed *less* location data (via finding clues) and referred fewer friends and family members as the benefits of disclosure increased. As hypothesized above, this is because consumers become increasingly risk averse after finding themselves in a gain position relative to their original reference point. However, privacy calculus still was appropriate in one scenario. In particular, when consumers made their initial and early-term disclosure decisions, their profile information was positively related to the benefits of disclosure. Rather, it wasn't until later when participants returned to edit their profile page that they decided to reduce this effect.

With several measures of disclosure (except for clues and referrals), trust played a larger role than perceived risks. That is, when consumers considered disclosing their own information, they based it on the trustworthiness of the app provider. However, when it comes to disclosing the email addresses of their friends and families, they considered the likelihood and impact of privacy risks. Consequently, our consumers treated the privacy of others as a commodity while their treated their own privacy as a right or a desired state. If this holds in other contexts, then researchers will need to more clearly focus on these distinctions going forward.

Another interesting implication for research is the role that perceived benefits *does not* play in disclosure decisions. After accounting for the *direction of the change* in benefits, perceived benefits had no direct effect on any form of disclosure. This finding underscores the importance of considering risk decisions (at least in the mobile app space) as processes rather than states. Consumers consider the directionality and likely future expectations of benefits over the current perceived benefit of information disclosure.

Lastly, general privacy concern played a larger role in actual disclosure than shown in previous studies of disclosure intentions [2, 3, 7]. Perhaps in known laboratory settings, general privacy concerns are more easily forgotten and relaxed because the participants have no legitimate threat to their privacy. In our context, privacy threats were naturally more legitimate. Another explanation may be that the privacy concern measurement used in this study was based on a more recent instrument that was targeted for mobile privacy concerns including location data [24].

6.2. Implications for Practice

The implications for practice are unique from prior studies. Most importantly, mobile app vendors should be wary of changes in app features and benefits. If the changes are perceived as an attempt to elicit more consumer information, they may have the opposite effect. However, it appears consumers are much more willing to disclose information about others and violate their privacy; hence, the natural points of focus for app providers should be on the perceived commodity of the information of "others" rather than on the consumer.

It appears from our study that privacy concerns in the field are much more salient than in artificial laboratory experiments. Thus, in practice, app producers need to place more effort on understanding and addressing specific concerns consumers might have that should be alleviated.

Perhaps the biggest conundrum of our study for practice is that consumers appear to be considering their original reference point of benefits when making risk decisions regardless of the fact that real risk has not changed. They become risk averse when they are in a "gain" position and risk seeking when in a "loss" position. Thus, the key for app developers is to find ways to move or keep consumers in a "loss" positions, perhaps by making the consumer feel

6.3. Limitations and Future Research

As with all research, there are several limitations of this study that also present useful areas for future research. First, not all consumers were perfectly explained by the prospect theory hypotheses. Some followed the commodity-based view of privacy and increased (decreased) their disclosure as the benefits increased (decreased). All we can tell from this study is that the majority of consumers in this context were best explained by prospect theory. Therefore, it would be useful to further develop theory by explaining why consumers would behave one way versus the other.

Next, we examined only one form of benefits manipulation. Changing the game points for profile data was an easily-quantifiable adjustment. Participants may have been skeptical about the reasons for point changes—leading them to behave differently than, for example, if new levels were added to the game for pure enjoyment unrelated to their leaderboard position.

Another limitation is the context of our field study. Although the perceived risks were real, our app was a game. The enjoyment of a game may trade off differently with perceived risks than, for example, the productivity benefits of an office app, or the health benefits of a fitness app. Future research should explore additional contexts and theorize about the differences between them.

Lastly, our population was not randomly selected and focused on college students in a close geographic area. This was a conscious tradeoff that allowed us to improve the realism of the field experiment. Any social network based context will require that many of the participants be geographically collocated. However, other apps could be examined without the social network context to obtain a more random sample.

7. Conclusion

In conclusion, we executed a realistic, longitudinal field experiment that allowed us to examine the effects of *changes* in the benefit/risk tradeoff. We discovered that consumers exhibit "bounded rationality" in their information disclosure decisions regarding mobile apps. As a result, the commodity-based view of information privacy is only partially appropriate for the mobile app context which incorporates personal information, location data, and social network data. Overall, prospect theory was more strongly supported

8. References

[1] Smith, H.J., Dinev, T., and Xu, H., "Information Privacy Research: An Interdisciplinary Review", MIS Quarterly, 35(4), 2011, pp. 989-1015.

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

[3] Xu, H., Teo, H.H., Tan, B.C.Y., and Agarwal, R., "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services", Journal of Management Information Systems, 26(3), 2010, pp. 135-174.

[4] Keith, M.J., Babb, J.S., Furner, C.P., and Abdullat, A., "The Role of Mobile Self-Efficacy in the Adoption of Location-Based Applications: An Iphone Experiment", Proceedings of the Hawaii International Conference on System Sciences (HICSS '11), 2011

[5] Xu, H., "Locus of Control and Location Privacy: An Empirical Study in Singapore", Journal of Global Information Technology Management, 13(3), 2010, pp. 63-87.

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

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

[8] Acquisti, A., and Grossklags, J., "Privacy and Rationality in Individual Decision Making", IEEE Security & Privacy, 3(1), 2005, pp. 26-33.

[9] Norberg, P.A., Horne, D.R., and Horne, D.A., "The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors", The Journal of Consumer Affairs, 41(1), 2007, pp. 100-126.

[10] O'donoghue, T., and Rabin, M., "Choice and Procrastination", The Quarterly Journal of Economics, 116(1), 2001, pp. 121-160.

[11] Smith, H.J., Milberg, S.J., and Burke, S.J., "Information Privacy: Measuring Individual's Concerns About Organizational Practices", MIS Quarterly, 20(2), 1996, pp. 167-196.

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

[13] Belanger, F., and Crossler, R.E., "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems", MIS Quarterly, 35(4), 2011, pp. 1017-1041.

[14] Bélanger, F., Hiller, J.S., and Smith, W.J., "Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes", Journal of Strategic Information Systems, 11(3), 2002, pp. 245-270.

[15] Westin, A.F., Privacy and Freedom, Atheneum, New York, 1967.

[16] Margulis, S.T., "Conceptions of Privacy: Current Status and Next Steps", Journal of Social Issues, 33(3), 1977, pp. 5-21.

[17] Warren, S.V., and Brandeis, L.D., "The Right to Privacy", Harvard Law Review, 4(5), 1890, pp. 193-220.

[18] Davies, S., "Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity", in (Agre, P., and Rotenberg, M., 'eds.'): Technology and Privacy : The New Landscape, MIT Press, 1997

[19] Thompson, S., Keith, M.J., and Posey, C., "Putting Privacy in Its Place: A Taxonomy of the Costs and Benefits of Location Data Disclosure through Mobile Devices", Dewald Roode Workshop on Information Privacy (IFIP WG8.11/11.13), 2012

[20] Beresford, A.R., Kübler, D., and Preibusch, S., "Unwillingness to Pay for Privacy: A Field Experiment", IZA Discussion Papers, 2010.

[21] Gingrich, A., "The Mother of All Android Malware Has Arrived: Stolen Apps Released to the Market That Root Your Phone, Steal Your Data, Open Backdoor", retrieved May 20th, 2011 from http://www.androidpolice.com/2011/03/01/the-mother-of-all-android-malware-has-arrived-stolen-apps-released-to-the-market-that-root-your-phone-steal-your-data-and-open-backdoor/.

[22] Xu, H., Teo, H.-H., Tan, B.C.Y., and Agarwal, R., "Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services", Information Systems Research, 23(4), 2012, pp 1324-1363.

[23] Posey, C., Lowry, P.B., Roberts, T.L., and Ellis, T.S., "Proposing the Online Community Self-Disclosure Model: The Case of Working Professionals in France and the Uk Who Use Online Communities", European Journal of Information Systems, 19(2), 2010, pp. 181-195.

[24] Xu, H., Gupta, S., Rosson, M.B., and Carroll, J.M., "Measuring Mobile Users' Concerns for Information Privacy", International Conference on Information Systems (ICIS '12), 2012.

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

[26] Gefen, D., and Straub, D.W., "A Practical Guide to Factorial Validity Using Pls-Graph: Tutorial and Annotated Example", Communications of the AIS, 16(5), 2005, pp. 91-109.

[27] Liang, H., Saraf, N., Hu, Q., and Xue, Y., "Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management", MIS Quarterly, 31(1), 2007, pp. 59-87.

[28] Pavlou, P.A., Liang, H.G., and Xue, Y.J., "Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective", MIS Quarterly, 31(1), 2007, pp. 105-136.

[29] Straub, D.W., Boudreau, M.C., and Gefen, D., "Validation Guidelines for I.S. Positivist Research", Communications of the AIS, 13(2004), 2004, pp. 380-427.

[30] Ringle, C.M., Wende, S., and Will, S., "Smartpls 2.0 (M3) Beta", Hamburg 2005, http://www.smartpls.de.

[31] Chin, W.W., Marcolin, B.L., and Newsted, P.R., "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), 2003, pp. 189-217.

[32] Fornell, C., and Bookstein, F.L., "Two Structural Equation Models: Lisrel and Pls Applied to Consumer Exit-Voice Theory", Journal of Marketing Research, 19(4), 1982, pp. 440-452.